**UNIVERSITY OF SOUTHAMPTON**

FACULTY OF PHYSICAL AND APPLIED SCIENCES

Electronics and Computer Science

# Provenance Framework for Additive manufacturing

by

**Nawfal F. Fadhel**

Thesis for the degree of Doctor of Philosophy

September 2017

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

FACULTY OF PHYSICAL AND APPLIED SCIENCES
Electronics and Computer Science

Doctor of Philosophy

# PROVENANCE FRAMEWORK FOR ADDITIVE MANUFACTURING

by Nawfal F. Fadhel

Advances in additive manufacturing have had a disruptive influence to the conventional manufacturing process by bringing manufacturing to the hands of the customer and shortening the supply chain. The customer can customise and manufacture any 3D object using additive manufacturing without leaving their office, lab or home. This paradigm shift in manufacturing raised concerns about the intellectual property rights of 3D objects. At the moment additive manufacturing has allowed owners of 3D printers to fabricate any 3D object with no accountability and no provenance measures for the original authors of the 3D objects. This is a problem because licensing usually allows for limited use and provenance reflects the value of the 3D object.

This work presents a framework for provenance of 3D objects that investigates the transition of security properties from digital 3D objects to 3D printed objects because of the absence of such mechanisms. A wholistic security view of additive manufacturing process by presenting a additive manufacturing security reference model and a tool to benchmark security of additive manufacturing. This framework is intended to facilitate for the industry with the adaptation of 3D printing by engineers, designers and other types of users. The proposed framework is based on digital security measures, physical signing principles and following archival principles to maintain accurate records because of the nature of the transition of properties from digital to analogue records. The proposed framework has the potential of pushing 3D printing adaptation thought sharing and exchange of 3D objects by public and academic domain by using our security framework as enabling technology.

The security reference model for additive manufacturing is intended to provide security by design for any additive manufacturing process, this reference model also covers the cyber to physical security aspect of additive manufacturing.

The benchmarking tool provides a security measure that is flexible and is tailored fit assessment process to any additive manufacturing workflow, it give freedom to security practitioners to fit it to any organisation structure to report on the organisation state of security.

# Contents

# List of Figures

# List of Tables

## Declaration of Authorship

I, Nawfal F. Fadhel , declare that the thesis entitled *Provenance Framework for Additive manufacturing* and the work presented in the thesis are both my own, and have been generated by me as the result of my own original research. I confirm that:

- this work was done wholly or mainly while in candidature for a research degree at this University;
- where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated;
- where I have consulted the published work of others, this is always clearly attributed;
- where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;
- I have acknowledged all main sources of help;
- where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself;
- parts of this work have been published as: (Fadhel et al., 2013a), (Fadhel et al., 2013b), (Fadhel et al., 2014) and (Fadhel et al., 2015)

Signed:.....

Date:.....

## Acknowledgements

To my father, family and friends for patience and support during my studies as a PhD student. To my supervisors, Gary Wills and Richard Crowder who motivated me to think critically and guided me thought the rough road to get a PhD. To my wife Mrs Istebreq Fadhel whom my life was empty then she came into my heart and filled it

# Nomenclature

| | |
|---|---|
| $3D$ printer | Additive Manufacturing Machine |
| $3D$ print | Fabricated Three Dimensional Object |
| $3D$ object | Three Dimensional Object |
| $3D$ scan | Three Dimensional Scan of an Object |
| $3DOI$ | Three Dimensional Object Identifier |
| $3DS$ | Three Dimensional Solid |
| $3MF$ | 3D printing File Format |
| $AM$ | Additive Manufacturing |
| $AMF$ | Additive Manufacturing File Format |
| $CRUD$ | Create, Read Update and Delete |
| $DFX$ | Drawing Exchange File Format |
| $GQM$ | Goal Question Metric |
| $IP$ | Intellectual Property |
| $OBJ$ | Object File Format |
| $MRI$ | Magnetic Resonance Imaging |
| $MVC$ | Model View Controller |
| $PLY$ | Polygon File Format |
| $SAT$ | Spatial ACIS File Format |
| $STL$ | STereoLithography File Format |
| $STEP$ | Standard for The Exchange of Product Model Data File Format |
| $SECaaS$ | Security as a Service Cloud Based System |

# Chapter 1

# Introduction

Piracy, counterfeiting and unlicensed exchange of digital objects are rampant in cyberspace according to an assessment by (Chaudhry and Walsh, 1996) on the global market, with the introduction of affordable 3D printers, there is a genuine concern that 3D printers will be exploited to produce illegal and unlicensed 3D objects (Bradshaw et al., 2010). On the other hand, creators of 3D designs struggle to prove their ownership of 3D printed objects as the provenance associated with digital objects is not transferable. Information such as author, created date, description, etc. is lost in the 3D printing process. As an introduction, this chapter reports on the first attempts in digitising and transmission of a 3D object, to be fabricated by a 3D printer. The first digitizing attempt to reproduce a 3D object was the Michelangelo project, as a case for large-scale digitisation. The first transmission attempt of an object was the 3D faxed Buddha (Curless and Levoy., 1996a). In this work the term 3D printing and additive manufacturing is used interchangeably.

## 1.1 First attempts to 3D scan objects and 3D print them

This research attempts to understand the provenance of additive manufacturing, and for this purpose two examples are presented. The first is Digitisation and the other is Transmitted Fabrication Figure 1.1. These will be explained using the cases of the Michelangelo project and the 3D Fax. Both have been researched by Professor Levoy from Stanford University who specialises in 3D digital technologies and computer graphics (Curless and Levoy., 1996a),(Koller and Levoy, 2005) and (Curless and Levoy., 1996b).

### 1.1.1 Digitisation - The Michelangelo Project

Between 1998 and 1999 the Universities of Washington and Stanford sent a project expedition of 30 people from staff, students and faculty members to Rome. They had an

opportunity to study the statue of David, one of the great Michelangelo masterpieces, as illustrated in Figure 2.4(a), which is a 3D digital capture of the actual sculpture. This was called *The Digital Michelangelo project* (Koller and Levoy, 2005). The project's aim was to digitise the works of Michelangelo and make them available for study as a digital preservation measure.

### 1.1.2 Transmitted Fabrication - 3D Faxed Buddha

In 1996 Levoy successfully 3D scanned and transmitted a 6-inch Buddha statuette, as shown in Figure 2.4(b), in the form of a 3D digital file, to a company called 3D Systems located 400 miles away (Curless and Levoy., 1996a). Previously, Levoy and Curless constructed a 3D Fax machine to build complex 3D models from bulk images describing a single object (Curless and Levoy., 1996b). After 3D Systems received the faxed 3D design, consisting of 300 layers, the company sent a 3D printed replica back. This was a world first on transmitting 3D data, and cuts production time of high quality detailed objects, as discussed by Levoy in his interview (Curless and Levoy., 1996a).

(a) 3D digital capture of the digitised Michelangelo's David

(b) Replica of 3D printed Buddha Statuette

Figure 1.1: 3D scanning and 3D printing samples by Professor Levoy

## 1.2 Research Conjecture

Personal fabrication at home using 3D printing technology is widely accessible. 3D printing, also referred to as additive manufacturing, is improving in build quality and material types. 3D printing libraries are getting a lot of attention with new easy-to-use 3D design tools such as google SketchUp[1]. This has resulted in a counter-reaction with an increased demand for restrictions, and intellectual property (Weinberg, 2010). There thus needs to be some means of establishing digital identity that is both transferable and measurable; transferable from digital to physical, and measurable of the degree to which the physical is identical to the original digital file. *Is what you have, what you print?*The following are research terms that are used throughout the research:

**Digital Identity for 3D objects and 3D prints** by which a 3D object or a 3D print is identified by a unique global number that can be cataloged and meta data associated.

**Transferable Identity** Means the intellectual property rights are transferred to 3D object when its digitised or released through digital design. Also means the intellectual property rights are transferred to a 3D print if the object is fabricated using additive manufacturing technology.

**Measurable Identity** Means there are quantifiable evidence to establish that the transference of intellectual property has occurred.

## 1.3 Thesis Structure

This chapter sets the scene with the importance of 3D digitisation and 3D objects.

Chapter 2 reviews the literature on the technologies and concepts that are at the centre of additive manufacturing. It discusses the human-object relationship and the nature of these objects, as well as the uniqueness of 3D objects and the meta-data that establishes provenance for a 3D printed object.

Chapter 3 explores the motivation for tackling this problem. Therefore, this starts with careful examination of the legislation for additive manufacturing, as well as a discussion of a case of attempted infringements of additive manufacturing. The chapter explains the security procedures for protecting digital content and provenance for digital objects in general, such as the use of digital media and electronic documents. Then use the threat types that are usually associate with digital files such as office documents, music and film, then apply these threat types to additive manufacturing. The chapter then investigates the same procedures for 3D objects and articulates their shortcomings.

[1] www.sketchup.com

Chapter 4 presents the research question and research methodology. The discussion identifies the research gap, derived from current concerns with additive manufacturing using threat analysis. Three research questions are formulated that focus on exchange of 3D objects, based on information security research for protecting digital objects, not specific to additive manufacturing. The research methods concentrate on building an appropriate framework for establishing provenance for additive manufactured objects.

Chapter 5 focuses on the first research question that was answering using data sets and information models of the threat scenarios (actual and hypothetical) that could affect additive manufacturing to build an AM threat model. It also designs the additive manufacturing information model.

Chapter 6 following publication of the outline framework, work investigated the second research question to find out the components of the framework, using the goal question metric approach from which framework version 1.0 was constructed describing the components and the metrics.

Chapter 7 focuses on the second research question that was answered using an expert review preceded by these preparation stages: First stage an initial set of components was proposed using GQM as illustrated in Framework version 1.0 in Chapter 6; Second stage refine the initial components by the using several processes and third stage conducting the first expert review to confirm the components through interviews and focus groups to gather quantitative and qualitative data.

Chapter 8 focuses on the third research question that was answered using a second expert review. The second expert review was longer and more comprehensive than the first expert review, the main objective was to answer research question three to confirm and refine the proposed metrics for the components of the framework.

Chapter 9 focuses on the fourth research question that was by providing the information necessary to build a provenance system that serves additive manufacturing process using software requirement validation by protoype method.

Chapter 10 Summarise the research output and future work.

## 1.4 Research Outputs

This work has led to the following publications:

Fadhel, N. F., Crowder, R. M., and Wills, G. B. (2013). Maintaining provenance throughout the additive manufacturing process. *IJISR*, 3(3):466-475.

Fadhel, N., Crowder, R. M., and Wills, G. (2015). Provenance in the Additive Manufacturing Process. *IFAC-PapersOnLine*, 48(3):2345-2350.

Fadhel, N. F., Crowder, R. M., Akeel, F., and Wills, G. B. (2014). Component for 3D printing provenance framework: Security properties components for provenance framework. *World Congress on Internet Security (WorldCIS)*, pages 91-96.

Fadhel, N. F., Crowder, R. M., and Wills, G. B. (2013). Approaches to Maintaining Provenance throughout the Additive Manufacturing Process. *World Congress on Internet Security (WorldCIS)*, pages 82-87.

# Chapter 2

# Background Literature

Additive manufacturing, sometimes referred to as additive manufacturing or rapid prototyping, is a disruptive technology that carries a significant risk. The idea of additive manufacturing started as a mock article in 'New Scientist' under the name 'Daedalus' by David Jones (Jones, 1974). David described how a computer could be used to control a laser using a program to create 3D objects. This technique takes advantage of photo-polymerization phenomena of some resin material that hardens when exposed to light. It was later found that Wyn Kelly Swainson had filed a patent in 1971 Swainson (1977) for the same concept that was later published in 1977. Since then there have been great advances in quality, price and adoption rate. When additive manufacturing is examined it is observed that these machines could be used legally or illegally to replicate or counterfeit someone elses intellectual property.

A part of good research is building an understanding of the research background and research problem (Shaw, 2002). Therefore, this work starts by listing the available technologies for additive manufacturing. These techniques are used by a wide variety of vendors such as Stratasys, and Inkjet head additive manufacturing. These machines require 3D files as input to fabricate 3D objects and these are produced in many formats, such as 3MF, AMF, and STL. The data stored in these files arise from the object creation processes of designing, scanning, and sketching of 3D objects. The value of the 3D object created will depend on the object type and its intellectual property. These 3D objects are protected in a number of ways under existing laws and legislation that was formed to originally protect physical goods but is also used for 3D digital objects. Laws and legislation depend on some cyber security measures to make sure that the provenance of digital information received are described correctly (Davies, 1983).

Whether it is legal, legislative or cyber security measures, all are measures of protection. Further examination shows that there is a lack of knowledge feedback mechanism and tracking. There are gaps in knowledge transfer or weakness in the cyber to physical transition of the 3D object.

Figure 2.1 is an illustration of areas in sequential order that are involved in creating 3D objects. These areas are directly related to this work, as these need to be discussed before examining the provenance of 3D objects and 3D printed objects.

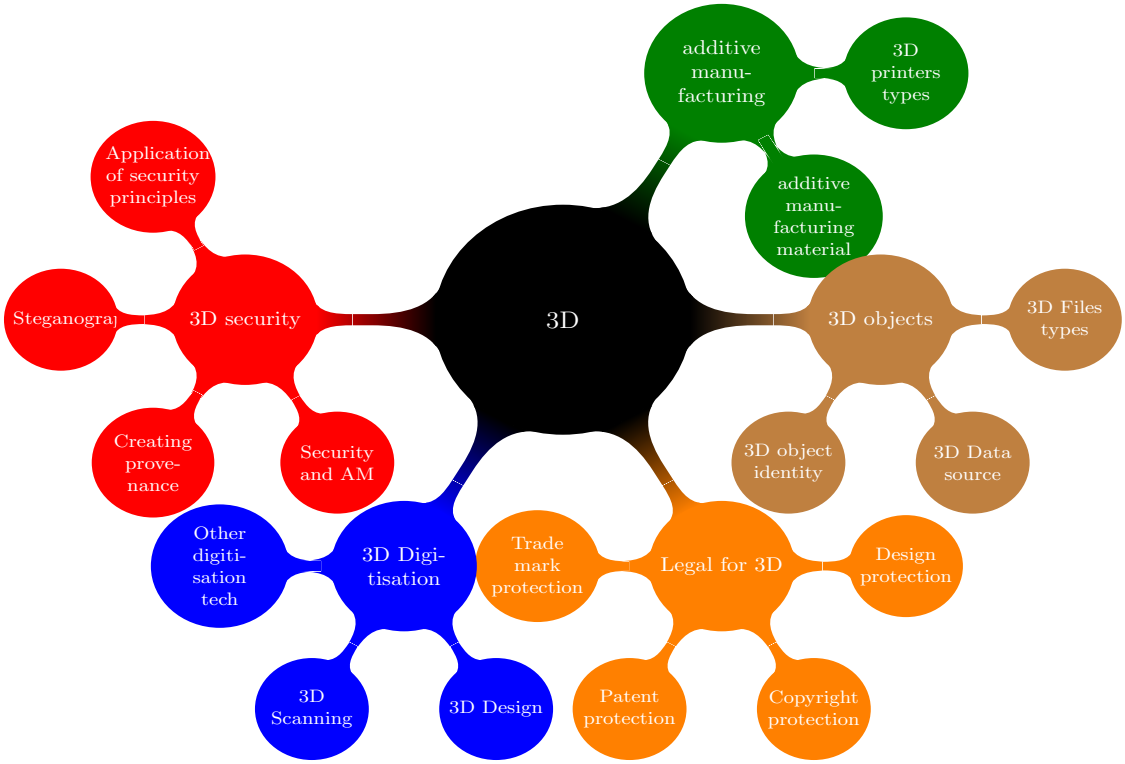



Figure 2.1: Mind map of all areas associated with creation and securing 3D objects and 3D prints

## 2.1 additive manufacturing technology

Additive manufacturing technology is an additive manufacturing technology where a 3D design is uploaded into a machine that accepts a digital design as input, which the machine will then build out of physical materials such as polymers, ceramics or metals. The process is illustrated in Figure 2.2

The three types of additive manufacturing methods are: Granular material binding, Molten polymer deposition, and Photo-polymerization. These methods are adopted by an array of manufacturers so there are many brands [1].

**Granular material binding** uses polymer powder that is spread and heated after which another layer is added. The end result is a smooth 3D object with movable parts embedded inside the object (Mellis, 2011).

[1] www.imakr.com

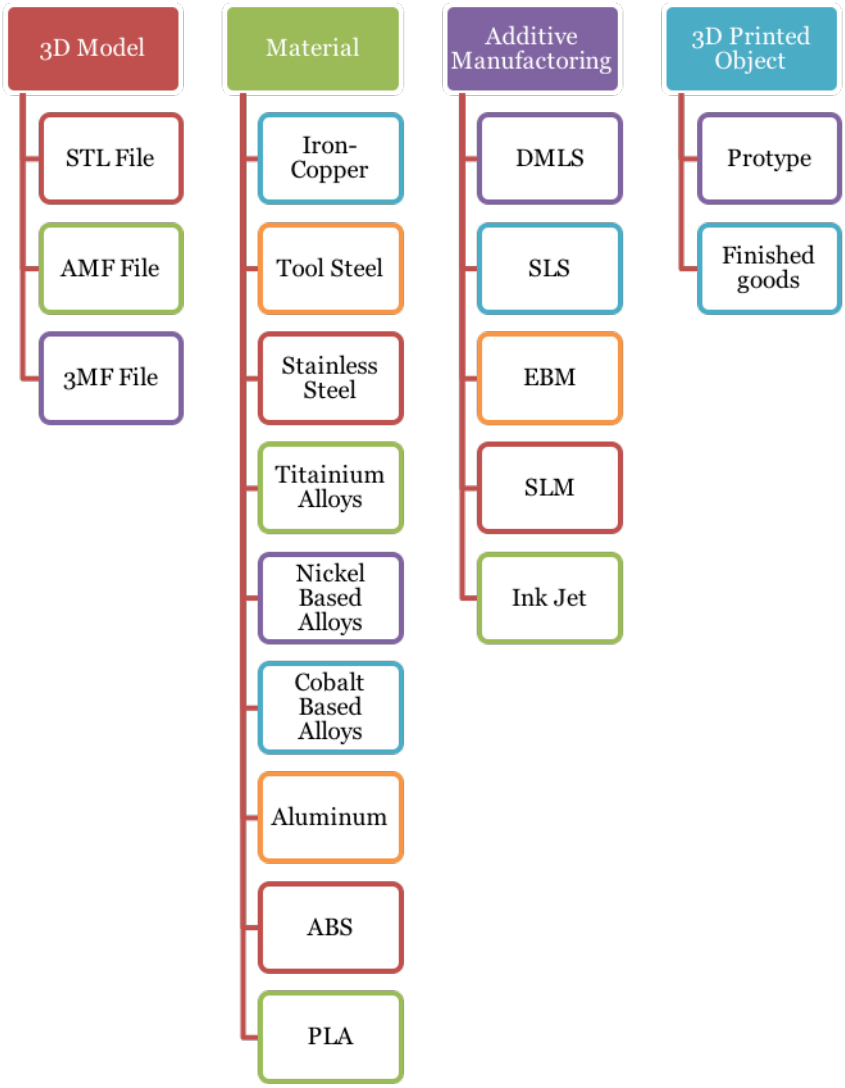



Figure 2.2: additive manufacturing Technology Work Flow

**Molten polymer deposition** uses a robotic arm with a heat gun that heats a plastic tube and melts it over a levelled surface, adding layer over layer resulting in a crude 3D object with unmovable parts (Mellis, 2011).

**Photo-polymerization** takes advantage of light-sensitive material that hardens when it is exposed to a light source (Mellis, 2011).

The commonality between the three methods is that they all use additive manufacturing technology, where the object is built incrementally one layer after another. The goal of additive manufacturing is to be able to achieve tool-less finished goods using rapid manufacturing (Bak, 2003). The quality of the object produced by additive manufacturing is dependent on the resolution capability and material. The method of printing affects the end product complexity and whether it can have movable parts within an object. The complexity, material, weight, colour and texture of object determines the type of

additive manufacturing. For example, research is being carried out on additive manufacturing of cultural heritage artefacts such as bones in zoology or in reconstruction efforts of damaged artefacts (Allard, 2005).

According to BS ISO Draft 17296-4 Additive manufacturing - Rapid technologies (rapid prototyping) (17296-4:2014, 2013), Figure 2.3 illustrates the 3D object printing process with the pre-processing involved. Note that all generation of new knowledge stops after creating the 3D printed object.

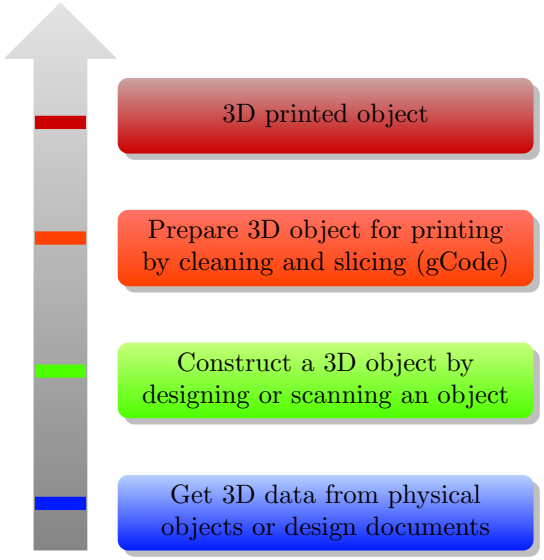



Figure 2.3: Data Creation from Design to Fabrication inspired by the British standard for digitisation engineering artefacts

### 2.1.1 Granular Material Binding

This technology uses powdered polymer. The material powder is sprayed, and the particles are then heated with a laser to solidify them. Layers are added incrementally, and this process can last for hours or days, depending on the level of detail and accuracy required (Levy et al., 2003). The infused material will serve as support for the layers that are being printed and the material can vary for a range of metals and polymers. Five techniques are used to achieve this: Directed metal laser sintering (DMLS), Selective laser sintering (SLS), Electron beam melting (EBM), Selective laser melting (SLM), Inkjet head additive manufacturing.

SLS and DMLS are very similar, except the SLS requires the polymer binder to be removed or de-binded after sintering; they also require thermal treatment after printing and both operate below the melting point of the polymer. The EBM and SLM produce similar results; the EBM uses an electron beam in a high vacuum, while SLM uses a high focus laser. They do not require thermal treatment, as both operate at temperatures up to 1000 °C; the result is heavy, solid, dense and void-free. The final technique is referred

to as Inkjet additive manufacturing; it is similar to laser sintering, but instead of using a laser or an electron beam it uses a liquid binding material to bind the material on the powder bed (Sirringhaus et al., 2000).

### 2.1.2 Molten Polymer Deposition

This technology was developed by Stratasys by Scott Crump in 1988, which is based on fused deposition modelling (FDM) technology (Gill and Syan, 2006). The method follows these stages: a geometric AutoCAD Design is created, the design is fed into slicer software, and the slicer splits the object into horizontal layers. The resulting object is aligned and oriented, and the support structures added, which are pieces of polymer to support the design weight while it is printed. The slice thickness is between 0.172 and 0.356 mm. The design is uploaded into the 3D printer to be printed using a tube of plastic polymer filament which is pulled from a reel, fed into a moving robotic head that moves in the X,Y-axes with a heated extruder. The head moves in X and Y directions building the 3D design from the plastic polymer filament incrementally. The increment slices are printed on top of each other until the last slice is printed.

### 2.1.3 Photo-polymerization

Commonly known as Stereolithography was developed by 3D systems by Charles Hull. This additive manufacturing technique exploits the property of liquid resin that changes state when exposed to UV light, resulting in a hardened material. The UV light pattern is projected on the surface of the liquid resin with a flat platform underneath it; the UV light hardens the resin and as it hardens then platform is lifted up a layer and a different UV light pattern is projected. The hardened resin starts to build up on the previous layers in an incremental manner (Okubo et al., 1972).

## 2.2 Digitisation technologies

Data acquisition of 3D objects is the initial step toward a concept design, digital archiving or digital preservation. An object source could belong to either a physical object that is acquired with precise measurement, such as the scanning method discussed by Celani et al. (2009), or an original creation by an individual that is realised through digital-aided tools like AutoCAD. The domain is split into: the information such as Designing, Scanning and Sketching, and the technology such as 3D printers and scanners. Makerbot 3D printer and NEXTGEN 3D scanner are examples of the technology domain processing. 3D laser scanning is used for generating 3D designs using specialised hardware, and sometimes specialised imaging hardware is used for digitising archaeological finds or other special needs. The environment to be digitised has a impact on which

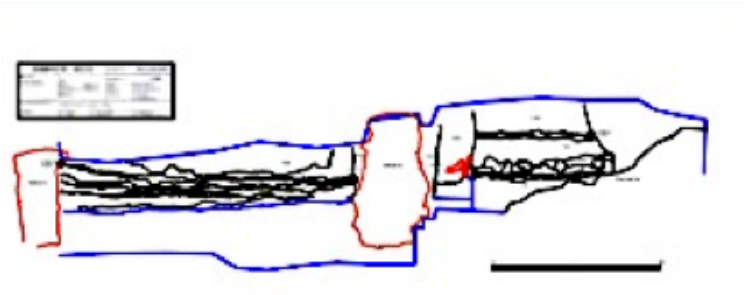
specialised hardware is used, and that depends on environmental conditions such as a controlled environment or outdoors, such as a desert or a jungle. (Schäfer et al., 2011) and (Celani et al., 2009).

### 2.2.1 Designing objects

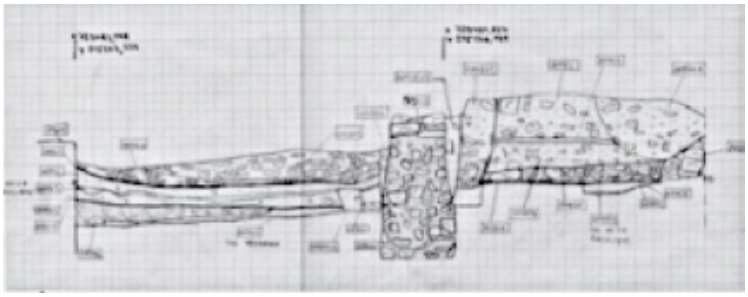
3D design tools like AutoCAD and other graphical design applications (Delgado et al., 2012) are used to create 3D object files. Image processing techniques such as pixelated texture mapping at a software level are also examples of the information domain processing.

### 2.2.2 Sketching objects

Sketching by hand or using digital tools such as Ispace by Nikon (Beuvray, 2008) are methods used to digitally capture the dimensions of a site or used to scan very large objects; Figure 2.4 is an example of this method. Google sketchup is also a popular free software tool that has received a lot of attention recently due to its user-friendliness [2].



(a) Digital sketching using Ispace by Nikon



(b) Hand sketching using pencil

Figure 2.4: Sketching excavation site using hand drawing and Ispace

[2] www.sketchup.com

### 2.2.3 Scanning objects

There are several steps for acquiring 3D digital data (Celani et al., 2009), (Grosman et al., 2008) and (Karasik and Smilansky, 2008). A typical scanning process has three steps in common.

**Preparation process** This involves tasks such as proper alignment, for example, on rotating scanning tables, where the object has to be centralized on the tray; and cleaning the object properly with the correct tools and with the help of professionals, or curators in the case of museum artefacts.

**Scanning process** Several solutions could be used, such as NEXTGEN scanner, which is handheld. The scanning hardware comes in different brands and packages; for that reason, some work has been carried out on benchmarking procedures.

**Cleaning process** Cleaning digital data and removing unwanted pixels or edges. Meshlab is one of the open source tools used for this purpose.

A number of problems occur in 3D scanning such as the reflective property of certain objects, or the size being too big for the scanner. There are a number of solutions for these problem objects (Celani et al., 2009). A completely different set of problems occurs when an object is scanned in an uncontrolled environment and not on museum grounds. One example is the lighting conditions; in a museum the lights can be switched off. If, for example, the scan was taking place in a jungle in Cambodia, nightfall may bring wild animals close, whereas in the morning inside a tent, the temperature could rise as high as 65 °C, as discussed by Schäfer et al. (2011).

In summary technologies used are laser scanning using structured light with motion tracking, and hybrid technology that uses sensors with geo-location. These technologies are used to extract 3D object geometry to create a 3D object of the original physical object; additional metadata then is added to the 3D object when the digitisation is complete.

## 2.3 3D objects information

3D objects can either be natively digital or natively physical, which refers to the initial object inception when first created, for example, chiselling a statue or creating a design using a 3D design tool. Not all 3D objects are printable because they do not hold structural integrity therefore these virtual replicas are visually observed on screen displays (Forte and Kurillou, 2012). Examples of 3D technologies used for visualisation purposes include the fashion industry using additive manufacturing to print new types

of fabric (Perona et al., 2012). A medical profession example would be a MRI scan as a diagnostic tool to filter for disease and anomalies with the body, and also to train future doctors.

Development of new data types and digitisation technologies is driven by a need in a specific domain that lacks a specific imaging feature, or by improving an existing feature or manufacturing procedure. The following section discusses 3D objects and file formats. Constructing 3D digital objects started with the invention of the .obj file format by Wave Front Technologies (Burkardt, 2004), which was followed by a number of file formats to accommodate different industrial or commercial needs, such as .amf (52915, 2013).

### 2.3.1 3D Data sources

There are two streams of 3D data for digital media content, classified into four types of object data source. The first stream is based on actual physical objects, which are:

**A Replica** : a digital copy of an object with exact measurements taken using a digital tool such as 3D a scanner.

**A Reconstructed Replica** : a digital copy of an object with reconstructed design based on fragments and documentary description of the missing areas of the original object. For example, reassembling pieces of bones of a dinosaur (Niven et al., 2009).

The second stream could be based on descriptive or artistic visualisation of an object such as described in ancient texts or a genuine artistic creation, which are:

**A Dictated realisation of a design** : a digital copy of an artistic presentation based on a description of an object that was measured and documented in the archaeological record. For example, the Bayman Buddha in Afghanistan that were destroyed by the Taliban (Manacorda and Chappell, 2011).

**An Inspired realisation of a design** : a digital copy of an artistic presentation based on a description of an object that was mentioned in historical record in poems and/or inscriptions. For example, the artistic presentation for the Colossus of Rhodes (Maryon, 1956).

### 2.3.2 Human-Object relationship

The emergence of affordable home fabrication using 3D printers has created an historical precedent in changing our understanding of human-object relationships. Sterling (2005) cites five types of object in the object-human relationship:

**Artefact** : one-time creation, no two artefacts are completely identical.

**Machine** : precise replicas of the same artefact.

**Product** : precise replicas of the same artefact that are widely available.

**Gizmo** : precise replicas of the same artefact that are widely available and offer new knowledge.

**Spime** : precise replicas of the same artefact that are widely available that offer new knowledge and are traceable as well.

Affordable 3D printers are introducing a techno-social transformation to the manufacturing paradigm. The growing additive manufacturing community is producing objects that were un-manufacturable using conventional methods. This created sizeable novelty because 3D printed objects are neither Gizmos nor Spimes.

### 2.3.3 Digital identification of 3D objects

Digital identifiers not to be confused with digital indexes is where a unique identity is assigned to a digital object. Usually digital identity is established by assigning unique identifiers to a dataset using digital signing procedures and are best assigned when the object is created because the information documentation occurs after building an identity. The digital object identifier (DOI) is discussed by Wynholds (2011) who examined the characteristics of an information object and how it could be distinguished from other objects using metadata and other object identifiers. According to Birnholtz (2006), digital identity can also be associated with entire data sets instead of a single object. In industry today, unique identification numbers are assigned to physical objects similar to that used in packaging products (Simske, 2011) and are referred to by Physical Object Identifier (POI).

Hypothetically, the uniqueness of a 3D object can be achieved by adding a digital signature to the 3D design, rather than removing a part as in the case of watermarking 2D objects, where the Least Significant Bit (LSB) is manipulated to embed information (Ohbuchi et al., 2001). Or a unique identity can be imbedded into the 3D object XML meta data which this has been accounted for but not yet used in industry are AMF and 3MF that are described in 2.3.4

### 2.3.4 File Formats for 3D

Many data types are used to represent 3D objects - X3D (VRML), STEP, SAT, DFX, DWF, DWG, 3DS, SLC, OBJ, PLY, STL, AMF and 3MF - some of which can be used directly with 3D printers and some need conversion before manufacturing. However,

some 3D objects are not printable using 3D printers because some 3D objects do not have structural integrity once printed. 3D objects can be made of a variety of materials, such as PLA or ABS.

An STL file is the most widely used file format for additive manufacturing and only contains the geometry of the object. It lacks features describing the object, such as colour, or containing metadata about the object.

Discussing the shortcomings of the current STL and an initiative for starting STL 2.0 is described in Hil (2009), which eventually led to the creation of AMF (Additive Manufacturing File) format in draft BS 52915 (52915, 2013). AMF allows metadata as well as other features such as colour, texture and different materials in 3D object data files. For research purposes, the AMF format will serve as an appropriate file type because metadata accommodates these features and also the capability of including security identifiers (52915, 2013) unlike other file formats that do not support this feature.

**3DS file format** : Based on a triangular mesh created by Autodesk to handle 3D modelling and animation, it has definitions for texture and colour information as well as lighting and animation information, and can handle up to 65,536 vertices and polygons Velsen,M. (1997).

**3MF file format** : The 3D Manufacturing Format is third development of 3D file formats to support additive manufacturing after STL and AMF. This file formate allows stronger integration of design into manufacturing apparatus, including more support and XML space for digital signing and managed additive manufacturing (Consortium, 2015).

**ACIS SAT file format** : Spatial Corporation developed this file format that is mostly used in defining boundary descriptors (B-Rep) objects in CAD software. The entire format is based on a topological data structure which makes it difficult to understand and not suitable for exchange purposes.

**AMF file format** : ASTM Committee F42 on Additive Manufacturing Technologies developed the AMF file format (52915, 2013). The AMF file format is very similar to STL but offers XML externally for security and additional information. However, it is still not fully exploited.

**DFX file format** : Drawing Exchange Format was originally created by AutoCAD in 1982 to handle 2D drawing. It allows the definition of 3D triangles meshes and solids (AutoCAD, 2014).

**OBJ file format** : Developed by Wavefront Technologies, it is the most widely accepted 3D file format (Burkardt, 2004). The OBJ file format appeals to 3D graphics designers and engineers. The format is used to store object geometry and surface texture using triangles or higher degree polygon meshes. It also supports

ASCII and Binary encoding as well as containing more than one object in one OBJ file, and can include data about textures, but does not include information about the material or microstructure volumetrically.

**PLY file format** : Greg Turk developed PLY at Stanford graphics lab under the supervision of Marc Levoy (Bourke, 2012). The PLY design was based on the OBJ file format, which lacked grouping capabilities and arbitrary properties. PLY was originally designed to accommodate 3D scanning technologies and uses polygon meshes and can include data about texture and colour, but does not include information about the material or microstructure volumetrically.

**STL file format** : This was the first file format to be used with additive manufacturing. Designed by 3D Systems, STL was primarily designed to be used with stereolithographic additive manufacturing technology designed by Hull (1986).

**STEP file format** : Stands for *Standard for the Exchange of Product model data* and is an interface file format to exchange 3D information from and to different CAD systems. The file format has definitions for general-use solid model representation by extruded and swept solids, wireframe, Boolean primitives modelling, and other modelling paradigms that can be used to represent a 3D object (Gilman and Rock, 1995).

## 2.4 Legal and legislation

Copying a 3D object or 3D printed object without permission of the IP holder is considered infringement regardless of copying process whether its conventional manufacturing or additive manufacturing. Manufacturers of counterfeited products often produce in countries where the intellectual property rights (IPR) are either lax or where the IP is not registered or do where intellectual property rights do not exist. That leaves IPR owners dependent on customs authorities stopping counterfeited goods from being imported into areas where the IPR is enforced. However, 3D objects can be emailed cross borders and are not within the customs authorities detection ability which poses a major problem for IPR holders.

The concept of securing 3D designs or 3D objects, i.e. artifacts, is examined by the British Standard 52915 (2013) covered under secure designs/secure hardware and has applications in many domains. For example, the cultural heritage domain for the exchange of cultural heritage artifacts between universities and museums (Celani et al., 2009), (Scopigno et al., 2011), and in the private sector in the area of rapid prototyping and manufacturing. Therefore, it is important to secure designs by signing them to prevent theft or illegal exchange of information. The cultural heritage domain is a perfect workspace where the difference between native physical objects and native digital objects is evident and this clarity will allow for measurable goals when proposing

a new security framework. Provenance of physical objects is addressed by a number of intellectual property laws, trademarks, and hallmarks. The following are four scenarios in which a 3D printed object can infringe copyright, but under very specific conditions, as detailed in Bradshaw et al. (2010).

**Design protection** protects how an object looks as a whole or a part that makes the feature of a product. In general, it protects the products that cannot be protected using copyright law or patent. However, design protection is difficult to enforce because even the smallest of changes produce a derivative which makes copying hard to prove.

**Copyright protection** protects creative works, mostly covering literary and artistic works that last as long as the creator is alive then 70 years after the IP author passed away or 25 years if less than 50 items produced. produced

**Patent protection** protects the author of an invention from re-manufacturing without permission (normally for 20 years). It protects products based on function, not aesthetics.

**Trademark protection** protects the registered right of a company to indicate the origin of goods. So it protects companies from having its logo or brand from being used without permission.

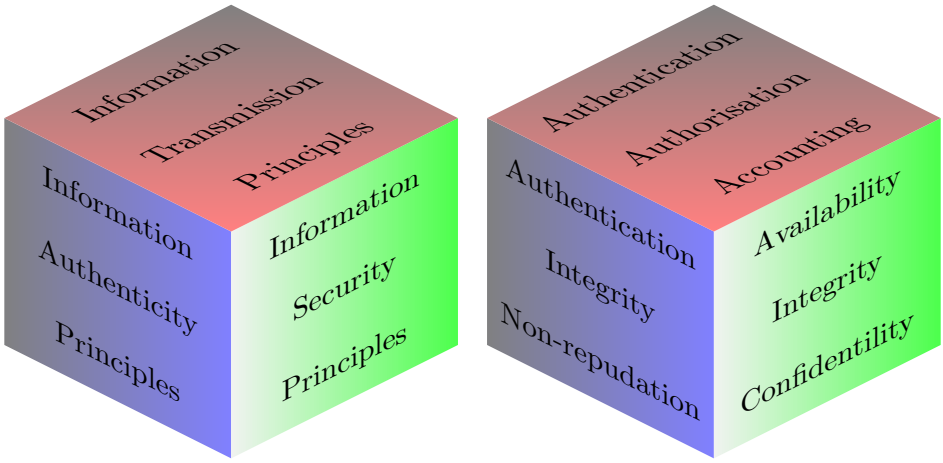
There is also the case of trade secrets where a formula can be registered and hidden from the public, but since the focus is on infringements on 3D printed objects or digital designs it falls outside the scope of this work. For a 3D design to be protected in the cultural heritage domain, it needs to follow one of the criteria described, otherwise it could either be watermarked with one the methods described in the survey by Alface and Macq (2007) or the owner could register the piece with an artwork registry or similar, such as the Artwork Registry [3].

Before addressing the complexities of securing additive manufacturing, digital rights management (DRM) for the music and film industries must be understood because exact replicas may be produced. However, low cost 3D printed objects do not have the same or close to the quality of the original, so they do not produce exact replicas, although that is the ultimate goal for developing additive manufacturing (Berman, 2011).

## 2.5 Security Principles

The three main components of security principles are: information security, information authenticity, and information transmission (McConnell, 1994). The principles and their properties are mapped in Figure 2.5

[3] www.artworkregistry.com




(a) Cyber security principles

(b) Corresponding properties for the security principles

Figure 2.5: Cyber security principles and corresponding properties

**Information security** requirements for physical and digital objects are confidentiality, integrity and availability (21827:2008, 2008), also known as the CIA security model as a universal security model:

**Confidentiality** : A property where information is only disclosed to authorised individuals, parties or processes (7498:1984, 1984).

**Integrity** : In Computer Science, data integrity is defined as the process where data is maintained to achieve a high level of accuracy and consistency over its life cycle (Boritz, 2005).

**Availability** : A property where authorised access is provided upon request from a trusted individual, party or process (7498:1984, 1984).

**Information authenticity** The principles for digital signing have not changed since its introduction in electronic exchange. Digital signing is a method by which the authenticity of electronic mail is proved by providing evidence that the message has not changed and the sender is identified (Davies, 1983). A digital signature holds the same value as a hand signature but is constructed using digital means to render it immune to counterfeiting by making the signature undeniable by the originator and receiver of the message. Digital signatures are used for signing confidential documents. The requirements for digital signing of digital documents is recognised by cryptographers as having three underlying principles: authentication, integrity, and non-repudiation (7498:1984, 1984). They are described in Davies (1983), Rivest et al. (1978) as:

**Authentication** : A property where a claim of identity is verified. The term authentication is used in conjunction with integrity, which is defined according the British

Standard as a property in which the data has not been altered or destroyed in an unauthorised procedure (Burrows et al., 1989), (Cullen et al., 2000).

**Integrity** : The same definition is used for data integrity that is used in physical security components but for digital components. It does not extend to the hardware (Boritz, 2005).

**Non-repudiation** : A state where an entity involved in a communication with other entities is unable to deny involvement in the communication between parties (7498:1984, 1984).

Digital signing must also fulfil some basic elements as described in Davies (1983), Rivest et al. (1978). In digital signing, a party of at least three is needed, which is why a signing authority is called a third party. When signed information is stored and accessed, a transmission occurs because provenance is achieved using the third party. The signature contains the information about the signed material, which is the message.

**Information Transmission** The requirement for digital exchange and storage is authentication, authorisation, and accounting, and is also known as the AAA model, which has the following properties:

**Authentication** : The same definition that is used in the digital security component.

**Authorisation** : A property where access is granted to resources based on access rights (7498:1984, 1984).

**Accounting** : A property where actions and interactions can be uniquely identified and traced (7498:1984, 1984).

### 2.5.1 Correlation between security principles and additive manufacturing

Security is defined in the OED as freedom from risk, danger, fear, anxiety, or avoiding any type of loss (Stevenson, 2010). The universal need for security, as eloquently put in 1956 by Dag Hammarskjold, the second Secretary-General of the United Nations, is defined as *Freedom from fear* which sums up the whole philosophy of human rights.

Securing a physical object is straightforward: place the object in a safe. It could be signed with a wax seal or ink to prove whom it belongs to, maker or manufacturer. These tasks can be automated; such is the case with HP Smart packaging (Simske, 2011). However, the same cannot be said about digital security. Digital security roots can be traced to World War 2 with the enigma encoder and the construction of the Colossus machine in Bletchley Park to break the enigma code. From then on, technological

acceleration in cryptography began between coders and breakers, as documented in *Colossus: The secrets of Bletchley Park's code-breaking computers* (Copeland, 2010).

With the introduction of additive manufacturing, usage of digital objects to reproduce a physical replica - sometimes with high precision - is an achievable task, using the STL file format and 3D printers. Physical objects are currently described as 3D objects using XML form, the transmission is digital, and the transmitted objects are 3D printed through a 3D printer. This process needs to be re-assessed to enable the legitimacy of a 3D object to be proved, whether it is in a digital or physical state. There exist a number of solutions to protect 3D content, but in general there are three streams.

**Protecting digital content locally**: Such technologies are focused on watermarking and data rights management that uses a watermarking scheme propagated throughout the polygon mesh as discussed in Alface and Macq (2007), and largely follows the framework available for multimedia content. Figure 2.6 illustrates the cause and effect diagram in the absence of information security properties to secure 3D prints fabricated using 3D objects.


Figure 2.6: Cause and effect diagram for securing additive manufacturing information

**Protecting 3D object after printing**: Such technologies focus on securing the 3D printed object (physical) by either adding information steganographically to the physical object or by embedding tagging chips into the 3D printed objects Sangoi and Smith (2005). Figure 2.7 illustrates the cause and effect diagram in the absence of information authenticity properties to authenticate 3D prints fabricated using 3D objects.

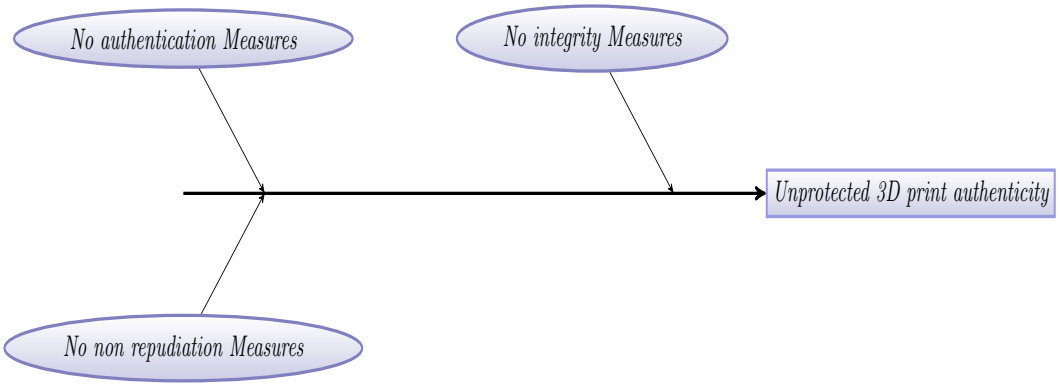



Figure 2.7: Cause and effect diagram for securing additive manufacturing authenticity

**Secure network transmission over the network**: Such technologies use secure digital transmission as discussed in Koller and Levoy (2005), who used an encrypted remote rendering approach to circumvent any data capture from a malicious source. Figure 2.8 illustrates the cause and effect diagram in the absence of secure information transmission properties of 3D prints fabricated using 3D objects.

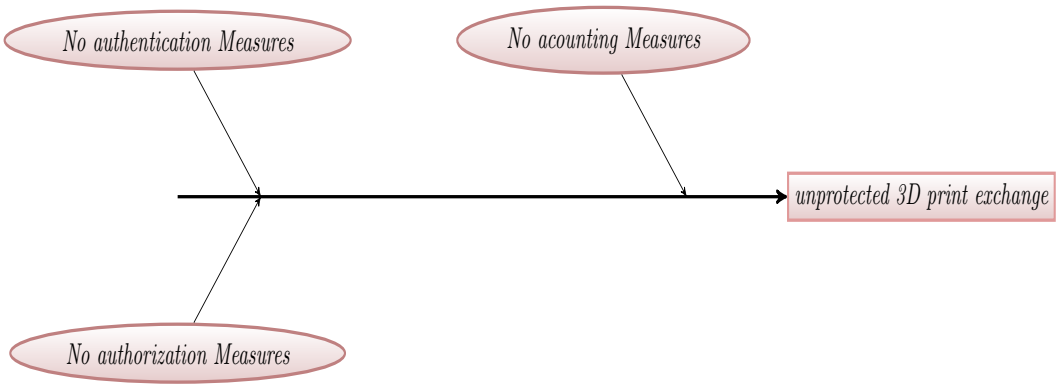



Figure 2.8: Cause and effect diagram for securing additive manufacturing transmission

The literature shows the additive manufacturing protection mechanisms are based on cyber security principles as showed in Figure 2.5. For example, the use of RFID (Sangoi and Smith, 2005) inside 3D printed objects or watermarking a 3D object (Wu and Cheung, 2012). Therefore the construction of new mechanisms for additive manufacturing can be achieved by using the same semantics that are used to provide security for digital objects such as E-mails and electronic documents, such as noting the author of a document, acknowledging the reception of a document, witnessing the document signing, and agreeing that the document is genuine when and where it was accessed, among other processes.

### 2.5.2 Application of security principles to 3D Objects

3D objects exist in one of two states; either the object is native digital and does not exist in the real world yet, or is a scanned digital copy of a real physical object and is therefore considered natively physical. The problem facing 3D objects and 3D printed objects is the issue of provenance. 3D printed objects at the moment have no metrics of provenance especially designed for them, but instrumental solutions outside the digital domain could prove viable, such as content streaming, digital watermarking, embedding RFIDs, and steganography. A number of watermarking methods are described by Alface and Macq (2007). Steganography and watermarking are similar in their philosophy of hiding the information, as both use part of the object they are protecting. However, steganography is a covert measure for protecting information within information, such as hiding images inside images or messages inside messages. Content streaming uses HTTPS to encrypt the connection regardless of the content streamed. Printing RFID inside 3D objects is a viable option but not all printing technologies support RFID insertion, as it requires special material and print heads.

### 2.5.3 Creating provenance measures by applying security principles

Provenance as a term describes the history of a thing. Provenance in 3D printing or additive manufacturing refers to the collective history of actions that the 3D object or 3D print was involved in this is important as it can help associate value and maintain intellectual property rights.

Provenance of digital objects is addressed using different information technologies; attempts in the commercial sector and academic circles regarding ownership are complex and can be considered from two levels.

**View and examine but not own**: The users have the right to print the object but not own it, and the object can be viewed remotely via secure streaming like the attempt describe by Engel and Sommer (1999).

Currently it is unknown if this method would be widely adopted because of similar cases where Amazon deleted content from users' Kindles, claiming the users only had the right to rent but not own the content Belanger (2011).

**Own the object but not in its original form or visual resolution**: The second approach is to allow users to possess the object, but in order to secure it a watermark or similar feature must be incorporated Ohbuchi et al. (2001).

The watermarking procedure removes, modifies, or changes a part of the object, and therefore can infringe on the objects purpose or quality. The Berne Convention for the

protection of literary and artistic works (WIPO)[4] states the copying procedure of artistic and literary works must be *'...substantially copied...'* to infringe its copyrights. This definition is somewhat different from the protection a patent or the implementation of a trade secret that can be invoked in the case of manufacturing. As a result, if forgers or illegal copyholders of 3D objects watermark an object and remove part of it, the claim of ownership from the original author will be harder to prove because a substantial copying must occur and removing part of the object will only make it harder. It can be concluded that watermarking of a 3D object by the holder or creator of the original is its intended purpose, which is to provide intellectual copyright, but in reality the resulting object ceases to be a replica if the watermarking substantially affects the quality or form of the copy. The focus of this research is to investigate the provenance of 3D objects without alteration of the physical geometry, by adding a signature to the 3D copy of an object, instead of subtracting or changing the information of a copy as is the case with watermarking.

## 2.6 Research Gap

After additive manufacturing, the object constructed is often referred to as a prototype or replica, and often that is the case. However, due to public attention and demand for customised 3D printed products such as prosthetics or artistic designs of household objects and jewellery, 3D printed objects can also be referred to as genuine 3D objects with a native digital state. The issue of intellectual copyright for protecting 3D prints created by 3D printers is that private owners of 3D printers are broadly exempt from the majority of intellectual property constraints when making 3D objects, so that private owners can claim it is for non-personal profit, when in some cases they are profiting from it. Commercial usage is also not very restricted according to Bradshaw et al. (2010) for legislation in the UK and Weinberg (2010) for legislation in the US. A number of technologies promote Intellectual copyright property for Digital Rights Management (DRM) of 3D objects such as content streaming using HTTPS, used on the Michelangelo project (Koller and Levoy, 2005), and digital watermarking, as illustrated in the survey by Alface and Macq (2007). Another method is InfraStructs by Microsoft research using secure hardware RFID or steganography by hollow binary insertions (Willis and Wilson, 2013).

**The Research Gap identified** Private owners of 3D printers are broadly exempt from the majority of intellectual property constraints when making 3D objects. There is currently no mechanism for establishing the provenance for 3D printed objects. There are no technical solutions to transfer digital provenance information into physical objects. There is a need for secure technical processes for the transfer of provenance of 3D objects

[4] Berne Convention for the Protection of Literary and Artistic Works, WIPO (http://www.wipo.int)

from a digital to a physical state and back again. Figure 2.9 is an illustration of the gap. The following observations can be extrapolated from the research gap.

- Hesitation and fear of additive manufacturing as a disruptive technology is due to file sharing restrictions and economic impact, Bradshaw et al. (2010) for the UK and Weinberg (2010) for the US
- Physical preservation is preferable (Abel et al., 2011).
- Genuine digital creations in the form of 3D objects have monetary value (Thompson, 2012)
- There is currently no means of tracking changes of digital identity of a 3D printed object. This is not to be confused with RFID as it is used to track objects not changes.

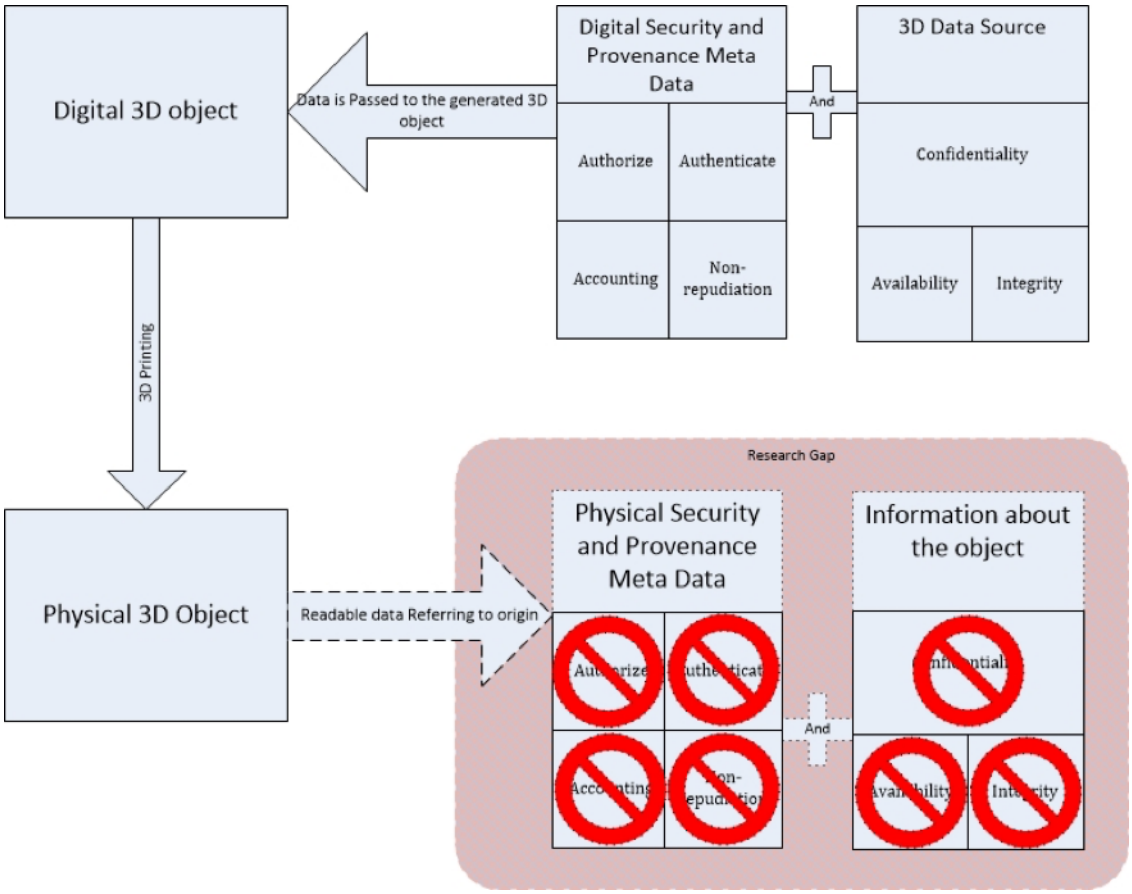



Figure 2.9: Identified Research Gap

This is shown in Figure 2.9 that shows the life cycle of a 3D object from its inception in digital form to physical production using 3D printers. As shown, there is a gap in the transition of the security attributes from digital to physical form.

## 2.7 Summary

This chapter examined 3D digitisation from various data sources, a process that has several components. These are the data source, data creation method, and data file types for recording the object that have varied attribute support. The result of the digitisation process is a 3D object that has geometrical measurements, texture surface, colour and sometimes material as well. After the 3D object has been recorded and digitised it needs some metadata to describe the object, such as purpose, author, location, etc. The acquired 3D object has many purposes: educational, entertainment, or just digital preservation. Some of these 3D objects can be made into physical objects using 3D printers that can make these objects from a number of materials such as ABS, PLA, ceramics, and metals, depending on the additive manufacturing technology. This chapter explored the main additive manufacturing types with examples of each method. 3D printers are available in different sizes and shapes and can vary from 200 to 20000 or more, depending on the type and the quality of the generated object. In July 2012, an entry-level 3D printer which required self-assembly cost around 300-400 (Berman, 2011). In 2017 the price has dropped to 200 for entry-level 3D printers, and prices are expected to drop further as commercial retailers are starting to take an interest in this technology (Snyder, 2014).

Security procedures used to protect intellectual property were discussed. The principles consist of a set of properties (Accounting, Authentication, Authorization, Availability, Confidentiality Integrity, Non-repudiation) and these properties are benchmark points for any security system. For example, the property of authentication does not provide security, but a strong authentication protocol does, and likewise for the rest of the properties. Last to be addressed was the additive manufacturing implication from a legal perspective.

# Chapter 3

# Relevant research

*The purpose of this work is to investigate the transfer or transition of 3D object provenance from the digital state to the physical one, where its claim of identity is proven after 3D printing.* This chapter discusses relevant cyber security methods applicable to additive manufacturing. Intellectual property is associated with digital objects such as mp3 audio, e-books and digital photos. Intellectual property is important because it links objects to their original authors. 3D objects fall under the same intellectual property rights (Bradshaw et al., 2010). Unfortunately, digital media content has been a target for piracy and counterfeiting, which is rampant on the web. This resulted in the Stop Online Piracy Act (SOPA) (Smith, 2011) and the Digital Millennium Copyright Act (DMCA) (Congress, 1998).

The intellectual property requirements for 3D objects are somewhat different from music or films, because in the latter the consumer receives a digital experience. The 3D object consumer receives a physical experience that adds to the original object's intellectual value. Currently most 3D objects are scientific, mechanical, or artistic, aimed at special audiences. Unfortunately, fears of piracy and counterfeiting has made authors of 3D objects wary because of deep concerns for the provenance of data sets they create or acquire, and will not give access to the data unless the work is published or permission is given to specific individuals (Andrew Moir, Anthony Dempster, Rachel Montagnon and Woods, 2016).

Intellectual property can be associated with a digital object as long as it has some means of identification and tracking. However, the majority of 3D file formats do not support metadata. At the time of writing only the AMF and 3MF formats/standards have this ability, but have not been popularly adopted so far. Even if their popularity increases, the use of the metadata space is not fully utilised and does not adequately provide a means of provenance. Therefore, there is a gap between the information generated by 3D objects and information derived from 3D prints. The digital identity is not carried forward once the object is 3D printed, as it stops being digital.

This chapter will compare a selection of 3D file formats that are 3D printing ready and metadata available for 3D objects that are printable using 3D printers. This will enable an understanding of what can and cannot be achieved using the metadata space. Also examined are security methods that provide provenance for 3D objects. Lastly, cyber security methods applied to 3D digital media are compared.

## 3.1 Evaluation of cyber security methods for securing 3D objects

The four methods for protecting 3D content which are HTTPS content streaming, digital watermarking, RFIDs and steganography. They are designed to address a specific threat but not all security threats. No framework exists for protecting 3D objects after fabrication. Some methods cover more security principles than others, as defined by the market, but are still lacking in overall design to accommodate the security principles. These four methods illustrated in Figure 3.1, Figure 3.2, Figure 3.3, and Figure 3.4, describe the process that each method uses to fulfil their intended purpose in providing cyber security. The methods are evaluated using the following criteria.

1. A clear definition of the cyber security methods used in one form or another to protect 3D objects and the information flow for the method.
2. Capturing the process in a flow chart diagram describing start/end, inputs/outputs, processes and decisions.
3. Applicability of the seven security principles using the definitions and flowcharts.
4. Rationale for applicability of the security method to the security properties.

### 3.1.1 Content Streaming

3D objects can be streamed securely using secure protocols such as HTTPS without downloading any files. The 3D object stream can be only viewed (Koller and Levoy, 2005) without any permission for manipulation. Some companies propose content streaming as a new solution for 3D printing as the content is streamed directly to the 3D printer without the user downloading a copy. This method allows the user to have a 3D printed copy but not own the digital file. For example, a user commissions an artist to produce a sculpture; although the user can print a copy, the user cannot download the original 3D data file commissioned. Thus this technology allows for licensing content but not ownership. In summary, content streaming allows for end-to-end secure transmission of the 3D content only.

Table 3.1: Content streaming fulfilling security properties

| **Security Principle 1: Information Security** | | |
|---|---|---|
| **Properties** | **Applicable** | **Rationale** |
| Confidentiality | No | Secure streaming does not secure the content locally but only protects it point-to point (Koller & Levoy, 2005). |
| Integrity | No | |
| Availability | No | |
| **Security Principle 2: Information Authenticity** | | |
| Authentication | Yes | Fulfils the authentication property because it is part of the information exchange. However, digital integrity and Non-repudiation is not fulfilled as secure streaming does not have the functionality to provide them. |
| Integrity | No | |
| Non-repudiation | No | |
| **Security Principle 3: Information Exchange** | | |
| Authentication | Yes | Secure streaming secures the content by encapsulating it in an HTTPS header to protects it point to point (Koller & Levoy, 2005). |
| Authorization | Yes | |
| Accounting | Yes | |

Table 3.1 lists the security properties covered by content streaming compared against the three security principles: Information security, Information authenticity, and Information exchange. The figure shows that streaming only fulfils only one security principle, that of *Information Exchange*.

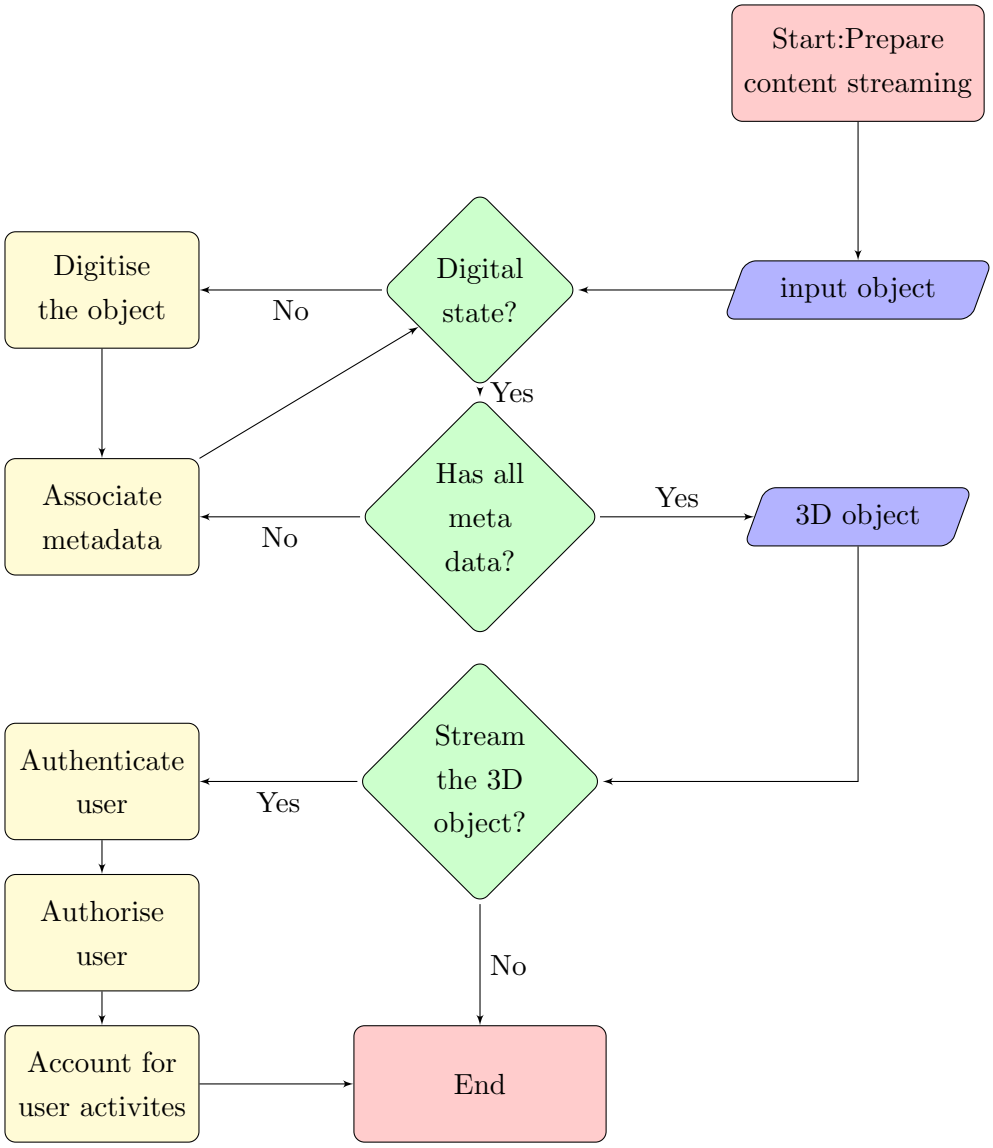



Figure 3.1: Content streaming method

Figure 3.1 illustrates the process. Three actions are taken to certify the user who wishes to stream the content: Authenticate user to validate the claim of identity, Audit user to know who wants to see it, and Authorise user if the user is allowed.

### 3.1.2 Digital Watermarking

Digital watermarking (or simply watermarking) is the process of adding or embedding information into a digital medium to prove its origin and protect the intellectual property. Watermarking is a provenance measure that is similar to a signature, but the difference is that signing is adding additional information to the object, while watermarking subtracts a part of the object, alters it and places it back with the modification. This results

in an altered version that is different from the original. Watermarking is a method where a part of the digital data is altered to embed data containing information about the author of the object proving intellectual property claims (Lin et al., 2008). An alteration is such as changing the least significant bit in a digital image (Lie and Chang, 1999).

Table 3.2: Digital watermarking fulfilling security properties

| **Security Principle 1: Information Security** | | |
|---|---|---|
| **Properties** | **Applicable** | **Rationale** |
| Confidentiality | No | Digital watermarking is a measure to protect intellectual property. Content that is not meant to be confidential like music and films and its availability is a condition, i.e. if you pay for it. |
| Integrity | Yes | |
| Availability | No | |
| **Security Principle 2: Information Authenticity** | | |
| Authentication | Yes | Watermarking is used primarily to protect intellectual property where an author can prove non-repudiation, the authenticity and complete integrity fulfilled as well (Garg et al., 2012) |
| Integrity | Yes | |
| Non-repudiation | Yes | |
| **Security Principle 3: Information Exchange** | | |
| Authentication | Yes | Watermarking is not a method that is used to exchange digital objects but only to prove ownership. Therefore, it cannot account for who can access it and what they do with it. |
| Authorization | No | |
| Accounting | No | |

Table 3.2 lists the security properties covered by digital watermarking and Figure 3.2 illustrates the process. This process only guarantees the authenticity of the digital content and does not extend to physical objects. It cannot be used to secure confidential information but only disclosed information. It also cannot be used to share the information, as it has no control over who to grant access to.

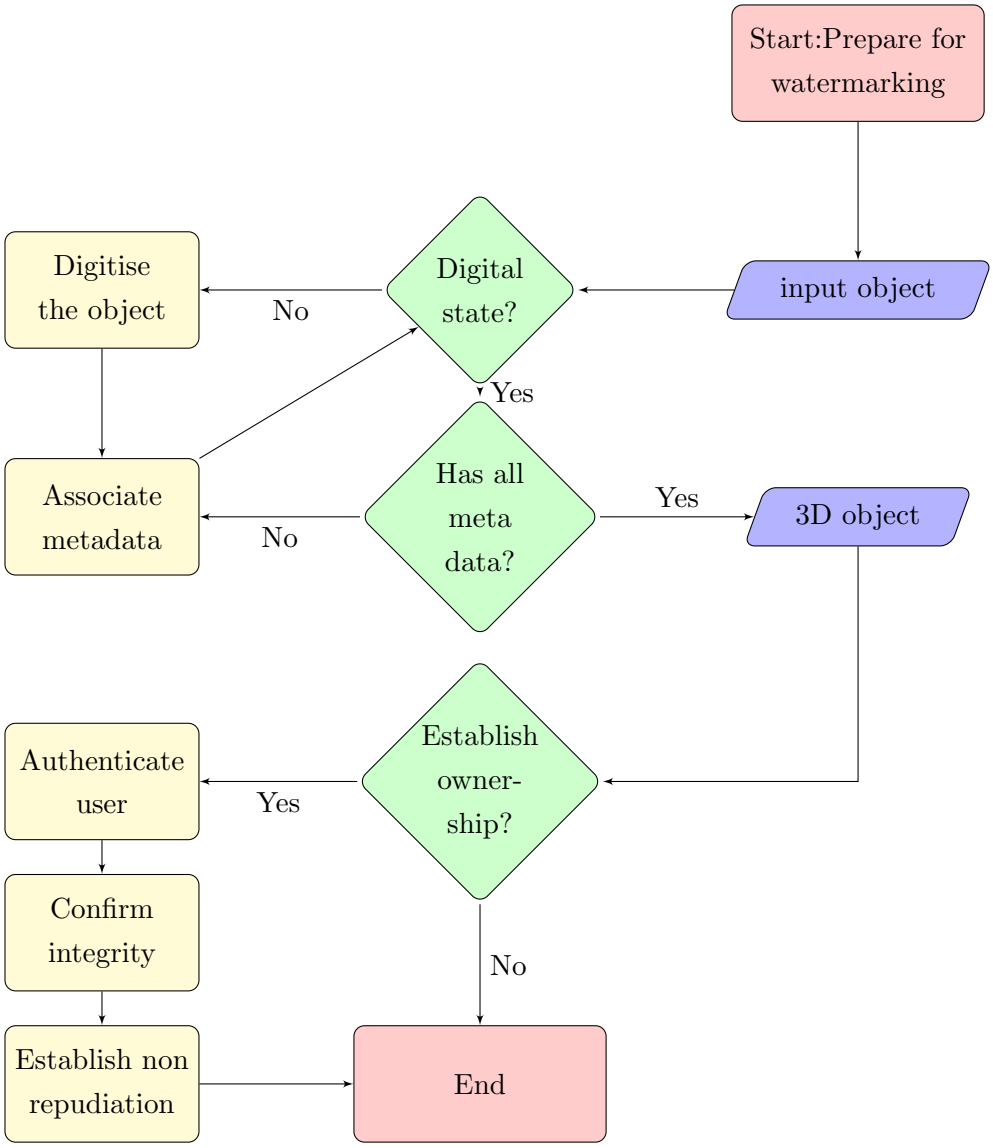



Figure 3.2: Watermarking process

Figure 3.2 illustrates the process. Three actions are taken to certify the user who wishes to watermark the content: Authenticate user to validate the claim of identity, Confirm integrity, and Confirm user identity with a third party to establish non-repudiation.

### 3.1.3 Steganography

Steganography is the art of hiding information in ways that prevent the detection of hidden messages. Steganography, derived from Greek, literally means covered writing. It includes a vast array of secret communication methods that conceal the message's very existence. (Johnson and Jajodia, 1998)

This is the most common definition for steganography, mostly used in textbooks and research papers. Current techniques for cryptanalysis can prove with acceptable accuracy that the cover medium has been exposed to manipulation, and by cover medium is meant the data carrier for the hidden message (Abolghasemi et al., 2008), (Hawi et al., 2004), (Ru et al., 2005), (Zhi-ping et al., 2007), (Zhi-ping et al., 2007). Steganography can also be used for digital linkage and storage, achieved by embedding information into digital media. For example, information such as personal or medical records can be inserted into a personal image or photo.

Table 3.3: Steganography fulfilling security properties

| **Security Principle 1: Information Security** | | |
|---|---|---|
| **Properties** | **Applicable** | **Rationale** |
| Confidentiality | Yes | Steganography is meant to hide information inside digital media and keep them confidential, so integrity must be maintained to carry the hidden message as well as making it available when required. |
| Integrity | Yes | |
| Availability | Yes | |
| **Security Principle 2: Information Authenticity** | | |
| Authentication | No | Although steganography addresses the integrity of the information, it does not have any mechanism for authentication or non-repudiation. |
| Integrity | Yes | |
| Non-repudiation | No | |
| **Security Principle 3: Information Exchange** | | |
| Authentication | No | Steganography cannot provide any additional information with the confidential information stored. Therefore it cannot satisfy any of them. |
| Authorization | No | |
| Accounting | No | |

Table 3.3 lists security properties covered by steganography and Figure 3.3 illustrates the process. A process which guarantees the security of the digital content and has the potential to extend to physical objects, it cannot be used to verify information authenticity. It cannot be used to share the information, as it has no control over who to grant access to the information.

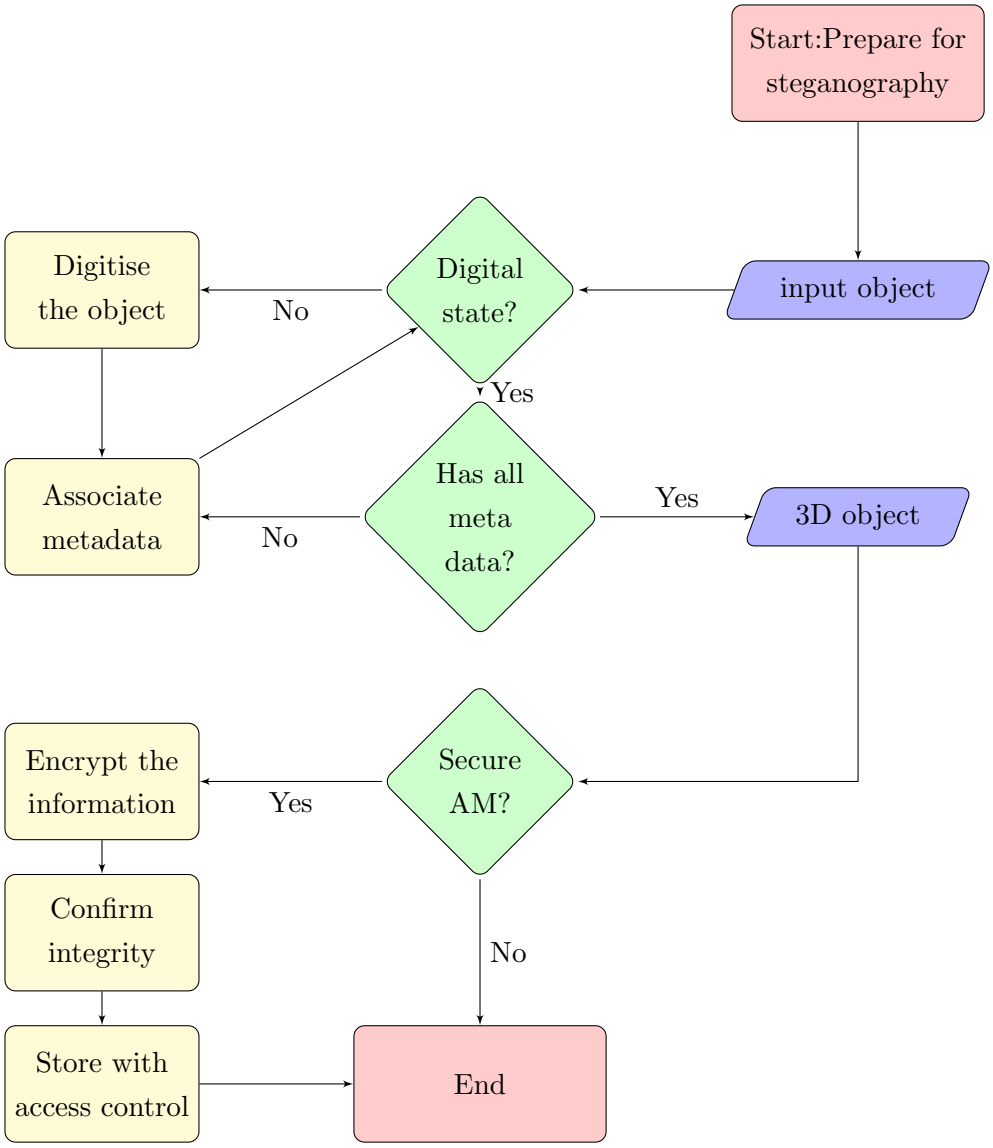



Figure 3.3: Steganography process

Figure 3.3 illustrates the process. No actions are taken to certify the user when steganography is added to the content.

### 3.1.4 Radio Frequency Identification (RFID) Secure hardware

3D printing is capable of fabricating RFIDs and other tagging methods. As shown in Sangoi and Smith (2005), RFID tags can be printed inside 3D objects and use frequency-domain spectroscopy. Another method uses terahertz for sensing infrastructure tags to embed information into fabricated objects (Willis and Wilson, 2013). This approach is innovative; however, it is not universal and not suitable for all available 3D printing

technology, and does not identify what kind of information is needed to establish provenance. The technology is moving towards incorporating secure hardware as a security measure for 3D printing.

Currently two types of security chip are available for 3D printers. The first is a security chip for the material refills to ensure the end user buys their material cartridges, which is common with proprietary ink cartridges for colour printers. The second type is designed check for copyright infringement of that 3D design, such as patent filed (Reid and Merkley, 2015), which uses the hardware to check if the 3D design was authorised to print, in a similar way to DVD players not playing pirated content.

Table 3.4: RFID fulfilled security properties

| **Security Principle 1: Information Security** | | |
|---|---|---|
| **Properties** | **Applicable** | **Rationale** |
| | | |
| Confidentiality | Yes | RFID is primarily used as a means of tracking and identifying goods but it is also classified as secure hardware (ISO, 1984). RFID is used in an ID card to protect confidential information or areas. |
| Integrity | Yes | |
| Availability | Yes | |
| **Security Principle 2: Information Authenticity** | | |
| Authentication | Yes | RFID hardware is meant to store data to establish information authenticity. RFID is a string of characters containing a unique number that acts as a reference for digital records that the RFID is attached to. |
| Integrity | Yes | |
| Non-repudiation | Yes | |
| **Security Principle 3: Information Exchange** | | |
| Authentication | Yes | RFID is secure hardware and is not meant for information exchange. |
| Authorization | No | |
| Accounting | No | |

Table 3.4 lists security properties covered by secure RFID hardware and Figure 3.4 illustrates the process. A process which guarantees the security of 3D printed objects, it can be used to verify information authenticity. It cannot be used to share the information, as it has no control over who to grant access to the information.

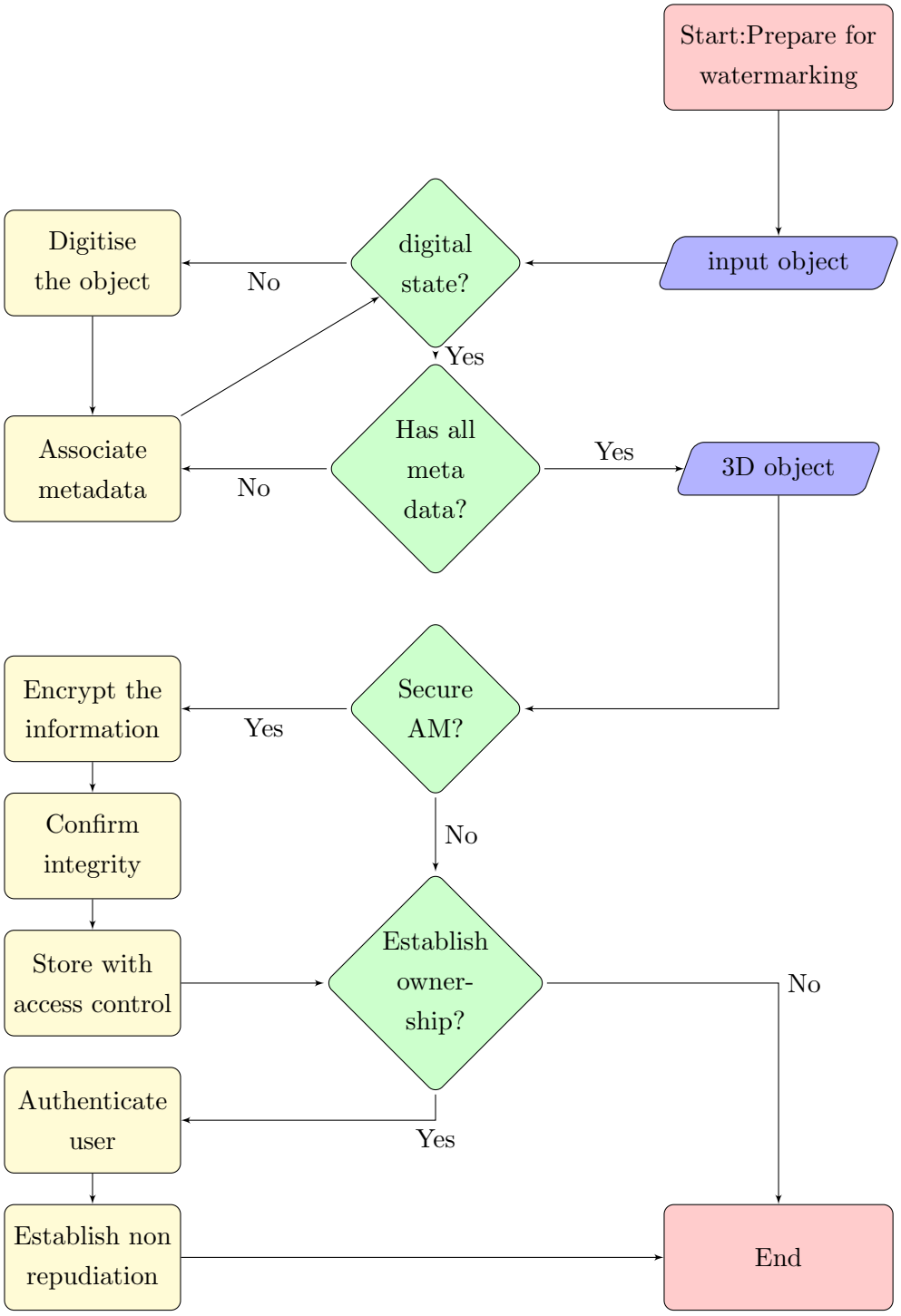



Figure 3.4: RFID secure hardware process

## 3.2 Comparison of cyber security methods

The methods discussed up so far all contribute to the protection of additive manufacturing goods. Table 3.5 is a comparison between these security methods for 3D objects.

There are seven security properties that are the basis for digital security, digital signing and secure digital transmission. This table shows security properties addressed by each individual technology and their shortcomings.

Table 3.5: Security method comparison

| **Cyber Security Method And Associated Properties** | **Content Streaming** | **Digital Watermarking** | **RFIDs** | **Steganography** |
|---|---|---|---|---|
| Accounting | Yes | No | No | No |
| Authentication | Yes | Yes | Yes | No |
| Authorization | Yes | No | No | No |
| Availability | No | No | Yes | Yes |
| Confidentiality | No | No | Yes | Yes |
| Integrity | No | Yes | Yes | Yes |
| Non-repudiation | No | Yes | Yes | No |
| Score | 3/7 | 3/7 | 5/7 | 3/7 |

Yes indicates that the method contributes to a property, and No for a property that it cannot cover. This comparison is hypothetical using ideal implementation to show if the method could potentially cover a property. The properties were then scored based on coverage.

In Table 3.5 a scale of one to seven was used to represent the overall coverage by the security methods of the security properties. For example, the RFID method covers 5/7 but cannot be used for sharing; streaming content only works for digital objects and does not permit ownership; watermarking works for digital objects but it is inapplicable for 3D printed objects. Steganography and watermarking use the same cryptographic techniques but the difference between them is whether the security is aimed at the object or the message. Watermarking is used to protect the 3D object itself, while steganography uses the 3D object to protect information and the 3D object is just a carrier.

In Table 3.6, the RFID scored the highest cover with two out of three principles for 3D objects. However, none of the methods covers all three security principles. The result is that no security solution can fit all, since there are different threat and response scenarios.

Table 3.6: Cyber security principles comparison table

| **Cyber Security Method And Security Principles** | **Content Streaming** | **Digital Watermarking** | **RFIDs** | **Steganography** |
|---|---|---|---|---|
| Security Principle 1: Information Security | No | No | Yes | Yes |
| Security Principle 2: Information Authenticity | No | Yes | Yes | No |
| Security Principle 3: Information Exchange | Yes | No | No | No |

However, there is no baseline security measurement for protecting and exchanging 3D content.

## 3.3 Comparison of 3D printer file formats

Architects, artists, engineers and game developers produce 3D designs as their intellectual property. Artists and graphic artists purposefully produce objects as genuine pieces of art to be appreciated and enjoyed (Scopigno et al., 2011), (Walters et al., 2009). A digital copy is either acquired through digital capture devices or produced by a user. These produced objects are frequently used to illustrate and share 3D designs or ideas, for example, the digitisation of museum sculptures (Celani et al., 2009). This geometrical description of an object needs some means of storage so it can be used later with 3D printing. Therefore, 3D printers usually use the STL file format; OBJ file format also works after conversion to STL. The same is true for other file formats for 3D objects. PLY is mostly used in scanning, while AMF is still an experimental file format for 3D printing, and 3MF is a new file format published in late 2015.

Table 3.7: File Format Feature Comparison

| **Properties** | **OBJ** | **PLY** | **STL** | **AMF** | **3MF** |
|---|---|---|---|---|---|
| Geometry Specification | Yes | Yes | Yes | Yes | Yes |
| Material Specification | No | Yes | Yes | Yes | Yes |
| Color Specification | Yes | Yes | Yes | Yes | Yes |
| Texture Specification | Yes | Yes | Yes | Yes | Yes |
| Print Constellations | No | No | Yes | Yes | Yes |
| Metadata | No | Yes | Yes | Yes | Yes |
| Compression and Distribution | No | Yes | Yes | Yes | Yes |
| Tolerances, Surface Roughness | No | No | No | Yes | Yes |
| Additional Information | No | No | No | Yes | Yes |
| Printer setting | No | No | No | No | Yes |

Table 3.7 compares the features for most supported file formats. Two very promising file formats are AMF and 3MF and both are suitable for this research. Provenance can be added to 3D objects by using the metadata space.

**AMF**: AMF is sometimes referred to STL 2.0 (Hil, 2009) which is an STL file with extra functionality which was added to accommodate future needs for 3D printing. The AMF XML descriptor in Figure 3.5 has five top-level elements: Object, Texture, Material, Constellation and Metadata. These are defined in the Standard Specification for Additive Manufacturing File Format.

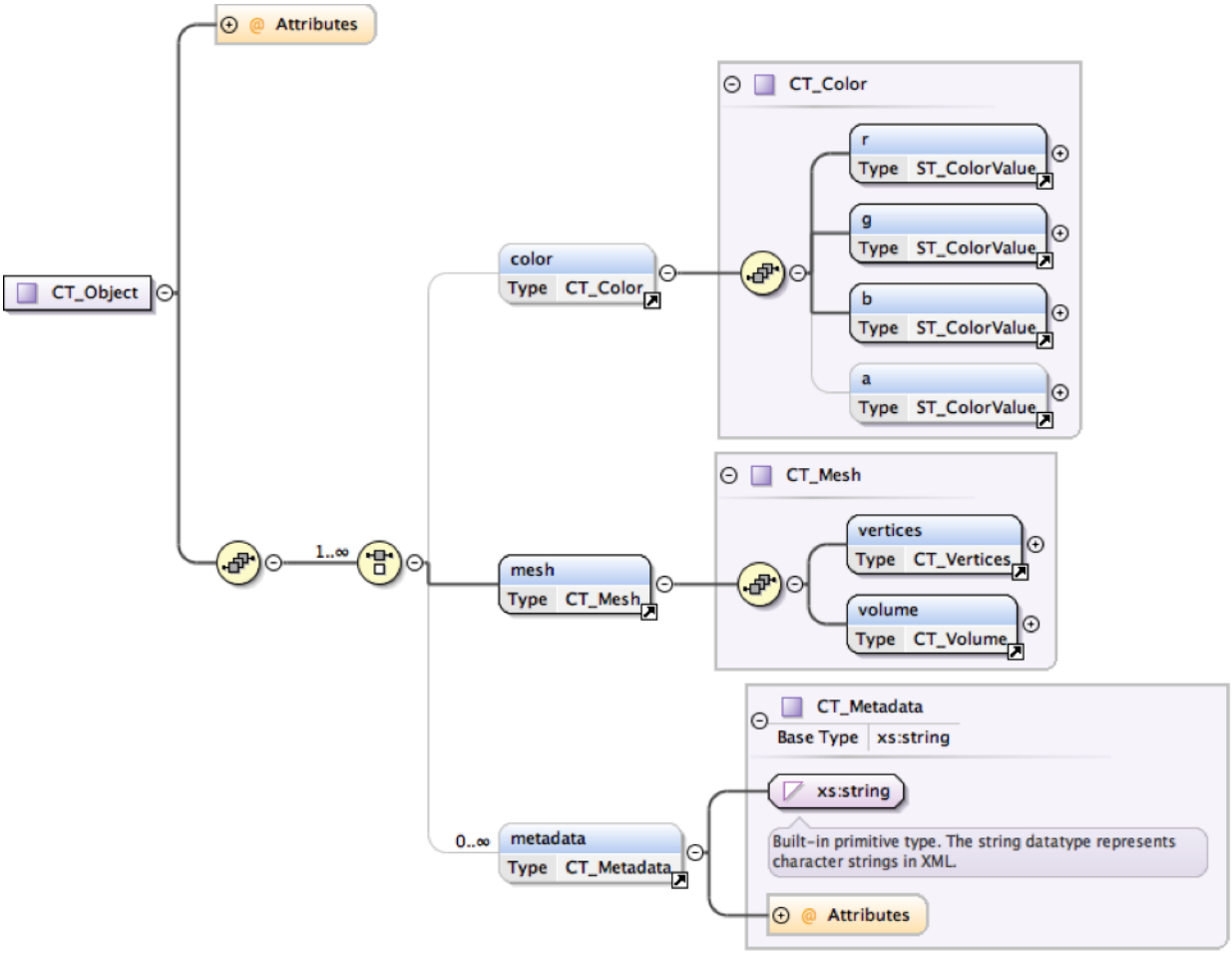



Figure 3.5: AMF XML object map including the metadata space

Figure 3.5 illustrates the XML descriptors hierarchy used to create 3D objects including geometry, surface texture, colour and material. The full descriptor definition is discussed in 52915 (2013). Below is an outline of the top 5 elements.

**Object** : Defines object geometry using vertices and edges and volume using triangles.

**Texture** : Optional element defines images on surfaces or colours.

**Material** : Optional element defines the material for 3D printing.

**Constellation** : Optional element that can hierarchically merge objects and other constellations into a pattern for 3D printing.

**Metadata** : Optional element specifies additional information about the object(s) and elements contained in the AMF file.

**3MF**: The 3MF file format has similar components but a different structure as illustrated in Figure 3.6. It adds two important features, digital signing and printer setting.

Adding digital signing is the first step to establish traceable, transferable provenance between physical and digital states. It utilises the metadata space more efficiently as it is specifically designed for additive manufacturing (Consortium, 2015).

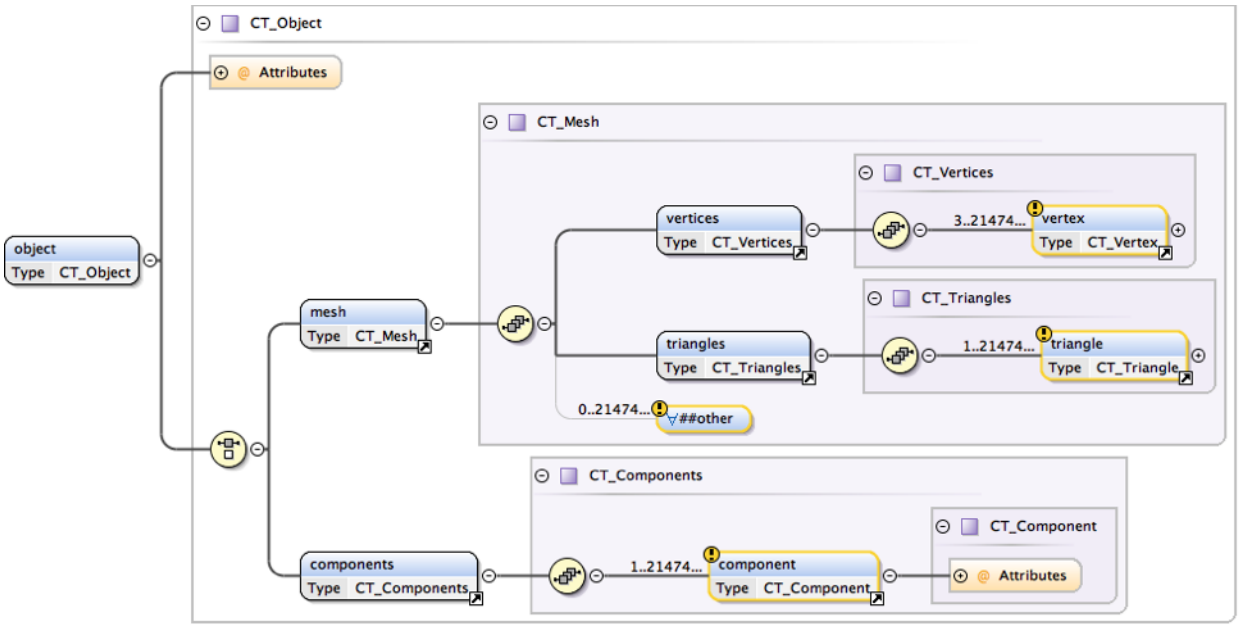



Figure 3.6: 3MF XML object map including the metadata space

**3D Model** : Contains the geometrical description of 3D objects for additive manufacturing. It may contain the geometry of several objects.

**Core Properties** : The open packaging convention part of 3MF that encapsulates various document properties.

**Digital Signature** : The open packaging convention part of 3MF that contains a digital signature.

**Digital Signature Origin** : The open packaging convention that contains the root of digital signatures.

**Digital Signature Certificate** : The open packaging convention part of 3MF that contains a certificate for the digital signature.

**Print Ticket** : Provides 3D printing settings to be used when printing the 3D object(s).

**Thumbnail** : Contains a small image of the 3D objects.

**3D Texture** : Contains a file used to apply complex information to a 3D object in the 3D model part of 3MF (used for object thumbnails and available for extensions).

## 3.4 Principles and properties building blocks

A literature review of 3D objects and additive manufacturing was conducted in chapter 2, including a review of relevant security solutions to 3D, and to identify the research gap in the provenance in additive manufacturing in section 2.6. This work identified the building blocks used by the cyber security methods that were designed to satisfy specific cyber security properties. This work then used these building blocks to lay the ground for establishing provenance in additive manufacturing.

The combined principles - Information security, Information transmission, Information authenticity described in section 2.5 will provide the building blocks for a transition framework of security properties from 3D objects to 3D printed objects for information securing/sharing/owning 3D objects using 3D printing technologies.

Combined, these principles have seven properties between them: Accounting, Authentication, Authorisation, Availability, Confidentiality Integrity, Non-repudiation. Figure 3.7 shows the principles, properties and how they relate to each other.

**Provenance** is at the core of Figure 3.7 to show that the combination of the security principle provide provenance information for additive manufacturing.

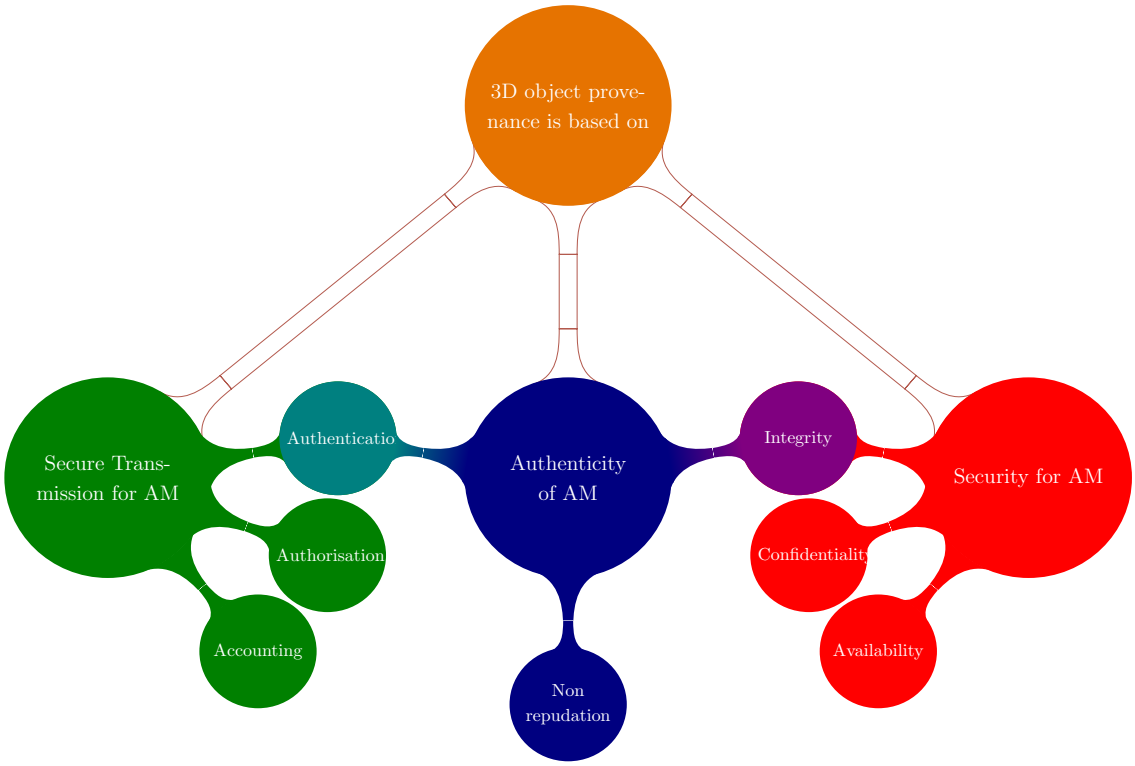



Figure 3.7: Overview of provenance showing the cyber security building blocks

Figure 3.7 shows that authentication mediates between Securing AM transmission and Authenticity of AM. Integrity also mediates between Authenticity of AM and Security for AM.

These principles and properties, with the provenance definition earlier in 2.5, are placed in the context of establishing provenance for cyber/physical objects as in additive manufacturing. The provenance building blocks in summary will be:

**Information security** is used to determine the origin or history of a thing, how long the thing existed. Information security is a term used for securing information from being leaked that could be stored inside a physical safe, cloud storage, network storage or on private work stations. Therefore, the digital requirements are:

**Confidentiality** measures used to keep the object safe.

**Integrity** procedures to check for integrity of the objects.

**Availability** the object availability and mirrored data sources.

**Information transmission** is used to determine the history of a thing or were it was, and who used it. Information transmission is a term used for securing information from point(s) to point(s) within connected parties and make sure that the information is secure while in transit. Therefore, the digital requirements are:

**Authentication** to find out who is involved and how he/she is authenticated.

**Authorisation** to find out what he/she was authorised to do.

**Accounting** for all activities that have happened while handling the thing.

**Information authenticity** to prove ownership records reflect a thing's authenticity . Information authenticity is a term usually associated with digital signing of document, emails and even artwork. Therefore, the digital requirements are:

**Authentication** to determine who is involved and how he/she is authenticated.

**Integrity** procedures to check for integrity of the objects.

**Non-repudiation** to make sure without a doubt that the object or action on the object was a result of someone's actions.

## 3.5 Relationships between properties

The first type of relationship for the properties (confidentiality, integrity and availability) refers to the object security, wherever it is stored.

- Confidentiality (Object) refers to the state of information disclosure between authorised parties, Party A and Party B.

- Integrity (Object) refers to the information integrity (Completeness), and error correcting, and recovery abilities while it is in the possession of Party A or Party B.
- Availability (Object) refers to an object or a lost object that was described in other records, that is made available when needed, Party A to Party B.

The second type of relationship for the properties (authentication, authorisation and accounting) according to (Burrows et al., 1989; Wang, 2005) must have the parties involved (Sender A, Receiver B) as well as an impartial third party (Trusted third party C).

- Authenticate (Owner of A and Owner of B using C): proving a claim of identity associated with granting or denying rights of access to 3D objects or its metadata.
- Authorise (Owner of A and Owner of B using C): level of access to an object or its related metadata.
- Accounting (Owner of A and Owner of B using C): audit actions that have been performed on an object to access or modify the object or its metadata.

The third type of relationship for the properties (authentication, integrity and non-repudiation) refers to the object intellectual property when bought, sold or freely given.

- Authenticate (Owner of A and Owner of B using C): proving a claim of identity associated with granting or denying rights of access to 3D objects or its metadata.
- Integrity (Object) refers to the information integrity (Completeness), and error correcting, and recovery abilities.
- Non-repudiation (Owner of A or Owner of B using C): un-deniability of any action including designing 3D parts or objects.

## 3.6 The framework data flow and data classes

The state of an object can change from a digital state to physical via 3D printing, and printed objects can be digitised again using any 3D scanning device. A digital object can be referred to by a digital object identifier, and a physical object by a physical object identifier. DOI can capture the identity of a 3D object as a first class identity. However, a 3DOI is meant to capture all provenance information regarding the object's second and third class information such as file location and the previous owner's history.

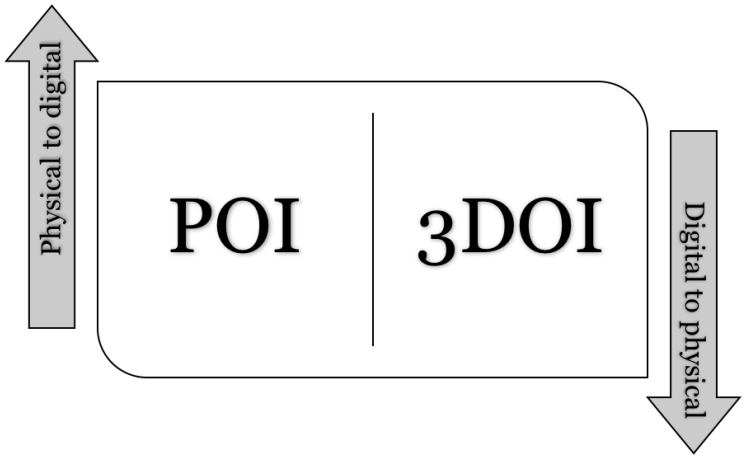



Figure 3.8: Relationship between physical and digital identities

Additive manufacturing as a process is defined as the relationship between digital and physical identity of a design, Figure 3.8 is a simplified figure of the transition process.

**First Class** : 3D object information is the 3D object itself

**Second Class** : is information about the 3D object's relationships, such as where it is stored and who has access to it.

**Third Class** : is information that could be extrapolated from data that already exists, for example threat severity to a 3D object.

An entire dataset can be referred to by a single digital identity. This issue was investigated by Birnholtz (2006) addressing scholarly publications and identity of data sets, before digital publishing, and it was noted that accreditation and citation of academic work has a number of purposes that by definition cover 3D objects as well if the 3D objects are in sets.

- Acknowledging credit for contribution of knowledge of a person or people.
- Associating the discovery with the discoverer.
- Building academic reputation for contribution in the field of study.

## 3.7 Discussion

Securing intellectual property of the 3D object can currently be achieved in three ways. First, using the law of patent or trademark, as explained in Bradshaw et al. (2010). The second method uses watermarking or encryption of 3D models as a measure for proving

ownership and integrity. The third method requires physically attaching a security device, such as an RFID (Simske, 2011).

Security requirements undergo continual evolution to cope with counter-measures designed to circumvent current security policies. The same holds for 3D printing, since the security domain expands as new areas emerge, and new security measures develop to protect it. For example, the case of the Michelangelo project (Koller and Levoy, 2005) in digital humanities, described a secure method to make the digital capture available for study using software called ScanView and the system used client-server architecture, which is considered as a first attempt for securing 3D content remotely encrypted across the http protocol. This case illustrates the importance of security for digital designs and intellectual property because high resolution digital capture can be a target for piracy attempts.

The current work investigates providing provenance for 3D printed objects as an enabling technology. The existing state of technology does not compensate for the threat level to 3D objects because 3D printing technology is growing faster than the security policies surrounding it. One of the objectives of this work is to add value to artefact exchange by introducing a digital-physical provenance scheme through a framework, which will add to the current processes of data preservation and exchange. The research aim was not to construct a certification authority but to provide a framework that a certificate authority could operate under. However, this is future work beyond the current scope (Appendix B).

The seven security properties (Accounting, Authentication, Authorisation, Availability, Confidentiality, Integrity and Non-repudiation), will be included in the framework design to provide provenance for 3D printed objects. Exchange of physical objects over digital transmission using digital networks has been illustrated using the Michelangelo project as well as the 3D Fax.

## 3.8 Summary

3D printers fabricate 3D objects, and illegal possession of unlicensed 3D objects is punishable by law - similar to illegal possession of MP3 and E-Books. However, when it comes to proving illegal possession, the law for 3D printed objects is loosely defined and hard to achieve (Bradshaw et al., 2010). For example, a counterfeiter can copy parts of the object without infringing on intellectual copyright as long as no substantial copying has been done. This, in turn, could potentially discourage artists and innovators from sharing their intellectual property as 3D printed objects currently have no track of provenance and cannot be traced. The exchange procedure of 3D digital captures is roughly undefined and current attempts are either remote display such as Koller and Levoy (2005) or mutual trust that an abuse will not occur. This option is not viable

for 3D printing at the moment, and will not pass on any intellectual copyright from the artists or creator to its new owner.

The availability of 3D printers to anyone who can afford them introduced a disruptive effect on intellectual property rights, as with the introduction of affordable video cassette recorders (VCR) (Swix et al., 2003), and the same was true when MP3 and E-Books were introduced, but that did not stop the technology being adopted. MP3 and the E-books are legally treated as objects rather than file formats, where the law punishes illegal possession of the files. In conclusion, there is no unified 3D object file format nor has legislation caught up with additive manufacturing; moreover, there is very little research in protecting 3D objects before or after fabrication.

# Chapter 4

# Research Methods

Setting a solid research plan is a defining quality of good research, and proper understanding of the research problem is the foundation for writing a proper research plan. This chapter will make a list of the research tools needed to design, build and evaluate the additive manufacturing provenance framework. The research problem stated in Chapter 2 is

- Private owners of 3D printers are broadly exempt from the majority of intellectual property constraints when making 3D objects.
- There is currently no mechanism for establishing the provenance for 3D printed objects.
- There are no technical solutions to transfer digital provenance information into physical objects.

The literature review highlighted the cyber security principles involved and additive manufacturing processes that must be a part of the security mechanism. Building on the cyber security principles and additive manufacturing principles a precise and well-outlined research gap is defined as shown in section 2.6. The research gap illustrated in Figure 4.1 shows a disconnect in information flow after the AM process. This figure is similar to Figure 2.9 except it shows the boundary of this research work.

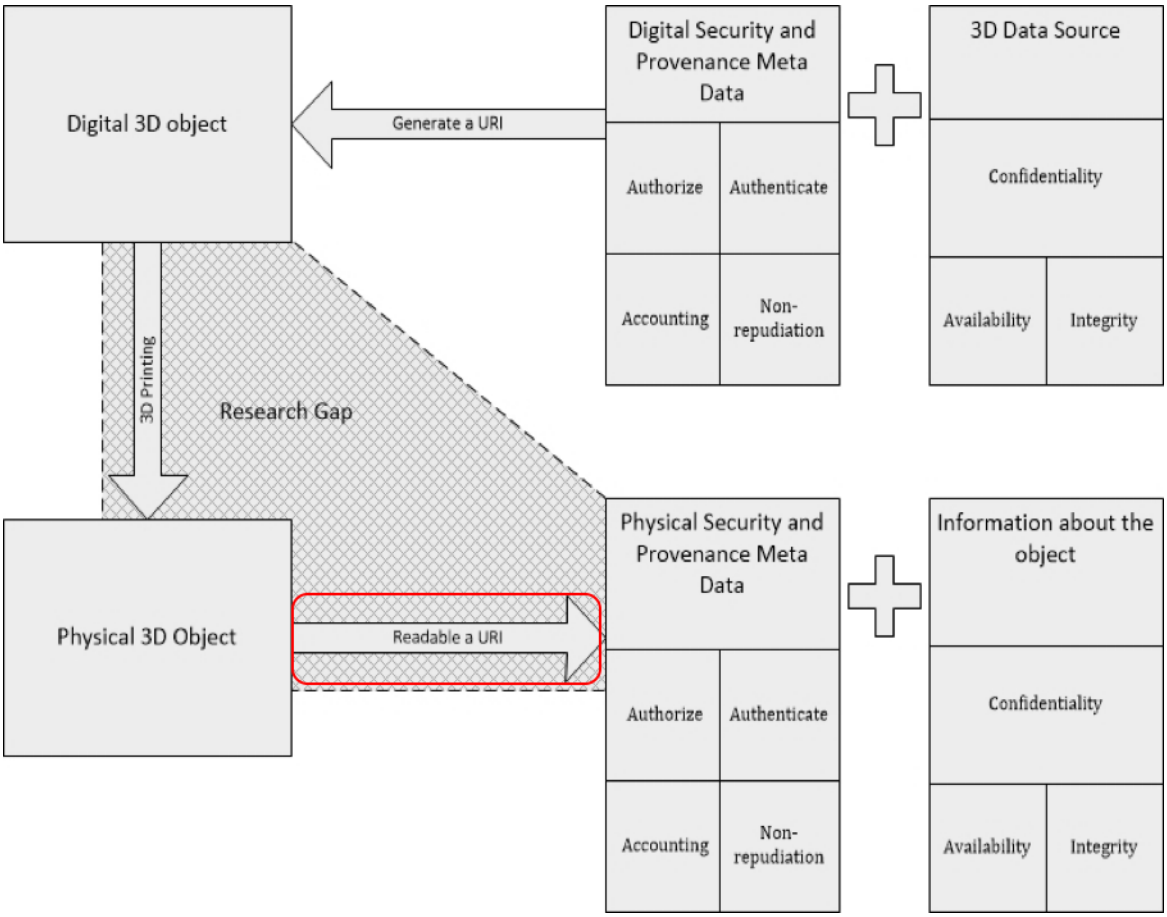



Figure 4.1: Research Gap and area addressed by the framework

These issues are addressed by the concept of 'Provenance', or the origin or how long the thing existed, history of a thing or where it was, who used it, and ownership records to reflect a thing's authenticity Dictionary (2007). The provenance framework for transferring security properties from digital to physical object is based on an investigation of digital security concepts from securing information systems (Software) and information technology (Hardware). From the literature review and the research gap, the most suitable requirement for this conceptual Framework is the following.

- The framework must be capable of providing coverage for the principles of Information transmission, Information security and Information Authenticity.
- The framework needs to cover the seven security properties: Accounting, Authentication, Authorisation, Availability, Confidentiality Integrity, and Non-repudiation.
- The framework must be able to provide coverage for additive manufacturing objects, that is cyber to physical.
- The framework must be customisable to fit different AM infrastructures. Therefore the components must be independent and can be used separately.

- The framework must provide a way of encapsulating the information.

## 4.1 Research Objectives and Research Questions

Research into provenance of 3D objects/3D prints is both new and multidisciplinary. First, the topic falls within computer science because it is a theoretical computer security issue, and at the same time it has aspects of engineering because it addresses the provenance of 3D printed objects using additive manufacturing (3D printing). In addition, the topic has falls within the law discipline because of the issue of provenance and legal implication of using 3D printers and their disruptive influence on personal manufacturing. Therefore, it is important to set clear research objectives that shape the overall research plan.

This section will set objects for the research, suggest research questions and the best research methods to investigate them. The overall objective is to "enable transition of security properties from 3D object (digital state) to 3D print (physical state) using 3D printers". Later sections will discuss research methods used.

**First Research Question** : What is an appropriate reference model for semantically describing additive manufacturing threats within a manufacturing line?

**First Research Objective**: Build a reference model for the digital/physical threats disconnect in the transition of security properties from 3D object (digital state) to 3D print (physical state) using 3D printers.

**Second Research Question** : What components are required for the provenance AM framework properties?

**Second Research Objective**: This work earlier established seven universal properties for security that will be used here as the platform to collect provenance information to prove who did what, where and when, why and how. Therefore, the objective is find a suitable set of components that covers the seven security properties.

**Third Research Question** : What metrics are required to measure the components of the provenance AM framework properties?

**Third Research Objective**: From the confirmed components, appropriate metrics will be proposed to complete the framework. These will be confirmed using expert interviews.

**Research Questions two and three combined provide a confirmed framework for providing provenance for additive manufacturing.**

**Fourth Research Question** : How can the framework be used to provide software requirement specification for the provenance of additive manufacturing?

**Fourth Research Objective**: Validate the research by using the framework to build a software tool to assess the provenance of manufacturing operations.

## 4.2 Research Methods

The following paragraphs describe the research methods used to answer the research questions. Each research question will be answered using the triangulation research method or "Within-Method" Guion et al. (2010), Hartley and Sturm (1997), that refers to collection of information from different data sources to evaluate a research question. Triangulation can uncover different aspects of a research area by extracting subsets of the results by correlating two or three of the triangulation elements Archibald (2016). This work will use different triangulation configurations to investigate the research questions. The research methods that will be used are:

1. Literature Review.
2. Provenance Modelling using PROV-N.
3. Cyber to Physical Security Taxonomy.
4. Threat analysis.
5. Goal Question Metric Approach.
6. Expert Review.
7. Software Requirement validation using prototyping.

### 4.2.1 Provenance Modelling using PROV-N

Provenance modelling is based on a language developed by the W3C working group Groth and Moreau (2013) to establish the provenance in things that are a product of people, processes and objects. The provenance notation (PROV-N) is composed of a series of relationships between agents, activities and entities. Figure 4.1 illustrates the shapes used here in describing the relationships.


Figure 4.2: PROV-Notation

The (Groth and Moreau, 2013) technical report describes all relationships that the PROV language uses to describe the provenance of things. This work uses a subset listed in Table 4.1.

Table 4.1: Provenance relationships subset from PROV-N

| **Relationships** | **Object A** | **With Object B** |
|---|---|---|
| Associated with | Agent | Activity |
| Generated by | Entity | Activity |
| Invalidates | Activity | Entity |
| Uses | Activity | Entity |
| Derived from | Entity | Entity |

### 4.2.2 Cyber to Physical Security Taxonomy

The analysis will use (Yampolskiy et al., 2013) cyber to physical taxonomy to examine the dataset to identify action, cause and effect. This taxonomy describes cyber physical attacks using three groups Table 4.2(action, cause and effect) the relationship between the states being

**Attack** is carried out using a method that needs a set of preconditions for the attack to be successful. For example, the targeted host machine needs to have certain software installed so that a particular vulnerability can be exploited to access confidential data.

**Cause** is the consequence of the attack that causes the service or system to be exploited. For example, the attack on a system caused it to shutdown, therefore resulting in the system becoming unavailable.

**Effect** Is the disruption of a service or system that was dependant on another service or system that was attacked. For example, an electric generator was attacked and resulting in all connected devices having no power.

Table 4.2 will be used to describe the use cases of cyber security threats.

Table 4.2: Cyber Security Taxonomy Yampolskiy et al. (2013)

| Cause | Effect |
|---|---|
| Influenced element | Victim element |
| Influence A,B,C | Impact A,B,C |
| Action | |
| Method | |
| Precondition A,B,C | |

### 4.2.3 Threat Analysis

Similar to 4.2.2, a threat analysis is based on describing the information flow from end to end and, instead of describing all possible threats, the threats will be analysed only on the threatened security property. The threats will only model violations that includes additive manufacturing in their information work flow. The threat analysis will be carried in the following order.

**Describe Scenario** : Describe the scenario where an infringement has already happened or propose a scenario where it could happen. Detailed or generic, depending on the information available.

**Model Threat** : Build the information flow with direction between processes involved and stakeholders or agents involved. If detailed information about the input or output is described in the previous step, then it could be added to the model.

**Identify Weakness** : Annotate the modelled threat with the affected security property in the scenario, such as compromised confidentiality due to espionage or affected availability due to denial of service attack.

### 4.2.4 Goal Question Metric Approach

This method aims to determine mechanisms for measuring software systems, such as software quality, management and security. Studies such as ("software management?") identify several qualities that are associated with good GQM design. The organisation must define specific goals/objectives for itself or the project, and the data needed to answer the set goals/objectives, and the means to interpret the data.

Initially developed for the NASA Goddard Space Flight Center environment to evaluate project defects Caldiera and Rombach (1994), it was mainly employed with use cases but the methodology has been expanded to include various experimental approaches.

The mature measurement model for goal question metric approach has three levels, as illustrated in Figure 4.3

**GOAL (Conceptual Level)** : Build a set of goals from the objects involved applicable to its process, products and resources life cycle.

**QUESTION (Operational Level)** : Build a set of questions to capture the best way to achieve the predefined GOALS.

**METRIC (Quantitative Level)** : Build a set of predefined answers that provides a quantitative response. The response will provide an interpretation that is based on understanding of the context, goal and environment of the organisation.

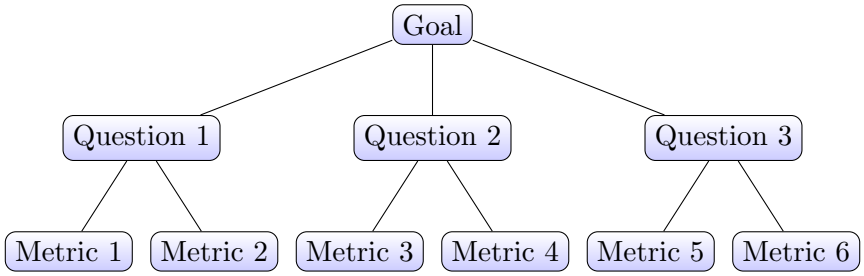



Figure 4.3: Goal Question Metric Approach

### 4.2.5 Expert Review

The expert review research method investigates a research question using the opinion of a selection of experts in that area to answer it. Best results are achieved using a mixed method Johnson and Onwuegbuzie (2004) and Johnson et al. (2007) to gather qualitative and quantitative data from experts. Therefore, the expert review should be semi-structured to capture qualitative and quantitative data. A set of predefined questions with quantitative responses are written for the purpose of directing the expert's attention to a specific issue, and open-ended questions are used to uncover their understanding of the components and the metrics. This implies the collection of quantitative and qualitative data that will answer what building blocks are required for the framework and why they were selected.

**Quantitative Data Collection**: is numerical measurement of information for statistical data analysis for closed questions. For example, a Likert scale Likert (1932). Information such as performance, behaviour or professional outlook is collected using questionnaires and surveys; however, the analysis can only be carried after the data is collected.

**Qualitative Data Collection**: is an understanding of people's responses to performance, behaviour or professional outlook with open-ended questions. This method is used to investigate areas that might be overlooked by the researcher. It is implemented in an informal and flexible setting. The data is analysed through dissemination of comments and transcribed audio recordings.

**Mixed methods Data Collection**: A balance of quantitative and qualitative data collection methods can be used together to overcome each other's shortcomings. Mixed methods can provide valuable insight into the issues being investigated by the researcher, especially for evaluating theoretical frameworks. This gives a better perspective than using a single study to verify the framework and research conjecture. Mixed methods can be used as a part of the triangulation Jick (1979).

The work here will use mixed methods, as some components might be overlooked or measurements exaggerated. There might also be concerns about the technology of 3D printing and reservation in securing 3D objects or missing factors to secure 3D prints. These opinions, concerns, reservations about the measurements are uncovered using mixed methods. The expert review will be conducted using:

**One-to-one interviews** These will be conducted with senior specialists in the fields of computer security, additive manufacturing and cultural heritage and will provide valuable insight into the research problem and also avoid dominant influence in focus groups (Rabiee, 2004). The expert review will be conducted following an explanation of the work to the interviewees individually. A discussion ensues including answering a few set questions and documenting the findings.

The results of the expert review should confirm that the components of the framework (properties) are correct and that there is nothing missing for the first research question. The expert review should confirm if the metrics specified are a good measure. This will be accomplished by asking the participant to complete a task sheet, then elaborate their responses to the quantitative questions.

**Focus groups** The focus group is a group of three to four people consisting of junior academics and postgrads Stewart and Shamdasani (1990) in the same field, so the conversation will not be dominated by one expert, as discussed by (Robson and Foster, 1989). After having them sign a consent form, they will be asked a number of questions and score the answers on a Likert scale. Then they will be asked, as a group, about their answers. The entire session will be recorded and later transcribed. This research uses two focus groups: one to confirm the components of the provenance framework, and the second to determine how the metrics should be measured in a meaningful and significant way to uncover shortcomings of the provenance framework.

The reasoning behind using one-to-one interviews and focus groups is that senior academics have more to add in general and so need more time. Having a senior academic

in a focus group could affect the outcome by potentially dominating the conversation. Also it was found by (Kaplowitz and Hoehn, 2001) that focus groups and interviews are not interchangeable, and very much complement each other as they uncover different perspectives about the same issue and this is crucial for multidisciplinary research.

### 4.2.6 Software Requirement validation using prototyping

This software practice works by discovering the requirement from the stakeholders using prototyping based on communicated operational scenarios. By presenting something tangible, the prototype anchors the conversation between the customer and developer about the requirements for the system. This process was used in research for the oil and gas industry in (Røkke et al., 2011).

## 4.3 Research Plan

The research plan describes the application of the research methods 4.2 using enumerated steps to form a clear action plan. 4.4 shows the research plan sequence, the plan start with building a threat reference to understand the threats to additive manufacturing and what to protect against to answer research question 1. Then build an initial to to build the components and metrics for research question 2 and 3. Question 2 and 3 will be confirming the components and metrics to provide provenance for additive manufacturing. The nested structure is (seven security properties and between them they have 19 components, and for each component its metrics that have several items measured using scales).

Lastly, research question four that will be addressed by using the framework to build a benchmarking tool for additive manufacturing and validated using software requirement verification using prototyping.

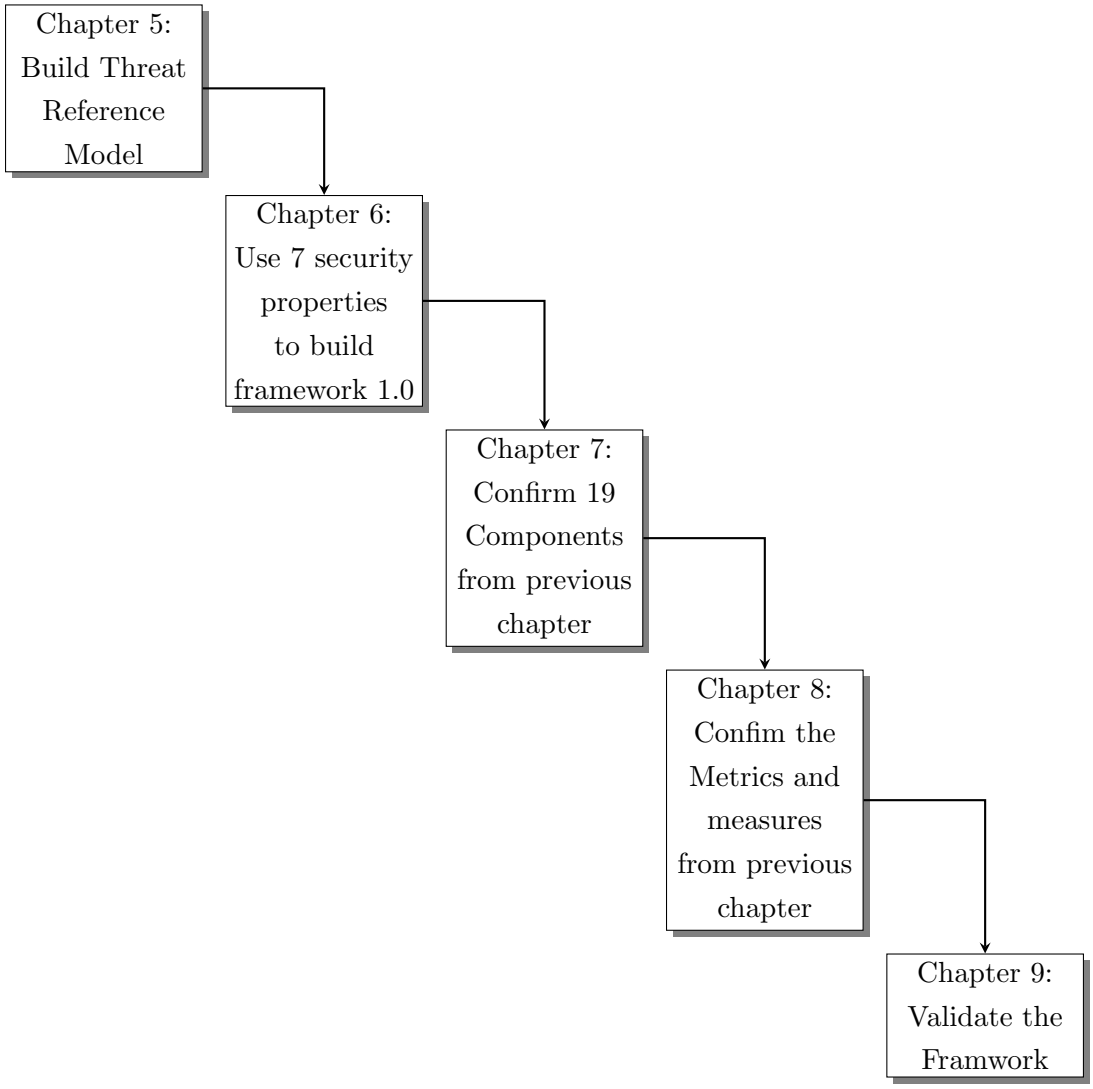



Figure 4.4: Framework confirmation methodology

### 4.3.1 Research plan for Question 1

The best method for investigating the physical/digital disconnect is to describe it semantically with the help of PROV-N provenance language. This language will be used to describe the AM process and identify the point of transition. Figure 4.5 shows triangulation of the research methods used to address this research question.

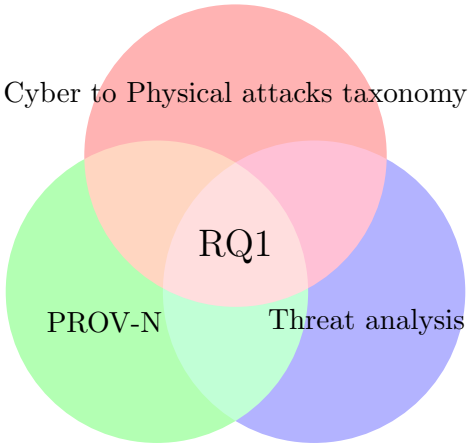



Figure 4.5: Triangulation for the first research question

The research will use as source data: 8 cases from Common Vulnerabilities and Exposures (CVE), 5 cases publicly published, and 9 hypothetical cases. The three data sets will be used as test scenarios to build the threat reference model and prototype test scenarios. The research method steps to build the test scenarios are:

1. Case study preparation: will commence by collecting and building an adequate set of use cases.
2. Data Analysis: Raw data will be analysed using semantic modelling.
3. Information Parsing: The data will be parsed and all the information that is not required for proving provenance will be discarded.
4. Security principle benchmarking: Confirm coverage of three security principles (Information Transmission, Information Security and information Authenticity).
5. Security properties benchmarking: Confirm coverage of the seven security properties (Accounting, Authentication, Authorisation, Availability, Confidentiality, Integrity, Non-repudiation) using the proposed components and metrics.
6. Provenance weakness report: Map security vulnerabilities to the final use cases using cyber to physical attacks taxonomy showing the threats to additive manufacturing.

The method for building the reference model will be conducted in the following steps.

1. Build an adequate description of the threat scenario that affects vulnerable entities, stakeholders and processes involved in generating entities and carrying out attacks.

2. Map the description to a cyber to physical taxonomy. The mapping will build three groups of keywords (entities, activities, and agents).

3. Semantically describe the manufacturing process that include additive manufacturing identified into relationships between entities, activities, and agents.

4. Build Scenarios for CVE testing of (CIA) Confidentiality, Integrity and Availability. The reason for this is CVE is a set of published incidents affecting information security of confidential data, such as car designs or Art.

5. Build Scenarios for real cases testing of (AIN) Authentication, Integrity and Non-repudiation. The reason for this is real cases are IP thefts, where the published item has been hijacked, not because of vulnerabilities in IT systems.

6. Build Scenarios for hypothetical cases testing of (AAA) Authentication, Authorisation and Accounting. The reason for this is network transmission hacking is not specific to AM (man in the middle is not used just to attack AM). Therefore, a scenario where this is possible is more appropriate.

7. Build the threat reference model.

### 4.3.2 Research plan for Questions 2 and 3

The plan for research into questions two and three is same because it will use the same triangulation.

**Answer to the second research question** The research area of addictive manufacturing information systems is relatively new and is in the cyber to physical domain. An attempt is made to build an initial version that can be improved on. Therefore, the Goal Question Metric approach (GQM) will be used to build an initial framework and these framework components can be later refined. The experts will examine and confirm the refined GQM components as being necessary and complete for the successful transition of security properties from digital to physical 3D objects.

An expert review, that is a combination of focus groups and interviews, will then evaluate the components of the framework. The expert review will collect quantitative and qualitative data to confirm the components. Figure 4.6 is a triangulation of the research methods used to address this research question.

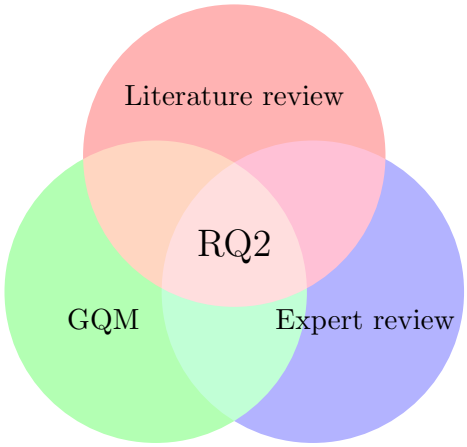



Figure 4.6: Triangulation for the second research question

**Answer to the third research question** This research activity is to evaluate the framework metrics using an expert review of focus groups and interviews. This second expert review will confirm the metrics for the provenance of 3D objects, as well as the measurements to ensure they measure the right things.

The literature review established that there are digital and physical AM properties involved in the AM process. Therefore, the components will have several metrics to cover the digital/physical software and hardware. An expert review will be used to confirm the metrics and measurements for the components of the framework.

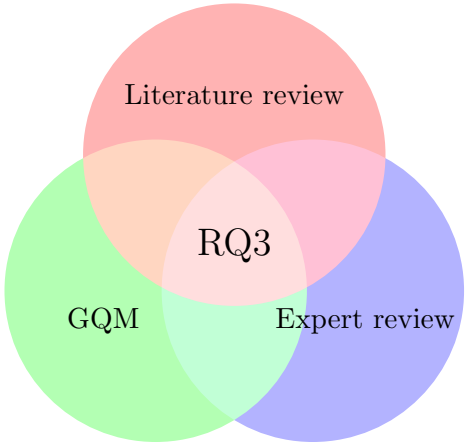



Figure 4.7: Triangulation for the third research question

The expert review process is the same for both research questions one and two. In both expert reviews the procedure is as follows.

1. Introduction to the research, explaining what the research is about and its purpose. Since this is multidisciplinary, terms and acronyms are also explained.

2. 30 Minute presentations explaining the framework.
3. Handing out the participant information sheet that gives them an overview of their rights in their voluntary participation.
4. Collect the information sheets.
5. Discussion the responses to the questions in the sheets.
6. Record the findings of the discussion.

**Experts**: Four types of expert are selected to insure a wide coverage of additive manufacturing users to investigate the transition of security properties between 3D objects and 3D prints. These are drawn from the following categories:

- Computer science experts already using 3D printing technologies within the academic community.
- Cyber security experts within the academic community.
- Experts in the cultural heritage domain, with experience in digital archaeology.
- Data consumers that use 3D printing in their work or research, with more than 2 years' experience working with 3D printers and 3D design tools.

The experts also need to satisfy the following:

- The experts in 3D printing, security and cultural heritage need to be active researchers and part of the academic community or in a leading research institute.
- The data consumers need to have experience of working with 3D printing and 3D design.

In summary, the triangulation will use expert reviews for the metrics and expert reviews for the measurement and literature review as shown in Figure 4.7 of the research methods used to address this research question.

**Statistics: Likert scale and Sample size** Likert scales are used to measure an individual response to a particular question and, in the case of research questions one and two, it will be used to confirm the proposed component, metrics and scales. Likert scale data is ordinal and the measure is which item accumulates more responses, rather than the difference between two points. In this work, Likert scale will be used to measure a trait or attitude so Mean and Standard Deviation is used. For the expert reviews, the One-Sample t-Test will be used because this research had a predefined mean and

the type of analysis is "A priory power analysis". Therefore, determines the number of participants for the first and second surveys. The results will show any difference from the mean that have a statistical significant result. Therefore a G*Power calculation will be used, implementing a one sample one tailed t-test to show the difference from the constant. The effect size type was large, therefore the effect size was 0.8. Type I error probability was 0.05, and type II was 0.2, which gives a power value of 0.8. Based on these values the sample size was 12 participant for each expert review. However and addition 4 experts were add to further confirm the results to bring the total to 16 per expert review.

### 4.3.3 Research plan for Question 4

By this stage, the research would have a framework confirmed by experts in the cyber security and additive manufacturing fields. The framework now needs to be validated. Therefore, requirement validation by the prototyping method will be used to validate the framework. The validation will use PROV-N to semantically describe the scenarios that will be presented to the stakeholders. These scenarios will help demonstrate the framework coverage and the attacks that invalidate additive manufacturing. Figure 4.8 shows triangulation of the research methods used to address this research question.

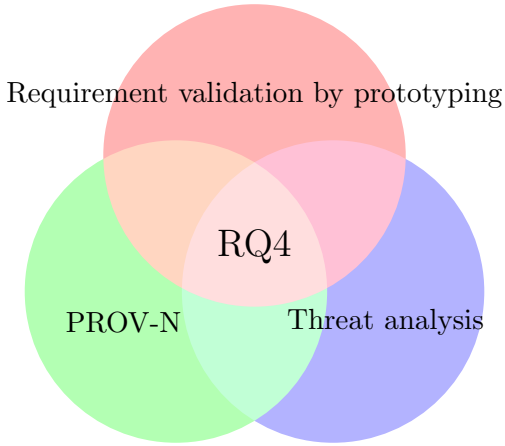



Figure 4.8: Triangulation for the fourth research question

The validation will show that all software/hardware configurations are accounted for and covered in the framework. The benchmarking tool will be evaluated using software requirement prototype validation and threat analysis that is described using PROV-N. The validation process will be as follows.

1. The entities (Target data), processes (Targeted processes), Agent (Targeted Stakeholders), will be extrapolated from the use cases.

2. The relationships (Uses, Generated By, Invalidated By, Associated with, Acted on behalf of, Derived from, and Informed by) are mapped between entities, processes and Agents.

3. The cases will be built using PROV-N to make sure the relationships are correct, and ensure unification of use case modelling.

4. The cases will be compared with the reference model built using the framework in research Question 1.

5. The cases including scenario, threats and recommendation will be mapped to the reference model that is composed of 21 cyber to physical relationships as described in appendix B.

6. The validation will use the scenarios from research Question 1 to test the framework coverage of all possible cyber security incidents that could be inflicted on additive manufacturing.

## 4.4 Ethics

The study involves human subjects and so the ethical side of the research was addressed to maintain professional integrity in protecting the subject's rights. Ethics approval was required from the University of Southampton Ethics team. Voice data recordings acquired from the subjects were transcribed and anonymised. The original data recording was destroyed and only anonymised data is kept. The ethics reference number is filed under ERGO/FoPSE/9287.

## 4.5 Summary

The research methodology is an important part of the work and follows good scientific procedure that helps to provide concrete evidence to answers the research questions, which address the successful transition of security properties from digital to physical objects and *vice versa*. This chapter set the scene by starting with framework structure and data flow, and then described two scenarios of how the framework could be applied hypothetically in an additive manufacturing environment. It then listed the research objectives and questions to create new contributions to knowledge. The concept of research triangulation was explained, then the research methods used in this work described. Lastly, a detailed research plan was proposed that would answer each research question.

# Chapter 5

# Threat Analysis of Digital Disconnect

This chapter addresses the first research objective which is:

> Build a reference model for the digital/physical threats disconnect in the transfer of security properties from 3D object (digital state) to 3D print (physical state) using 3D printers.

The objective aims to answer the first research question **"What is an appropriate reference model for semantically describing additive manufacturing threats within a manufacturing line?"** This chapter starts by explaining the additive manufacturing data flow process, to build a foundation for the reference model. It then describes three sets of threats. Following this, patterns should be identified in the additive manufacturing process and threat scenarios.

Examples of infringements in additive manufacturing are currently scarce and no live data set was readily available. Therefore, data was mined from CVE entries, published legal cases of intellectual property infringement, and hypothetical threat examples. The hypothetical use cases are a list of possible but not yet exploited threat scenarios. The modelling of cyber to physical threats is generic and able to describe a wide spectrum of security threats. The data collected will show violation trends and patterns that will be used to build the reference model, while the data modelling describes cyber to physical attacks using the (Moreau et al., 2011) provenance model. This is followed by a discussion of the recommended responses to these threats.

## 5.1 Analysis of Additive Manufacturing Information Model

The additive manufacturing information model described here is derived from the (Noorani, 2006) product development cycle, the last step being anaddition added to the original model. The description is generic, so it fits any AM process. The information model steps are:

1. Design concepts, where the design requirements are gathered
2. Parametric design step using (CAD)
3. Store (CAD
4. Optimisation step, where calibration of the machine and the material is preformed (Gcode)
5. Fabrication or rapid prototyping
6. Testing of prototype
7. Documentation of test result
8. Final product

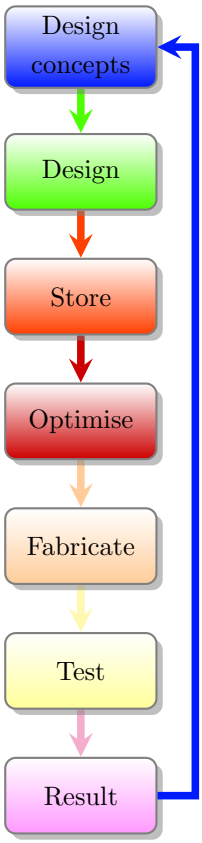



Figure 5.1: Additive manufacturing information model

In Figure 5.1, the results are documented if the additive manufacturing model is implemented properly. This is valuable as it determines if the object handled is the same or a

derivative of the original, because observations of the AM process indicates two possible results when trying after the fabrication of the 3D objects.

**First possible result** Once the additive manufacturing is successful, then the 3D object is AM ready. This process may take several iterations and revisions to produce a printable 3D object. All iterations and changes should be documented as this enriches knowledge of the object and how to make it.

**Second possible result** The additive manufacturing is not successful as the 3D objects does not fulfil its required purpose (fit), or breaks during the AM process. However, instead of discarding the failed 3D object, the information is used to create a new object and reasons for failure are documented to avoid future failed AM 3D objects.

The model in Figure 5.2 was constructed as part of this research to help transfer provenance information. At the moment the **Information enrichment process** box is missing. The knowledge to make 3D objects and fabricating them is a known area but transferring the information from physical to digital is not known, and to transfer information correctly, the right information needs to be embedded in the first place.

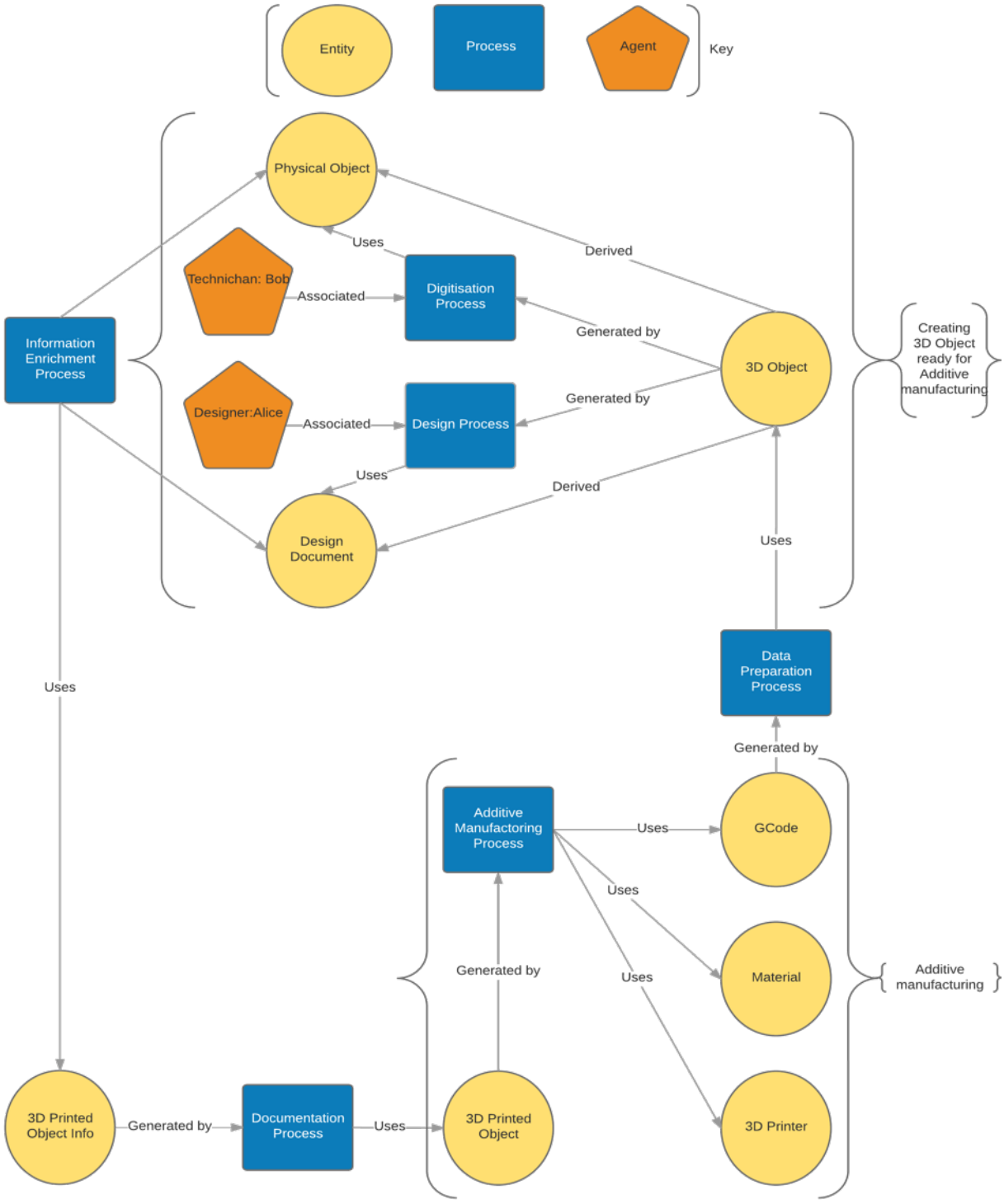



Figure 5.2: Additive manufacturing Information Model using provenance modelling

## 5.2 Threats to Manufacturing

How can we define real? Digital objects are computer-generated, physical objects are man-made and both hold value, and that value is under threat in one of five ways, depending on the type of object, as discussed in 2.3.2.

**Spime Threats** face a high value IP product, and this value requires Spime objects to be trackable. For example, mobile phones have a unique identifier IMEI number.

**Gizmo Threats** face a competitive IP, similar to Spime, but not trackable. For example, a branded wine bottle that has a leaflet with information about the wine.

**Product Threats** to branded IP for products bought and sold that are manufactured on a large scale that compete with other brands. For example, any generic bag of salt.

**Machine Threats** to machine-produced objects, not necessarily branded but unique to that machine. For example, a prototype produced using a 3D printer.

**Artefact Threats** to one-of-a-kind man-made objects. For example, a hand-made vase.

Items produced using additive manufacturing arguably can fit into any of the above threatened objects depending on the readiness of the goods once manufactured. For example, if a 3D printed object was considered one of a kind and not meant for distribution, it could be classified as an artefact, whereas if the object was produced in bulk using a 3D printer then it would be classified as a machine object. If a business completely relied on 3D printer to make products, then it is a product object. With Spime and Gizmo objects, the digital disconnect becomes more tangible, as all the information contained within Spime and Gizmo do not transfer once the object is 3D printed. This research will focus on Spime and Gizmo type objects that has metadata associated with it. This chapter will analyse the threats facing AM for these objects using a combination of threat analysis and semantic modelling to illustrate the impact and importance of protecting AM.

## 5.3 Documented Cases of IP infringement in Additive Manufacturing

Some view 3D printing as a disruptive technology because of its potential to infringe on intellectual property. Nevertheless, 3D printers are becoming cheaper thanks to companies such as Stratasys Berman (2011) as well as General Motors, Boeing, Nike,

Ford, and many others that have joined the race for better and more affordable 3D printing. The emergence of personal 3D printers at an affordable price has created a demand for 3D objects and an urgent need by their users to provide IP provenance for the 3D objects they create, such as art pieces or designer jewellery. Additive manufacturing is dependent on a plethora of logical assets, such as software packages, and hardware of 3D printers, computers and network infrastructure. However, this work focuses on the IP of 3D objects.

Additive manufacturing assets that are targets for attacks are not limited to Intellectual Property, Company Brand, and Marketing, but there are almost no recorded legal cases of exploitation of AM till very recently, although it was invented in the 1980s. The reason is that 3D printers are becoming more affordable and are now receiving a lot of attention and have become a target for exploitation. Part of this research is trying to understand cyber security issues affecting additive manufacturing.

In this section legal cases are described and modelled. It concludes with a list of documented attacks on AM. A 3D printed object can infringe copyright (Bradshaw et al., 2010) in four ways that affect functional designs and non-functional artistic works, functional work flow and branding. These four areas are: Design protection, Copyright protection, Patent protection, and Trademark protection. The following published infringement cases use additive manufacturing.

**Example 1: Penrose triangle** The Penrose triangle is an optical illusion artwork that was created by Swedish artist Oscar Reutersvard in 1934. Ulrich Schwanitz digitised this artwork and challenged others to replicate it. A member of thingiverse user community replicated the work and posted the Penrose triangle as a 3D object for people to download and 3D print. Ulrich Schwanitz threatened the thingiverse user community with Digital Millennium Copyright Act (DMCA) takedown. However, Schwanitz's claim wasn't answered because copyright of intellectual property does not cover derivatives, and the original artwork copyright had expired. However, for the sake of argument, suppose Schwanitz's claim was covered by DCMA. The infringement process is described in Figure 5.3.

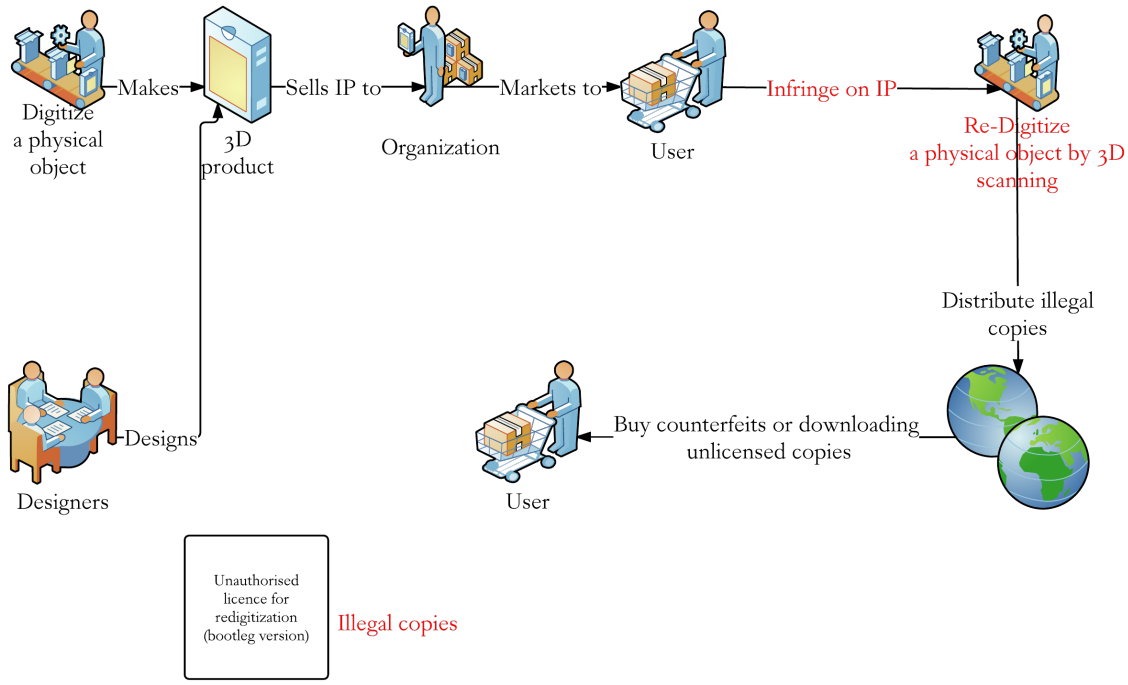



Figure 5.3: Penrose triangle possible IP infringement on Ulrich Schwanitz 3D object

**Example 2: Warhammer figurines** The case of the Warhammer figurines is clear infringement of copyright infringement since a member of www.thingiverse.com posted a modified Warhammer design, after which a lawsuit was issued. Game Workshop UK, who owns the copyrights for Warhammer, sent a legal notice citing the Digital Millennium Copyright Act to take down a modified Warhammer 3D model from their 3D library for 3D objects. The user unintentionally replicated original goods and produced counterfeits, because a substantial amount of copying of the original goods had been performed. The legal case was not escalated further but it served as taster of the consequences of affordable 3D printers. In this case, the user had all the information he needed to produce the counterfeits. The infringement process is described in Figure 5.4

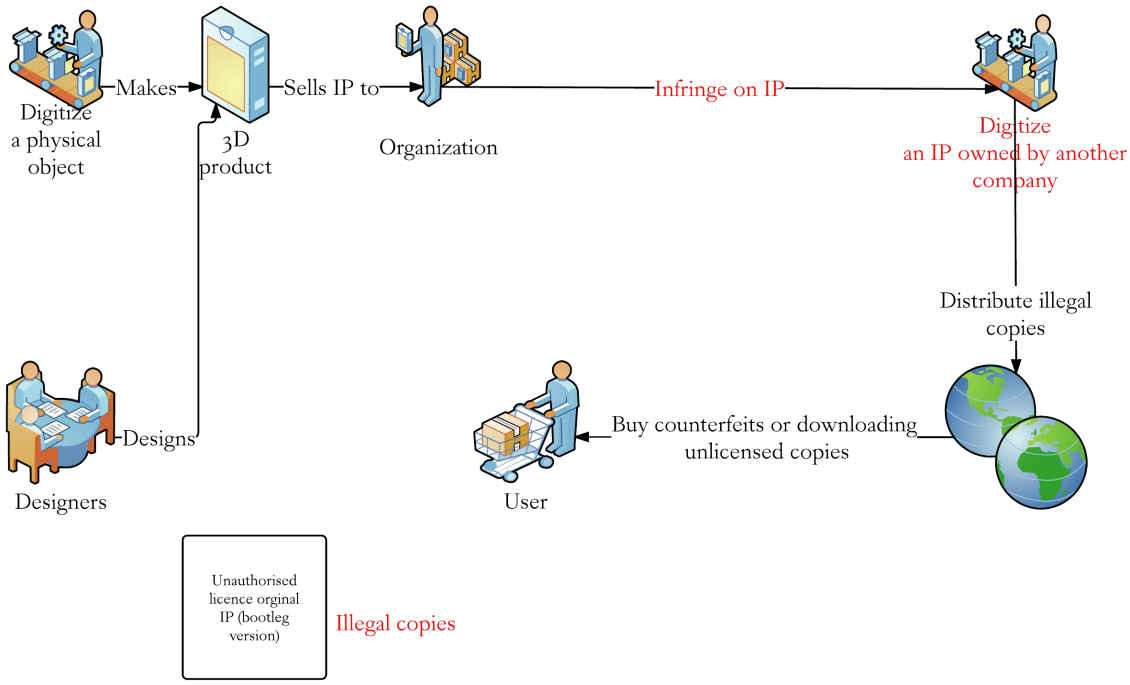



Figure 5.4: Copyright infringement of Warhammer figurines

**Example 3: Game of Thrones IPhone charger** nuPROTO, owned by Fernando Sosa, recreated a replica of the 'Iron Throne' from the HBO hit series 'The Game of Thrones' in the form of an IPhone cradle and charger. HBO delivered a Cease and Desist Notification to nuPROTO not to sell the object because it infringed their copyright. However, since nuPROTO had an official disclaimer saying that this object was not an officially licensed product, they felt they should be in the clear. The case is still open because functional objects are patented not copyrighted and the artwork is not textitseverable from the object, therefore no copyright exists as it is considered part of the function Kharif and Decker (2013). The infringement process is described in Figure 5.5

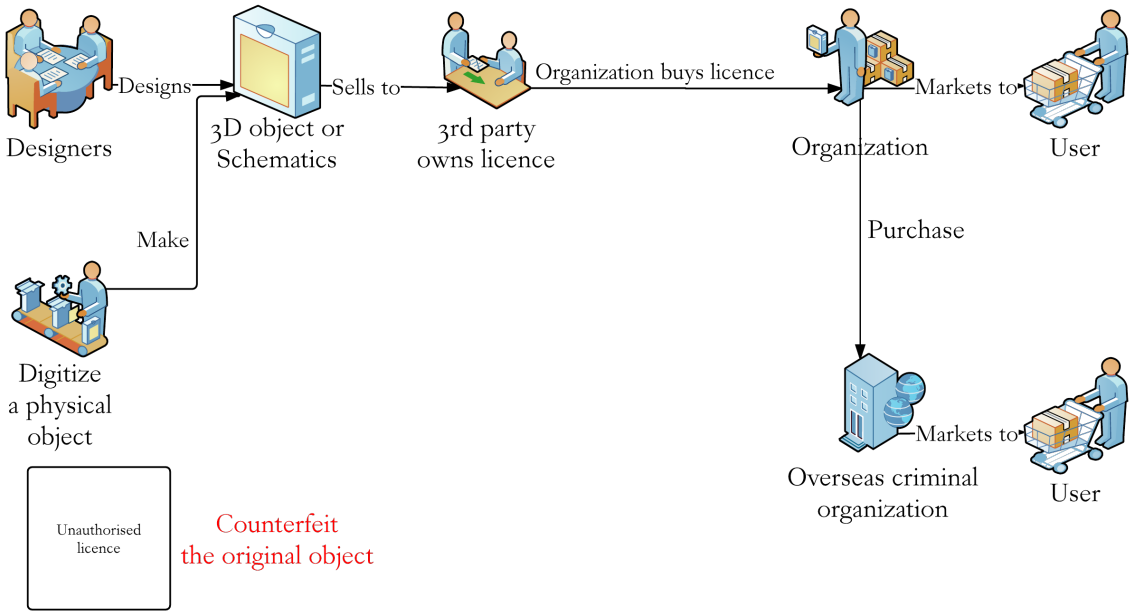



Figure 5.5: Game of Thrones possible IP infringement of HBO property

**Example 4: Ford and General Motors** Car manufacturers spend massive budgets on automotive research and development projects, consequently corporate espionage is a huge issue. For example, General Motors own millions of dollars in trade secrets concerning hybrid cars in the form of documents and 3D objects. Sensitive documents were leaked to a Chinese rival car manufacturer that now produces and sells these products. Ford is another example that has lost $50 to 100$ million dollars in intellectual property in a single case to another Chinese rival because of theft of the information by a former employee Smallwood (2012). Figure 5.6 illustrates IP infringement cases driven by competition.

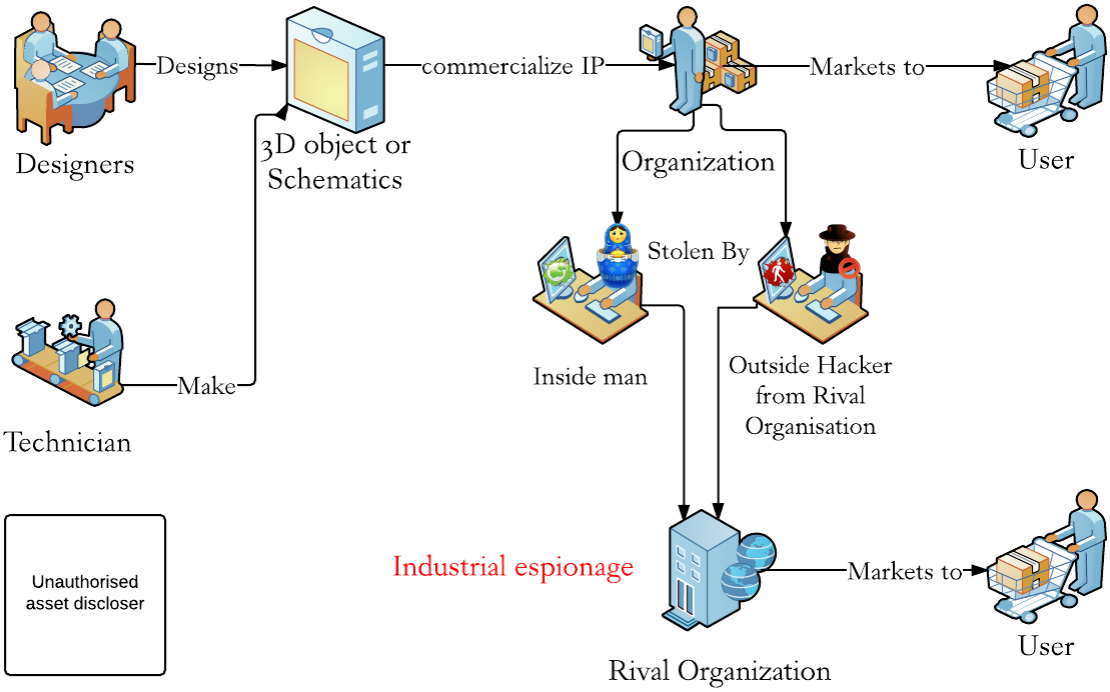



Figure 5.6: Industrial espionage on holders of original IP

Industrial sabotage of competitor organisation is illustrated in Figure 5.7 that happens between two competing organisations to gain a market advantage.

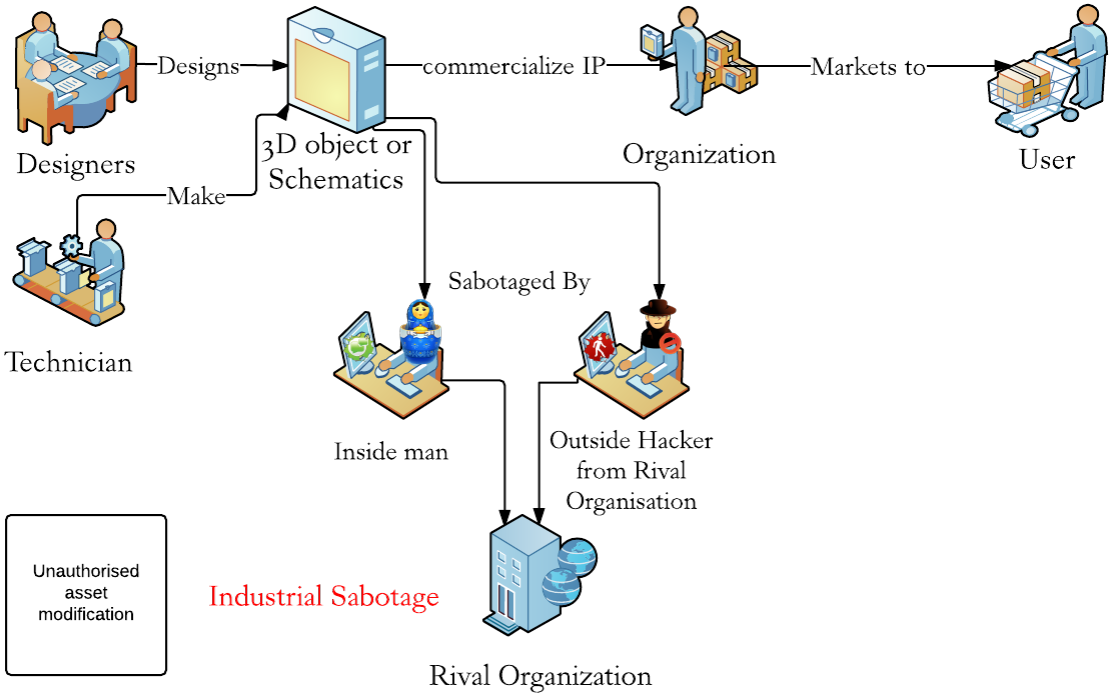



Figure 5.7: Industrial sabotage by competitor organisation

## 5.4 Hypothetical Threats to Additive Manufacturing

Different methods can be used to infringe the IP of an organisation. While these methods focus on additive manufacturing, they are also applicable to any manufacturing process that relies on the extensive use and distribution of electronic design files. Figure 5.8 summarises the work flow for a normal production process of a tested and finished 3D object. The solid lines represent digital information and the dotted lines a physical object; green indicates the normal work flow, while red indicates a security concern. The physical location of the designer, store and printer is immaterial for this discussion. The complete process could easily take place within a single manufacturing facility or at sites worldwide.


Figure 5.8: Conventional adaptive manufacturing work flow

The following methods can impact these basic processes (Design, Store, Printer and Use).

**Disclosure** : 3D object data is leaked to unauthorised parties. This affects buyers and sellers of 3D objects.

**Modification** : 3D objects or processes involved are modified and may cause corruption or change behaviour. This affects buyers and sellers of 3D objects as well as the 3D printers.

**Loss** : 3D object data are completely destroyed by an unauthorised party. This affects buyers and sellers of 3D objects.

**Interruption** : Processes such as storing and 3D printing can be interrupted and can potentially affect delivery or stop it altogether.

Figure 5.9 illustrates the effect of a cyber attack on the 3D printing process of a 3D object.

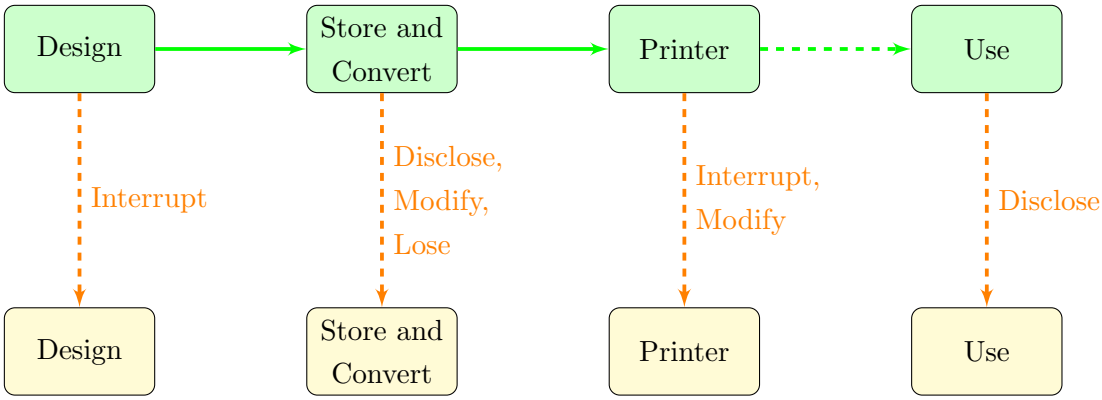



Figure 5.9: Cyber attack consequences on process and assets in AM

Security breaches can occur primarily at two points in the process: unauthorised access to the electronic data, and copying the physical artefact. The various approaches are summarised in the following diagrams.

- Security issues relating the misuse of electronic information
  - Service disruption of design tools, Figure 5.10
  - Infringement of the license agreement, Figure 5.11.
  - Independent hacker steals the manufacturing file and distributes it widely across the web, Figure 5.12.
  - Hacking of an organisation's server is undertaken by a third party, specifically to use the information for its own purpose, Figure 5.13.
  - Figure 5.14 details a variant of the case shown in Figure 5.13, where the artefact files are deliberately modified to impact on the quality of the product.

  - Figure 5.15 illustrates service disruption of 3D printers.
  - Figure 5.16 illustrates service modification of 3D printers.

- Security issues relating to the distributed artefact.
  - An organisation re-engineers the design of the printed artefact, Figure 5.17.
  - The artefact is directly scanned, the results of which are used to directly print a copy, Figure 5.18

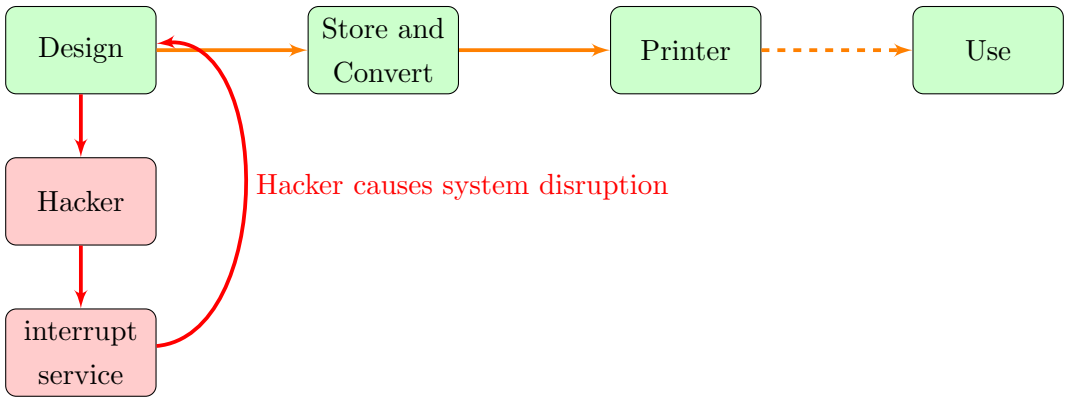



Figure 5.10: Design tools are tampered with, causing disruption

Design tools are susceptible to tampering and causing service outages. Figure 5.10 shows that this could compromise the entire 3D printing work flow. The following are two examples of tampering with services.

**Example 1: Man-in-the-Middle Attack between an organisation and its customers** An organisation provides custom-made jewellery in the form of 3D objects in STL file format to be sold to customers. The organisation sells the designs to be used with 3D printers, but an attacker carrying out man-in-the-middle attacks can interrupt the transmission and edit the 3D file, thus affecting the integrity and renders the STL file unprintable which causes the corruption of digital goods. This attack was possible because of weak boundary security, such as firewalls and access points.

**Example 2: Violation of access control policies between designers and organisations** A jewellery designer uses CAD tools to construct jewellery in the form of 3D objects in a STL file format for an organisation that fabricates or resells the 3D objects. An attacker gains illegal access to the designer workstation and downloads the file, stealing the jewellery designers intellectual property, and illegally distributes the jewellery design.

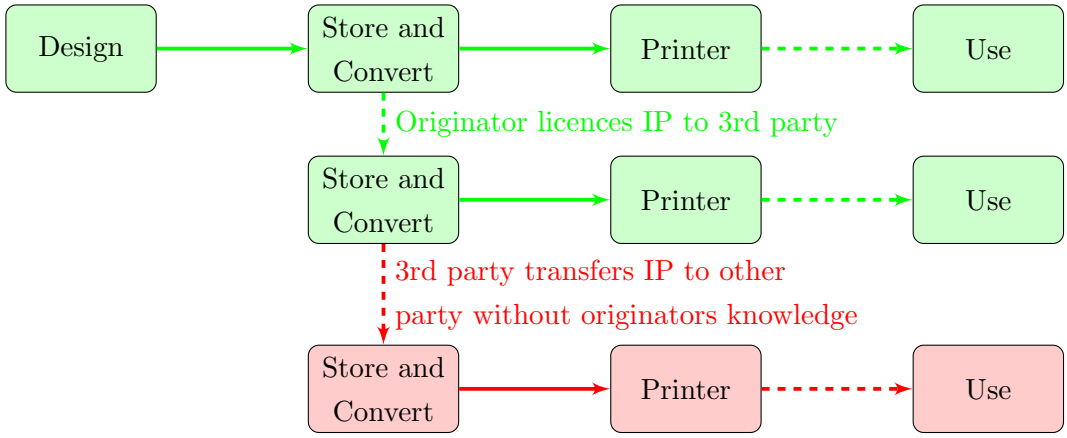



Figure 5.11: The Counterfeit process

In the scenario in Figure 5.11, the IP is compromised by a third party that distributes copies of IP without permission of holder of original IP. In this case the holder of original IP could be an established brand or a small design company as illustrated in the following scenario.

**Example 3: Plagiarism and counterfeiting of organisations IP sold to customers** A jewellery designer uses CAD tools to construct jewellery in the form of 3D objects in a STL file format for an organisation that fabricates or resells the 3D objects. The organisation who bought the designs starts selling the 3D objects without accrediting the original authors.

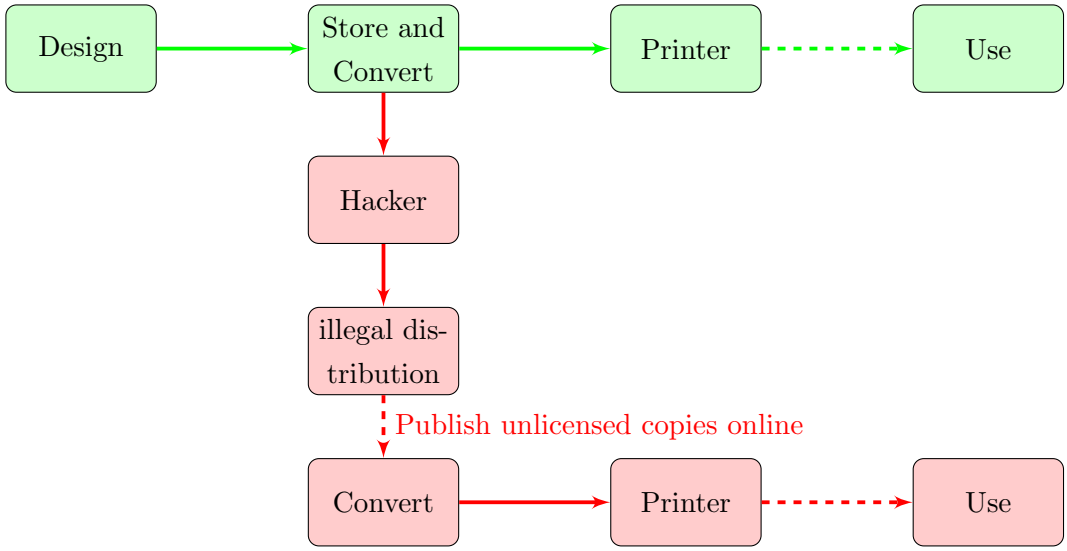



Figure 5.12: Independent hacker placing the file on the web for others to use

In the scenario in Figure 5.12, an infringement occurs when a black hat hacker, or a hacktivist, steals original IP to damage a company brand for self-gain or for a political cause.

**Example 4: Violation of access control policies of organisations** An organisation provides custom-made jewellery in the form of 3D objects in STL file format to be sold to customers. The organisation is responsible for storing the 3D objects in a STL file format, but an attacker gains illegal access and illegally distributes the 3D designs.

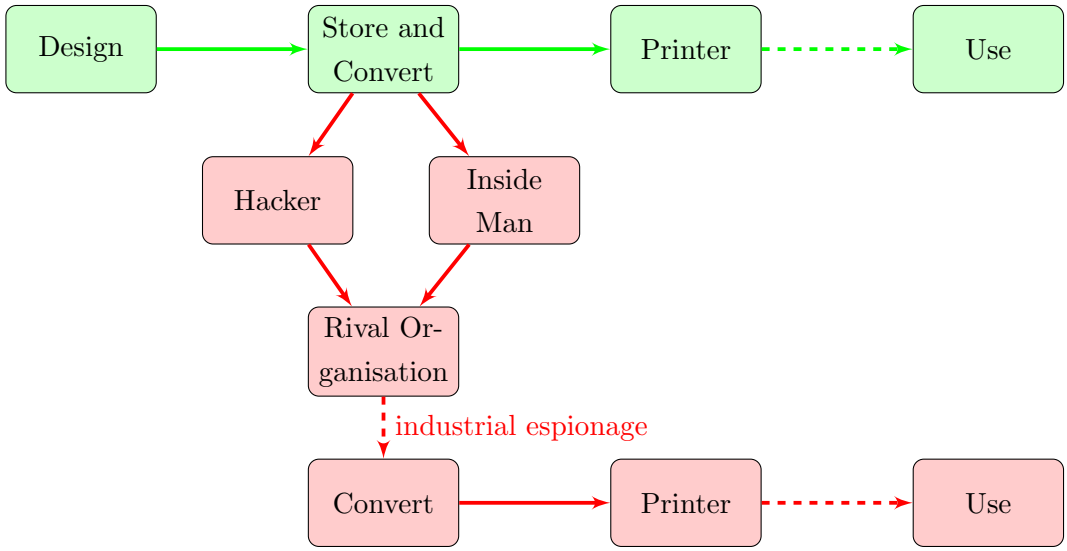



Figure 5.13: Hacking is done under the specific instruction of a rival organisation

Industrial espionage to get a market advantage is common ill-practice. Figure 5.13 shows that this can be done by hiring an experienced blackhat hacker, or paying an existing employee at the target company, to leak IP to a rival organisation.

**Example 5: industrial espionage of an organisation that holds original IP** An organisation provides custom-made jewellery in the form of 3D objects in STL file format to be sold to customers. The organisation sells the designs to be used with 3D printers. A rival organisation hires a black hat hacker, or a current employee to spy on organisation, and steal the IP.

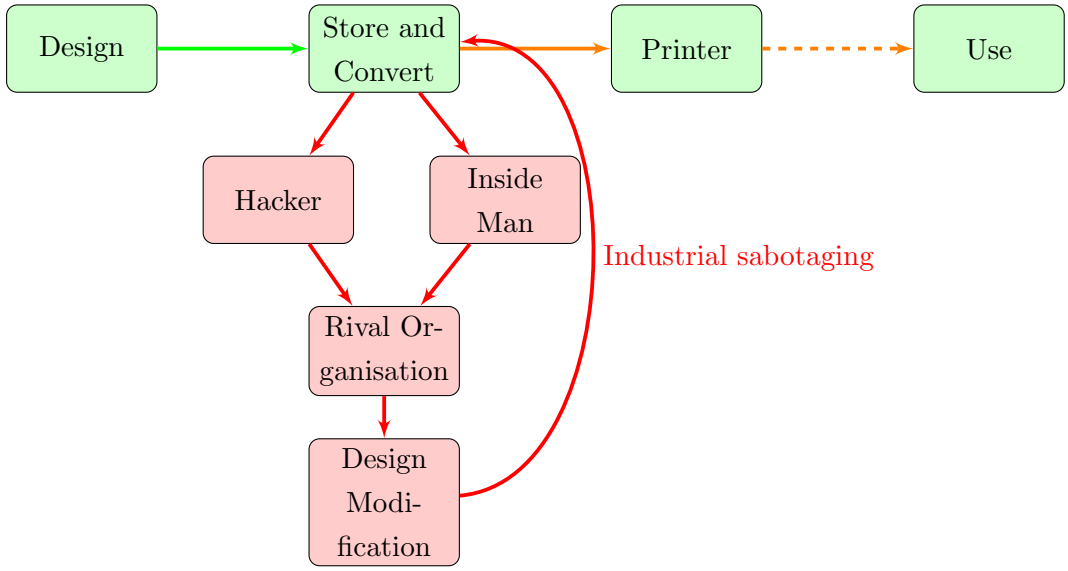



Figure 5.14: Unauthorised asset modification

In Figure 5.14 the targeted organisation brand is damaged by sabotaging market-ready products.

**Example 6: industrial sabotaging of an organisation that holds original IP** An organisation provides custom-made jewellery in the form of 3D objects in STL file format to be sold to customers. The organisation sells the designs to be used with 3D printers. A rival organisation hires a black hat hacker, or a current employee, to sabotage 3D objects or schematics.

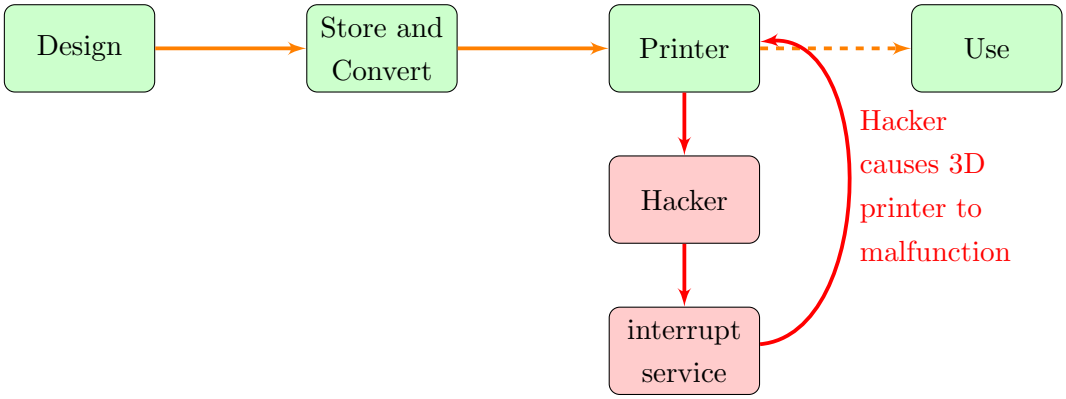



Figure 5.15: 3D printers are tampered with, causing disruption

Figure 5.15 shows service disruption of 3D printers. This causes unprintable 3D objects.

**Example 7: industrial sabotaging of an organisation's 3D printing equipment** An organisation provides custom-made jewellery in the form of 3D objects in STL file format to be sold to customers. The organisation sells the designs to be used with

3D printers. A rival organisation hires a black hat hacker, or a current employee, to sabotage 3D printing equipment.

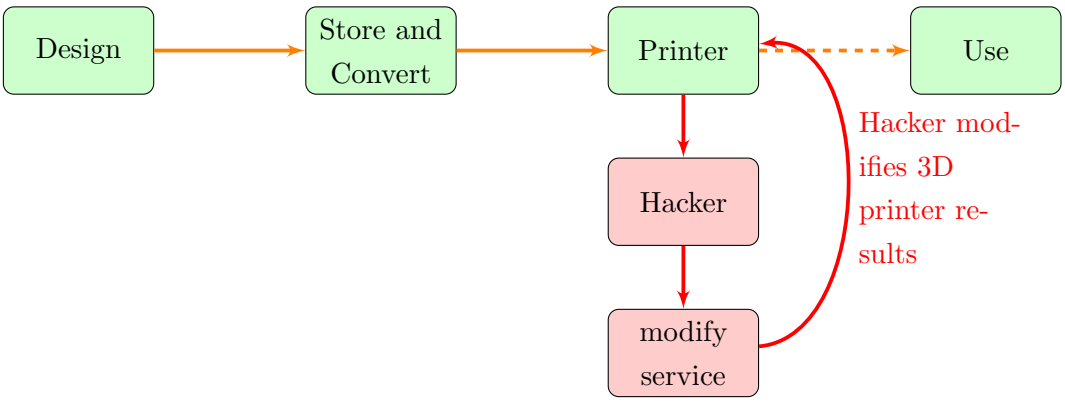



Figure 5.16: The 3D printers settings are tampered with, changing the outcome of the 3D printer

Figure 5.16 shows service modification of 3D printers. This causes changes in the 3D objects' aesthetics or function.

**Example 8: industrial corruption of an organisations 3D printing calibration** An organisation provides custom-made jewellery in the form of 3D objects in STL file format to be sold to customers. The organisation sells the designs to be used with 3D printers. A rival organisation hires a black hat hacker, or a current employee, to corrupt 3D printing equipment, which alters the final results.

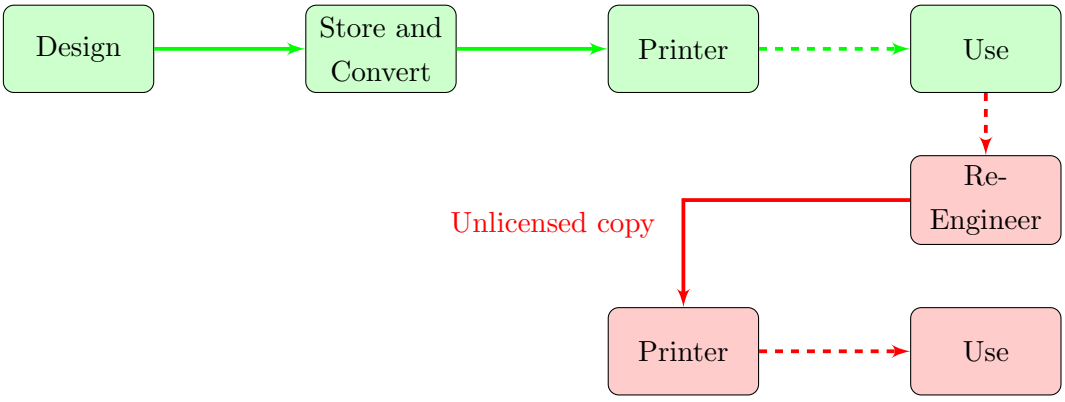



Figure 5.17: The original article is re-engineered, the key features may be copied, while the overall functionality is identical to the original

Figure 5.17 and Figure 5.18 show counterfeiting of original goods by rescanning or reverse engineering the product originally made using a 3D printer.

**Example 9: Reverse engineering of original goods** An organisation provides custom-made jewellery in the form of 3D objects in STL file format to be sold to customers. The organisation sells the designs to be used with 3D printers. A malicious user reverse engineers the original IP, then prints illegal copies of the company's intellectual property.

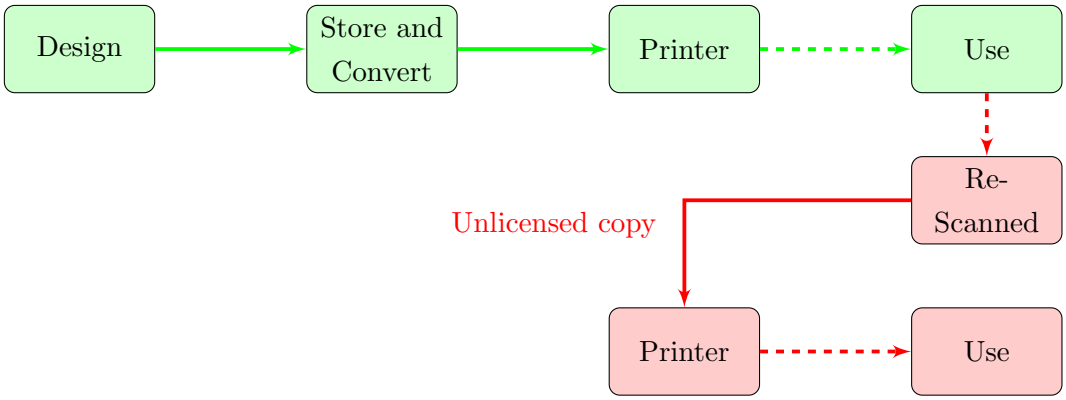



Figure 5.18: A third party illegally re-digitises the component and distributes the new file

**Example 10: Re-digitising of original goods** An organisation provides custom-made jewellery in the form of 3D objects in STL file format to be sold to customers. The organisation sells the designs to be used with 3D printers. A malicious user re-digitises the original IP, then prints illegal copies of the company's intellectual property.

## 5.5 Documented Common Vulnerabilities and Exposures (CVE) in Additive Manufacturing

There are 12 common attacks that can exist in any piece of software. These vulnerabilities can be technically exploited and in most cases are unavoidable. In cases that involve additive manufacturing, this work has identified 7 types of CVE. It is only a matter of time before there are incidents involving the remaining five types (Bypass something, SQL injection, File inclusion, Cross Site Request Forgery, and HTTP response splitting).

**Example 1: Denial of service** in CVE entry (2012-4894), Google SketchUp versions below 8.0.14346 allowed remote attackers, assisted by users, to cause denial of service (memory corruption) or execute arbitrary code via a crafted SKP file.

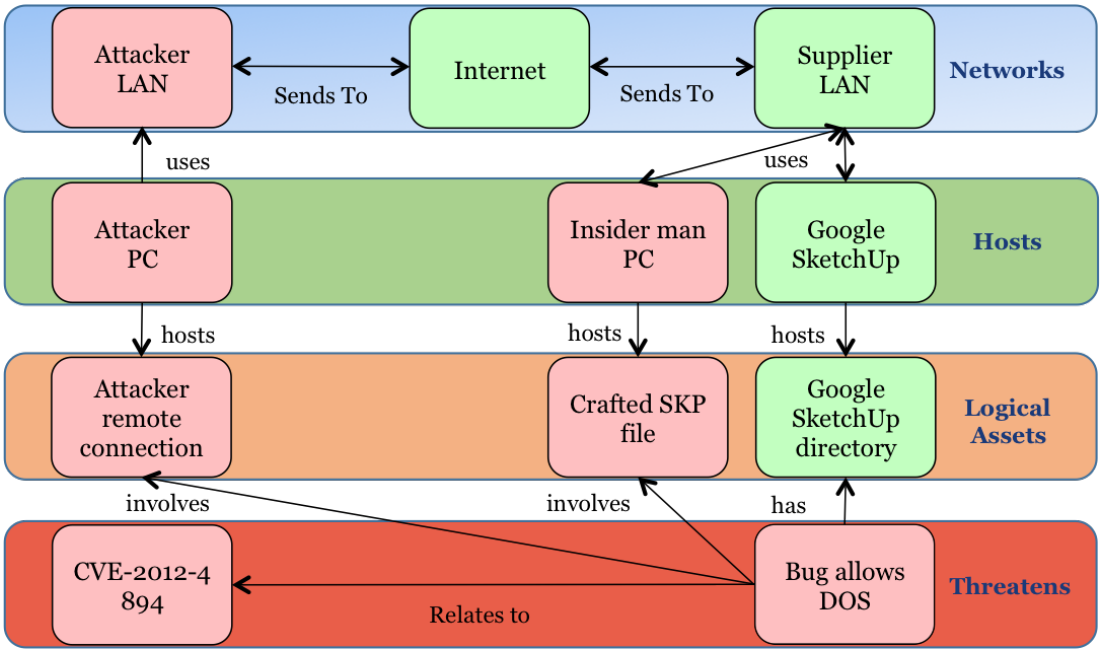



Figure 5.19: CVE entry (2012-4894)

**Example 2: Code execution** in CVE entry (2014-2967), Autodesk VRED Professional 2014 versions below SR1 SP8 allowed remote attackers to use Python, or library calls in Python, to execute arbitrary code via API commands to the integrated web server.

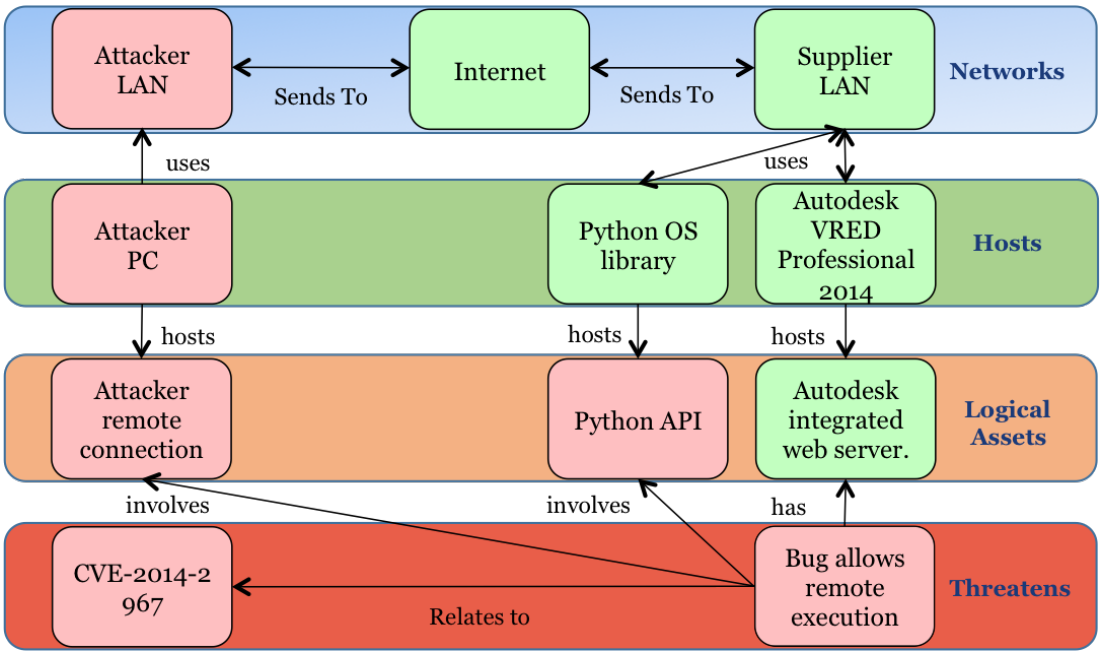



Figure 5.20: CVE entry (2014-2967)

**Example 3: Buffer overflow** in CVE entry (2013-7388), Trimble SketchUp versions below 2013 (13.0.3689), that contains paintlib, can be exploited by launching Heap-based buffer overflow. This allowed remote attackers to use crafted RLE4-compressed bitmap (BMP) to execute arbitrary code.

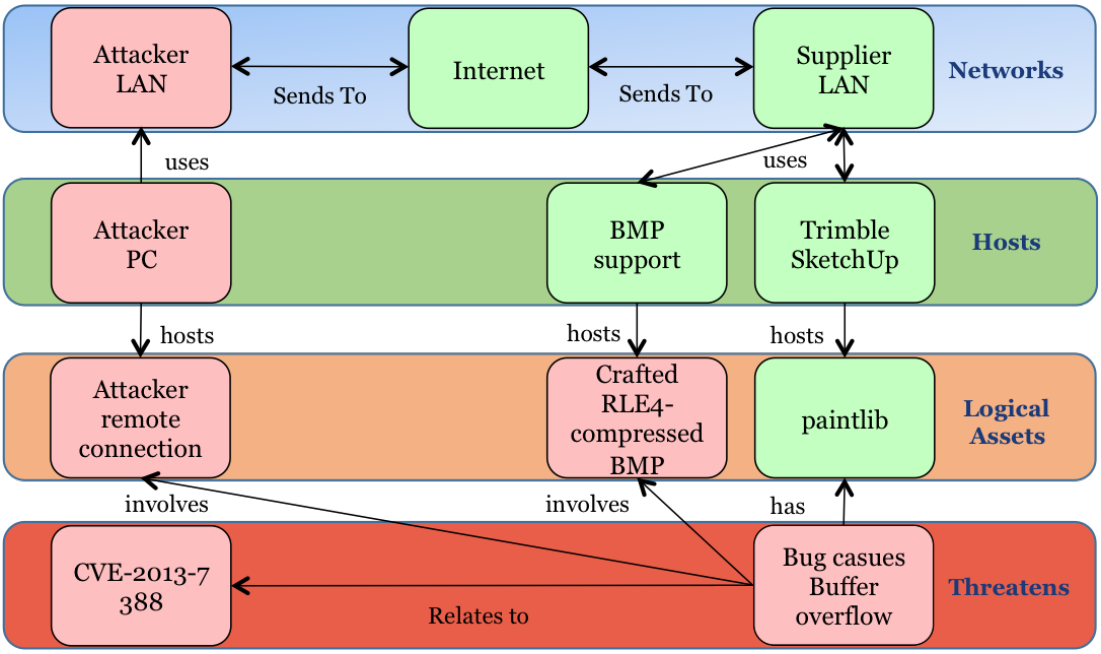



Figure 5.21: CVE entry (2014-2967)

**Example 4: Cross site scripting** in CVE entry (2012-5053), Trimble Web User Interface Infrastructure GNSS Series Receivers (NetR3, NetR5, NetR8, and NetR9 before 4.70, and NetRS versions below 1.3-2), allowed remote attackers to use unspecified vectors to inject arbitrary web script or HTML.

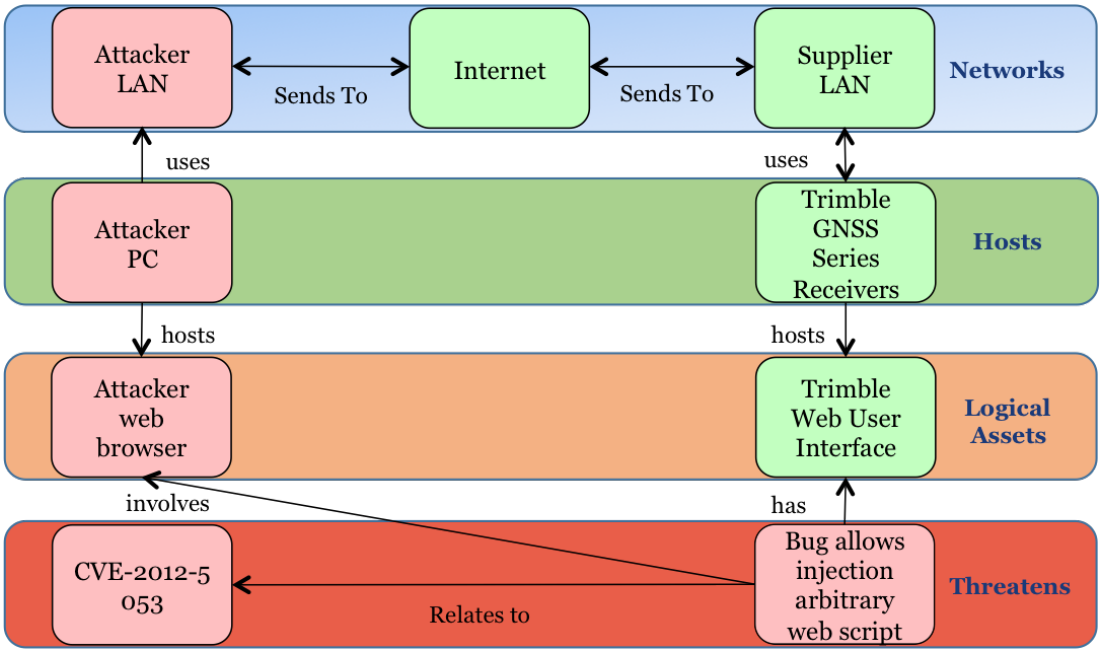



Figure 5.22: CVE entry (2014-2967)

**Example 5: Directory traversal** in CVE entry (2008-4471), DWF Viewer ActiveX control (AdView.dll 9.0.0.96), containing CExpressViewerControl class used in Revit Architecture 2009 SP2 and Autodesk Design Review 2009, allowed remote attackers to use sequences in the argument to the SaveAS method to overwrite arbitrary files.

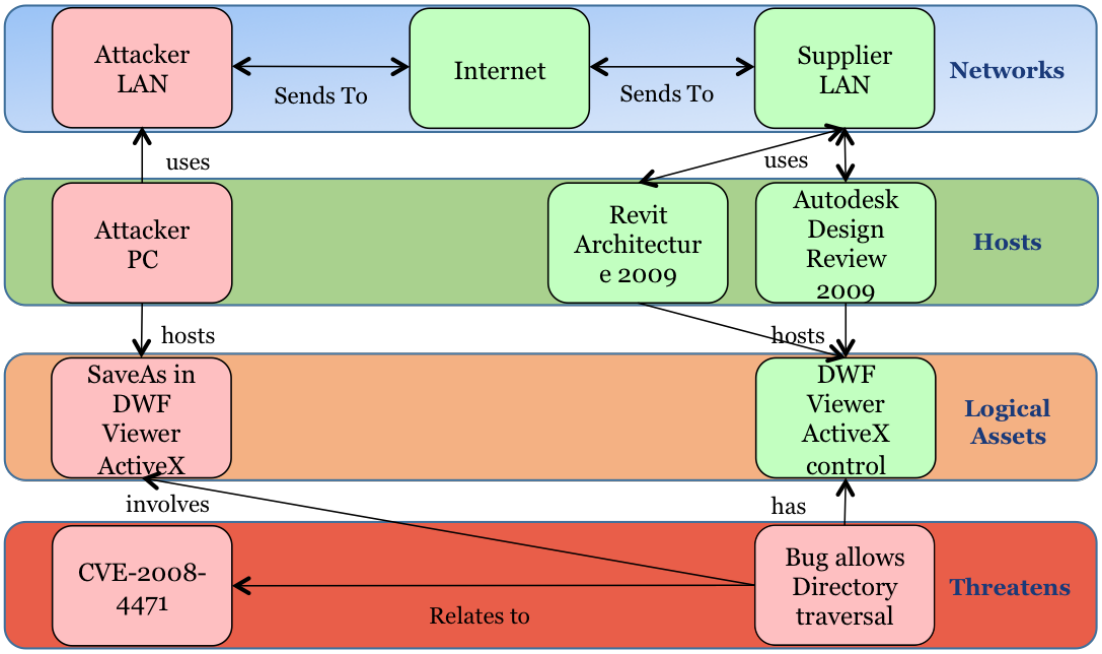



Figure 5.23: CVE entry (2014-2967)

**Example 6: Gain privilege** in CVE entry (2010-5241), Autodesk AutoCAD 2010 had multiple untrusted search path vulnerabilities that permitted local users to gain privileges using a Trojan horse in the directory that contains a DWG file, using dwmapi.dll or IBFS32.DLL files.

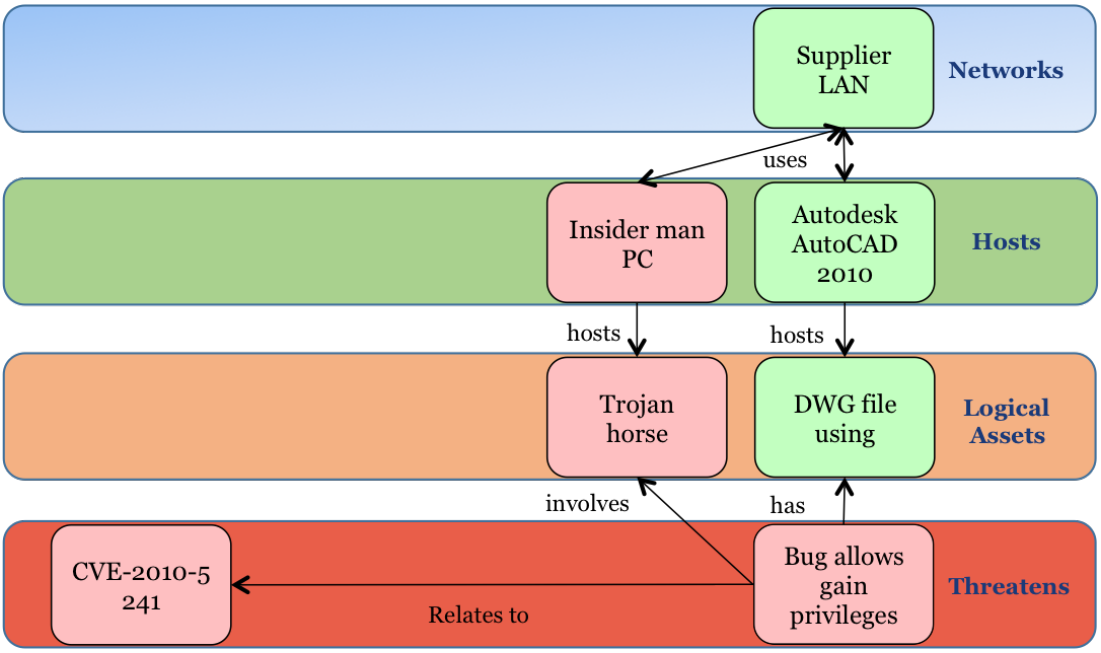



Figure 5.24: CVE entry (2014-2967)

**Example 7: Memory corruption** in CVE entry (2012-4894), Google SketchUp versions below 8.0.14346 allowed remote attackers, assisted by users, to use crafted SKP file to execute arbitrary code or cause a denial of service (memory corruption).

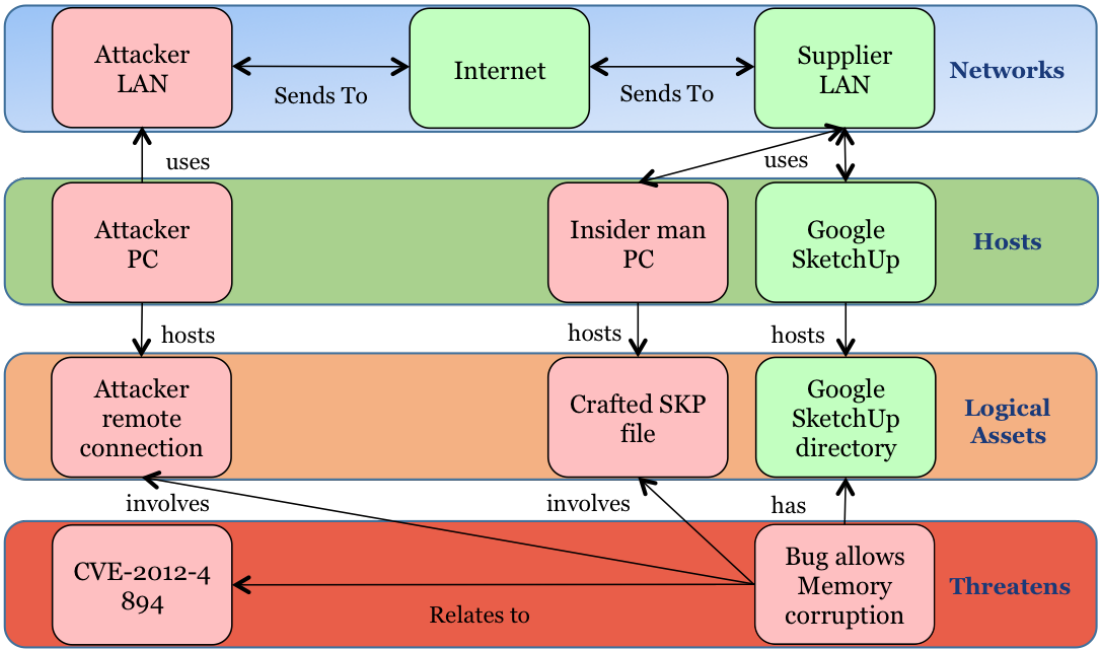



Figure 5.25: CVE entry (2014-2967)

## 5.6 Analysis of Threats

Threat analysis is a structured method for communicating threats by defining assets, threats and vulnerabilities. The threat modelling will describe the cyber security attacks that additive manufacturing is subjected to. These types of attack are classified as cyber to physical attacks, as changes in the digital entity or process can alter the final physical product. Analysis of hypothetical scenarios, legal uses cases, and CVE have been illustrated in sections 5.3, 5.4, and 5.5.

This work started with published legal cases related to additive manufacturing infringements. These cases helped identify basic **processes**, **entities**, and **stakeholders** involved in designing and fabricating 3D objects. These processes, entities, and stakeholders, were used to build hypothetical examples to help explore the threats in more detail. The hypothetical examples were built on the impacts of disclosure, modification, loss, and interruption. This produced 10 predictions of possible attack patterns on fully tested 3D objects, four of which were described in legal cases. The CVE analysed specific types that affect CAD software, which is only part of the design process. These type of attack have a nested structure Figure 5.27.

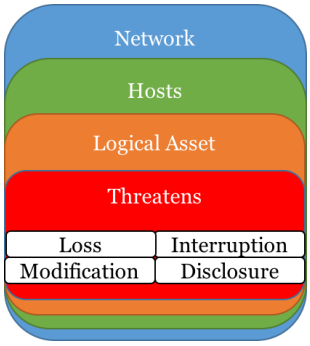



Figure 5.26: Nested CVE structure

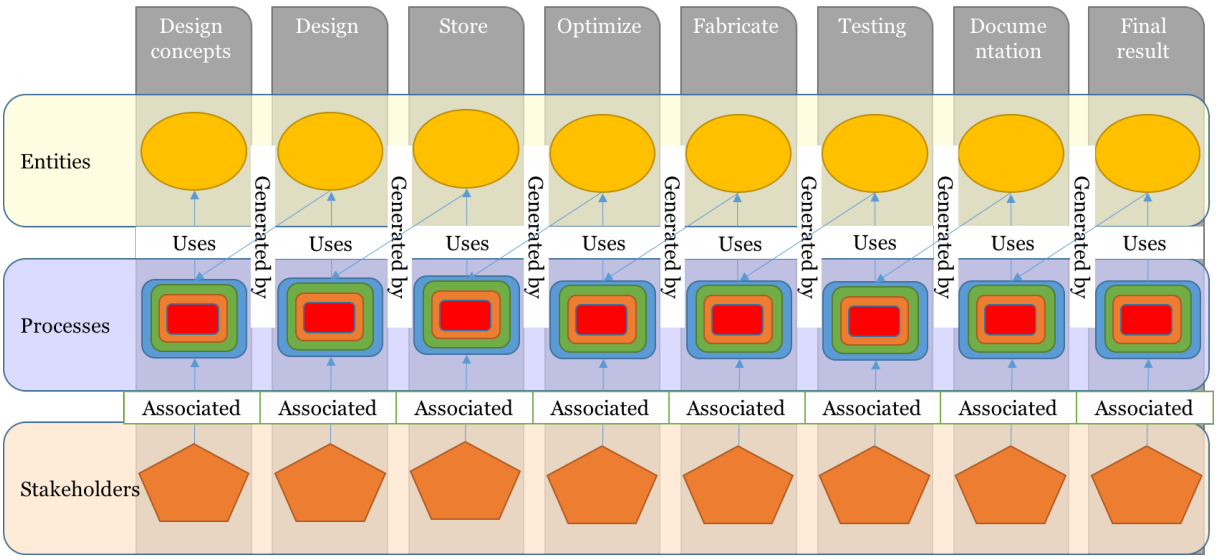



Figure 5.27: Reference architecture

**Generated by** An entity is always generated by an activity.

**Uses** An activity always uses entities to generate other entities.

**Invalidated by** A victim entity can only be violated through an attack process. Any entity linked to the victim entity are affected by the attack as well.

**Associated** An agent is always associated with an activity. An agent does not associate with an entity directly, but through an activity.

Figure 5.29 semantically describes the taxonomy using PROV-N data modelling Moreau, Luc and Missier (2013). The mapping identified the following relationships:

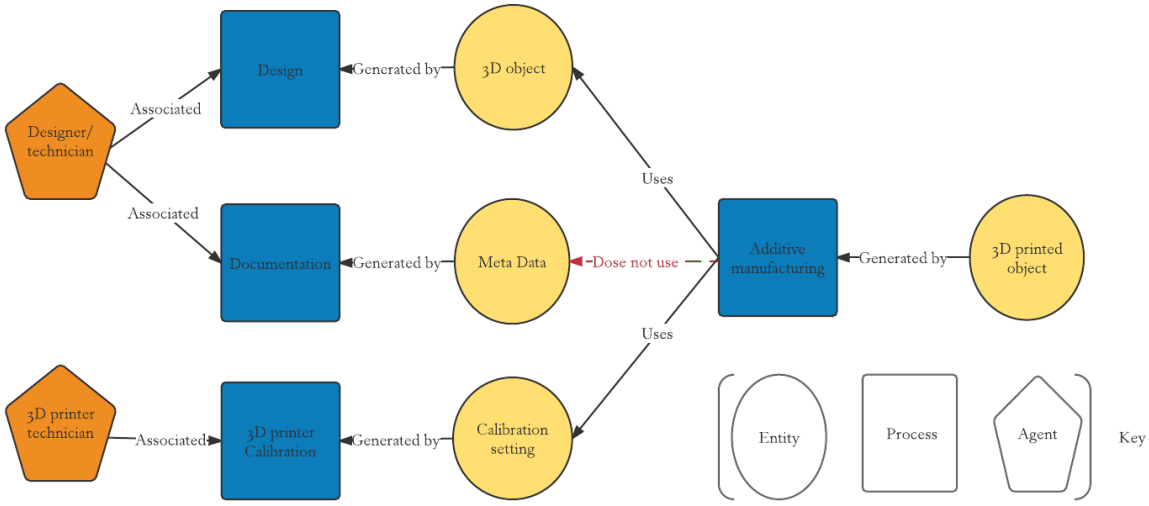



Figure 5.28: Cyber to physical taxonomy

Figure 5.29 semantically describes the taxonomy using PROV-N data modelling Moreau, Luc and Missier (2013). The mapping identified the following relationships:

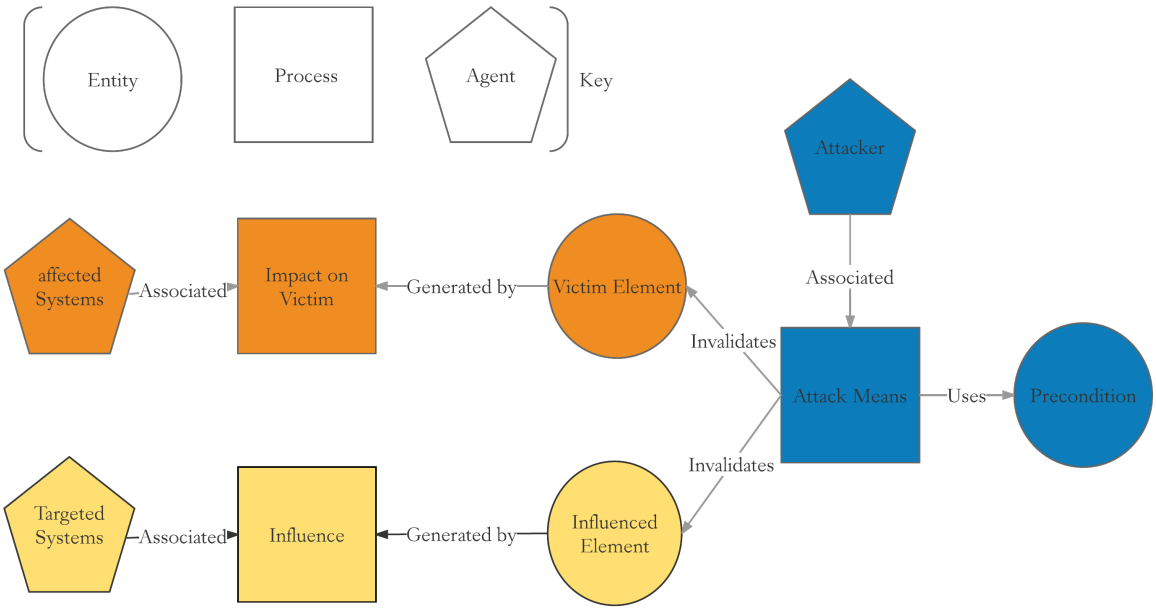



Figure 5.29: Cyber to physical taxonomy

## 5.7 Summary

The additive manufacturing infringements are scares and technology adoption rate is only starting to pickup in the recent years. The security, exchange, and authenticity, of 3D objects and 3D prints is an issue that has been receiving increased attention because of the disruptive effect of additive manufacturing. The chapter analysed three types of datasets, documented threats, CVE threats and hypothetical threat cases. The analysis served two purposes. The first, is building a unique threat model for additive manufacturing. The second, the cases are used in the research validation. The analysis is carried using Moreau, Luc and Missier (2013) provenance modelling [1]

[1] provenance.ecs.soton.ac.uk/validator/view/translator.html

# Chapter 6

# Initial Framework using GQM

> This work earlier established seven universal properties for security that will be used here as the platform to collect provenance information to prove who did what, where and when, why and how. Therefore, the objective is find a suitable set of components that covers the seven security properties.

This chapter addresses the second research objective which is: **"What are the components for the provenance AM framework properties?"** It starts by using the goal question metric approach to make an initial attempt at constructing this framework. The lessons learned from this will provide a list of components and metrics that can be presented to cyber security and additive manufacturing experts. The outline framework structure was published in (Fadhel et al., 2013a). The framework is composed of seven security properties (Accounting, Authentication, Authorisation, Availability, Confidentiality, Integrity, Non-repudiation). These security properties were investigated by the literature review in chapters 2 and 3, and analysed using threat analysis in chapter 4.

## 6.1 Building Framework v1.0 using GQM

The goal question metric approach Caldiera and Rombach (1994) guided the construction of framework version 1.0 using the requirement specification from chapter 4. This approach was used to make sure that nothing was overlooked for the framework design. The GQM used the seven security principles as goals for the method, and enabled the research to identify a comprehensive set of questions, metrics and measures. Similar work was carried out by (Islam and Falcarin, 2011), where the authors used GQM to refine security properties and metrics from an asset risk management point of view, which is similar to this work in that it has both digital and physical assets.

### 6.1.1 Accounting property

The goal is to establish accounting for additive manufacturing, taking the three items of interest (who did what, and when?). Figure 6.1 shows the GQM analysis for the accounting property.

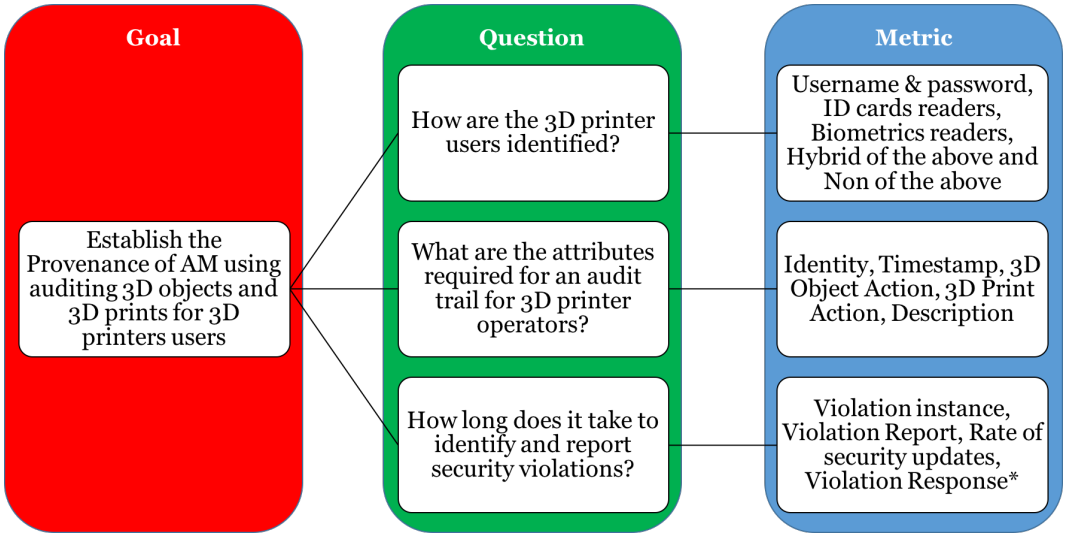



Figure 6.1: Goal Question Metric for accounting property [1]

Based on the analysis of the goal question metric approach, the work grouped each questions and its metrics into components. The following is the initial set for the accounting components.

**Identifying 3D printer users** : This component investigates the identity of digital content designer/provider so that action on 3D objects can be identified. This component is important because it will establish if there are any security identification polices in place.

**Audit trail** : This component investigates auditing of 3D printing services, such as who printed what and when? This component is important, as it will allow identification of actions associated with 3D printing services, such as 3D Design tools, 3D printing application, and 3D printing hardware.

**Security violations report** : This component investigates violation response time of security polices/Access control. Answering this question will assess response time to violation of security policies and procedures. The violation metric was later discarded because it is part of the discovery not the assessment process, and there is also reluctance in the disclosure of information.

[1] (Violation Response = Violation Report - Violation instance) The time difference between reporting a security violation and the time the violation occurred gives the Response to incident time. It is optimal to have Violation Response as small as possible.

### 6.1.2 Authentication property

The authentication property can refer to the authentication protocols used, authenticity of the data sources, or authenticity of information. This work intends to use the term holistically by exploring both digital and physical authentication processes that are used in additive manufacturing. The GQM is summarised in Figure 6.2.

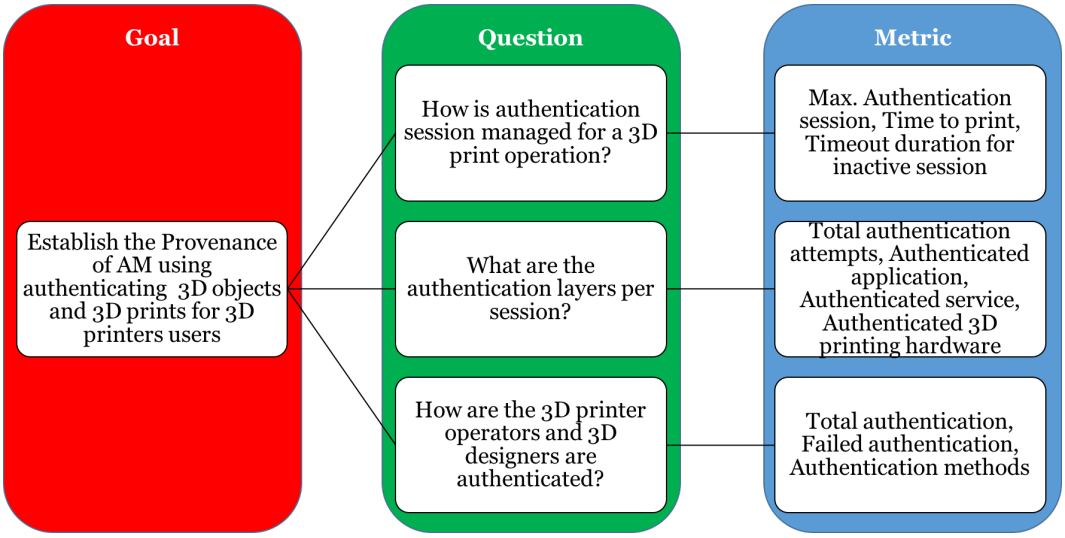



Figure 6.2: Goal Question Metric for authentication property

Based on the analysis of the goal question metric approach, the work grouped each questions and its metrics into components. The following is the initial set for the authentication components.

**Authentication session** : This component investigates session timing and timeout as it will enable the measurement of the authentication session.

**Authentication layers** : This component investigates authorisation levels as it will indicate available services and their total authentication requests.

**Authentication for 3D printer operators and 3D designers** : This component investigates the authenticity of digital content designer/provider as it will provide the basis for forming physical identity of a 3D printed object using inherited digital attributes.

### 6.1.3 Authorisation property

This property's main interest is authorisation for resources and confidential information. This property is unique as it is investigating authorisation access to physical resources

as well as digital resources. This property is also interested in documenting the physical access. The GQM is summarised in Figure 6.3.

Based on the analysis of the goal question metric approach, the work grouped each questions and its metrics into components. The following is the initial set for the authorisation components.

**Authorisation layers** : This component investigates the number of authorisation layers per session (Application layer, Service layer, Hardware layer) as it will enable the tailoring of security policies according to system size/scale.

**Available resources** : This component investigates the resources required by authorised personal/services. Answering this question will gauge the resource allocation for users with respect to size/scale that was determined in the previous question.

**Authorisation classes** : This component investigates the authorisation type in the organisation. Answering this question will provide organisation policy with needs, corresponding to authorisation type.

**Number of failed/successful authorisation attempts** : This component investigates the allocation of resources to authenticated users as it will provide an acceptance/rejection ratio.

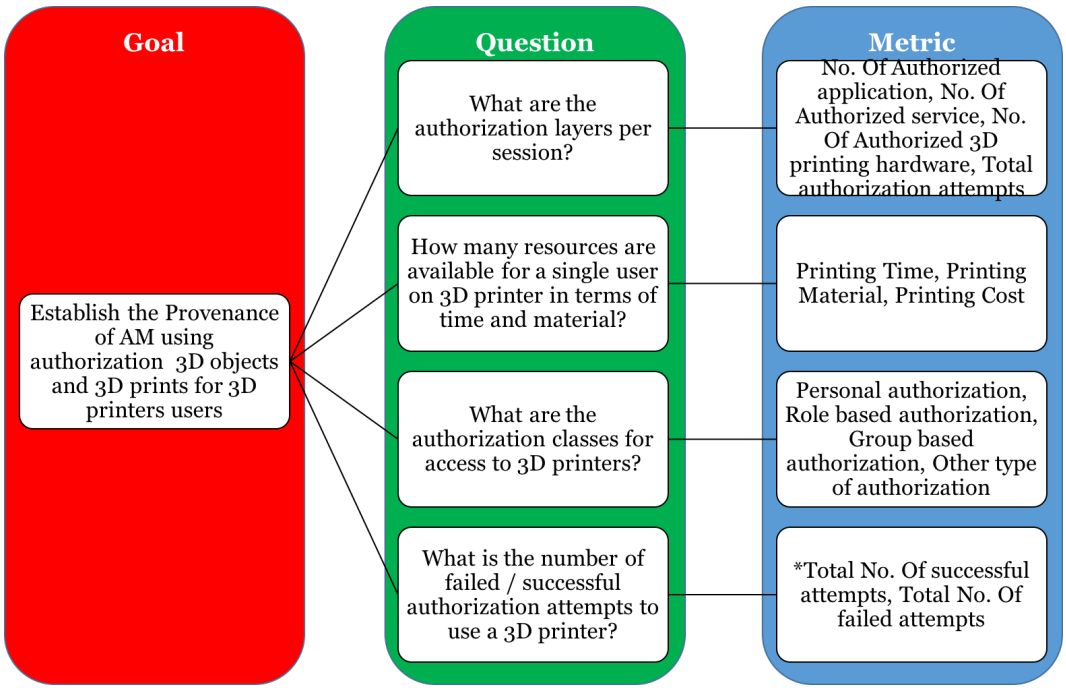



Figure 6.3: Goal Question Metric for authorisation property [2]

### 6.1.4 Availability property

The availability propertys main interests are the availability of resources, services, information, and recovery of failed services. This includes 3D printing resources and services as well. The GQM is summarised in Figure 6.4.

Based on the analysis of the goal question metric approach, the work grouped each questions and its metrics into components. The following is the initial set for the availably components.

**Available of 3D printer** : This component investigates the efficiency of time being used on 3D printers. Answering this question will reflect availability of services by utilisation of 3D printer time.

**Recovery of 3D printer** : This component investigates failure recovery time. Answering this question will reflect resilience of the system in recovering from failures.

**3D printing process failure points** : This questions where the failure of availability occurs. Is the failure in the transmission of information? Is the failure in the software or in the hardware?

**Trusted 3D objects** : This question reflects on the availability of information (in this case the information is a 3D printed object).

[2](Successful authentication = Total authentication - Failed authentication) Having successful and failed authorisation can give an indication of false acceptance and false rejection rates. (Total authentication attempts = failed attempts + successful attempts) The fail and success rate can provide a solid measure of printability of objects as some 3D objects fail in the printing process.

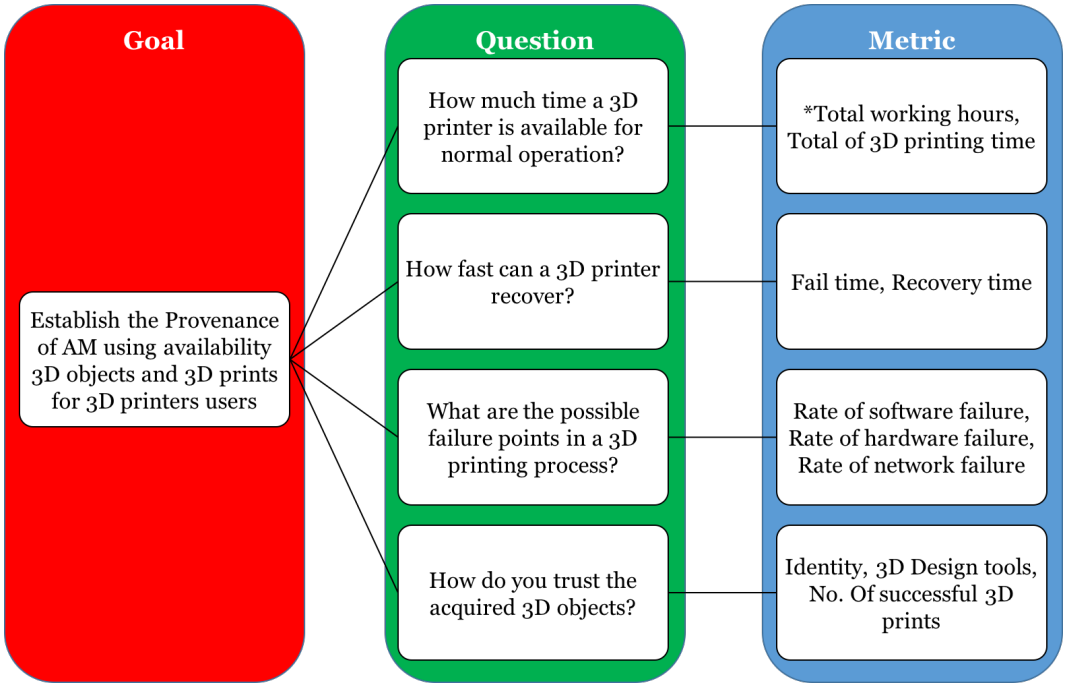



Figure 6.4: Goal Question Metric for availability property [3]

### 6.1.5 Confidentiality property

The confidentiality propertys main interests are disclosure of confidential information and the strength of the confidentiality measures. The GQM is summarised in Figure 6.5.

[3](Idle machine hours = Total working hours - total usage hours) It is optimal to keep this number as low as possible to use the 3D printer more efficiently. If the total working hours/total 3D print time = 1, then the service is being used for the whole time.

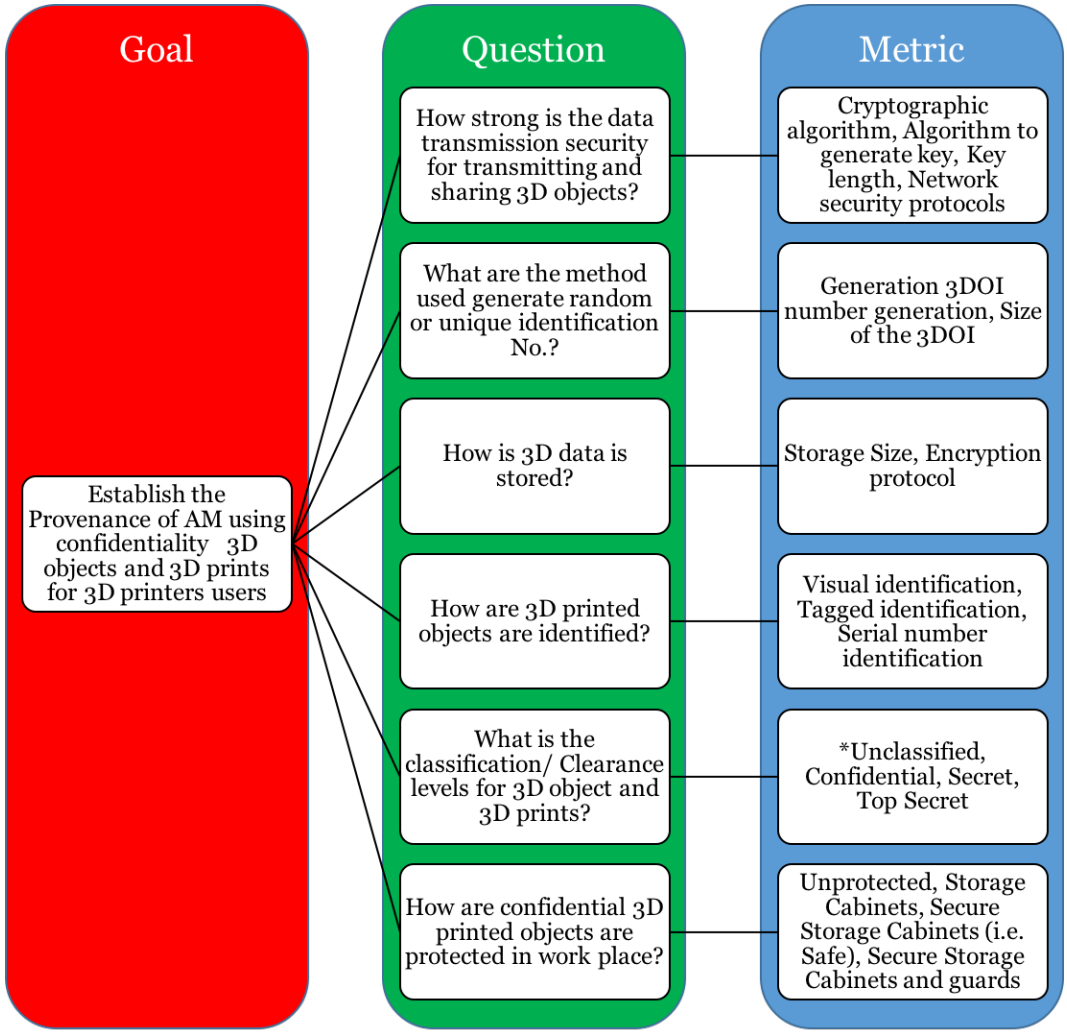



Figure 6.5: Goal Question Metric for confidentiality property [4]

Based on the analysis of the goal question metric approach, the work grouped each questions and its metrics into components. The following is the initial set for the confidentiality components.

**Security of transmitting and sharing 3D objects** : This question examines network security procedures used to carry 3D content.

**Unique identification Number** : This question examines the number generation of the 3D object identifier (3DOI) to be associated with 3D objects.

**3D object digital storage** : This component investigates the quality of storage to maintain information integrity during the 3D objects life cycle.

[4] In enterprise or academic settings, the variables can be referred to as: Public, Private, Special access, Embargoed.

**3D printed objects identification** : This component investigates the inspection of 3D printed objects to associate/identify them.

**Classification/Clearance levels for 3D objects and 3D prints** : This component investigates classification/clearance levels for personal, enterprise, legal, and governmental access to 3D objects and 3D prints.

**Securing 3D printed objects** : This question investigates the protection of 3D printed objects in the work place.

### 6.1.6 Integrity property

The integrity propertys main interests are data maintenance, information redundancy systems (i.e. backups), and secure disposal of information. The GQM is summarised in Figure 6.6.

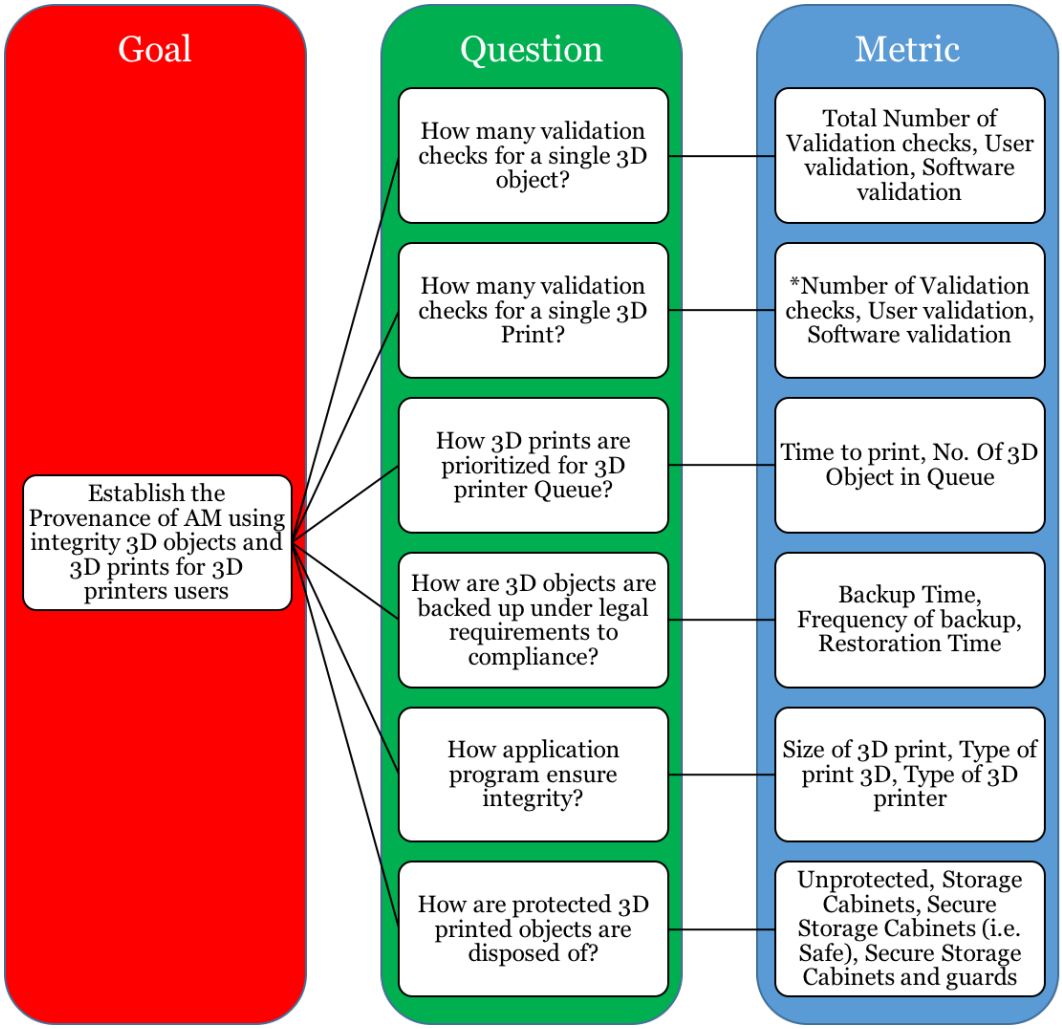



Figure 6.6: Goal Question Metric for integrity property [5]

Based on the analysis of the goal question metric approach, the work grouped each questions and its metrics into components. The following is the initial set for the integrity components.

**3D object validation checks** : This question examines the validity of the 3D object before printing. User validation refers to validation by the user that the object integrity is complete and there are no (gaps/breaks/holes) in the model, while software validation refers to the 3D printing software using 3D objects.

**3D Print validation checks** : This question examines the validity of the 3D object before printing. User validation refers to validation by the user that the object integrity will hold during the printing, while software validation refers to the object requirement in terms of material, type of printer, and type of object.

**3D printer Queue prioritisation** : This component investigates the efficacy of printing queues to present a clearer perspective of 3D printing availability.

**3D objects back up** : This component investigates the backup process to present a clearer perspective of 3D printing availability.

**Software integrity check** : This question addresses the integrity of printable 3D objects, as some objects require special conditions, which if met could result of higher availability of 3D prints.

**Secure disposal of 3D printed objects** : This component investigates the secure disposal of potentially confidential information.

### 6.1.7 Non-repudiation property

The non-repudiation propertys main interests are accuracy and consistency of the information in digital and physical form. The GQM is summarised in Figure 6.7.

[5]Number of physical Validation checks/User validation or Software validation, gives a strong validation and likewise for digital validation checks. The type of 3D printed object can be (Functional object or Non-functional object). *The main 3D printing technologies are Photo-polymerization (Resin), Granular Material Binding (Powder), Molten Polymer Deposition (ABS/PLA); the material is defined by the printing technology.

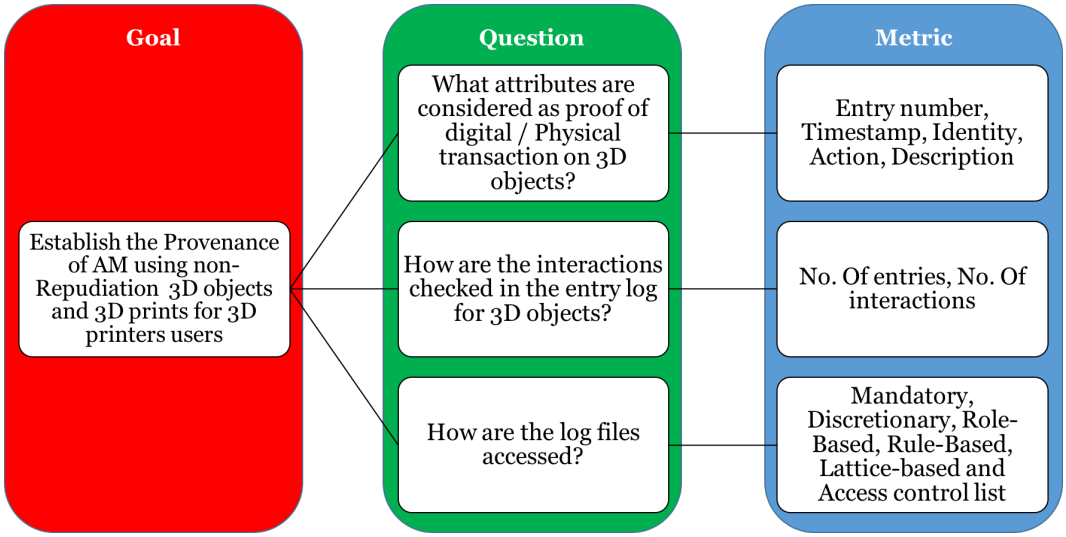



Figure 6.7: Goal Question Metric for non-repudiation property

Based on the analysis of the goal question metric approach, the work grouped each questions and its metrics into components. The following is the initial set for the non-repudiation components.

**Proof of digital/Physical transaction** : This question examines the attributes used to prove fraudulent attempts on 3D objects/3D beyond reasonable doubt.

**Logged interactions for 3D objects** : This component investigates how information is retrieved from the logs about the 3D objects/3D prints.

**Access to log files** : This question examines the access control procedures for log files.

## 6.2 Refinement of the GQM components

The goal question metric approach was a long and time-consuming process but the initial result showed that the task of building a holistic provenance framework for AM is feasible. The GQM analysis results are given in Appendix B, the components of which have been refined to produce a shortened and more accurate list. The refinement of the components in Table 6.1 was produced using the following processes:

**Re-Categorisation** of components under the seven security properties (Accounting, Authentication, Authorisation, Availability, Confidentiality, Integrity, Non-repudiation).

**Correlating** the final list of components with the properties definition so that they use the same vocabulary.

**Filtering** by breaking down components into independent measures.

**Refactoring** by grouping similar metrics together (semantically equivalent) into a new component.

**Replacing** and removing duplicate factors.

**Synthesising** new components from the remaining (ungrouped) metrics.

## 6.3 Summary

The framework presented the security properties needed to provide provenance, but did not describe the components nor how to measure them. Following publication of the outline framework, work investigated the components of the framework, using the goal question metric approach Caldiera and Rombach (1994) from which framework version 1.0 was constructed describing the components and the metrics. The 29 components each had a set of metrics, which are listed in A. The GQM results were then refined and reduced to 19 components Table 6.2.

Table 6.1: GQM Refinement Process

| **Properties** | **Before Refinement** | **Refinement Process** | **After Refinement** |
|---|---|---|---|
| Accounting | Identifying 3D printer users | Refactoring | Accounting Identity |
| | Audit trail | Refactoring | Accounting Protocol |
| | Security violations report | Synthesizing | Accounting Timestamp |
| Authentication | Authentication session | Filtering | Strength of authentication protocol |
| | Authentication layers | Filtering | Authenticity of data source |
| | Authentication for 3D printer operators and 3D designers | Filtering | Authenticity of information |
| Authorisation | Available resources | Re-categorisation | Authorisation for resources |
| | Authorisation layers | | |
| | Authorisation classes | Synthesising | Authorisation of confidential information |
| | Number of failed / successful authorisation attempts | | |
| Availability | Available of 3D printer | Correlating | Availability of resources |
| | Trusted 3D objects | Correlating | Availability of information |
| | 3D printing process failure points | Correlating | Availability of services |
| | Recovery of 3D printer | Correlating | Recovery rate of failed resources |
| Confident-iality | Security of transmitting and sharing 3D objects | Correlating | Disclosure of confidential information |
| | Unique identification No. | Re-categorisation | |
| | 3D object digital storage | Re-categorisation | |
| | 3D printed objects identification | Refactoring | Strength of confidentiality measures |
| | Classification/ Clearance levels for 3D object and 3D prints | | |
| | Securing 3D printed objects | | |
| Integrity | 3D object validation checks | Refactoring | Data Maintenance |
| | 3D Print validation checks | | |
| | Secure disposal of 3D printed objects | Correlating | Secure disposal |
| | 3D printer Queue prioritisation | Re-categorisation | |
| | Software integrity check | Replacing | Data backup |
| | 3D objects back up | Correlating | |
| Non-Repudiation | Proof of digital / Physical transaction | Correlating | Data accuracy |
| | Logged interactions for 3D objects | Synthesising | Data consistency |
| | Access to log files | | |

Table 6.2: Refined Components

| Properties | After refinement |
|---|---|
| Accounting | Accounting Identity |
| | Accounting Protocol |
| | Accounting Timestamp |
| Authentication | Strength of authentication protocol |
| | Authenticity of data source |
| | Authenticity of information |
| Authorization | Authorization for resources |
| | Authorization of confidential information |
| Availability | Availability of resources |
| | Availability of information |
| | Availability of services |
| | Recovery rate of failed resources |
| Confidentiality | Disclosure of confidential information |
| | Strength of confidentiality measures |
| Integrity | Data Maintenance |
| | Secure disposal |
| | Data backup |
| Non-Repudiation | Data accuracy |
| | Data consistency |

# Chapter 7

# First Expert Review

This chapter carries on the work from chapter 6 to answer research question two, and builds on the refinement of the goal question metric approach (GQM). The refined components were presented to 16 experts to confirm the components were necessary to provide provenance for printing 3D objects. The results from the first expert review are presented in this chapter, as well as the ranking of the properties and components based on the quantitive data from the expert review of the provenance framework.

## 7.1 First expert review - Component confirmation

Previous activity investigated the components required to establish provenance for additive manufacturing, which resulted in 19 components that provide coverage of the information security principles. These 19 components were reviewed by 16 experts, which involved gathering both qualitative and quantitative data. This step was necessary to help build the metrics for the provenance framework. The metrics were based on the initial version proposed in the GQM analysis as shown in chapter 6.

Participants in the expert review are lecturers in computer science, computer security and cryptography, and postgraduate researchers in the same fields. Seven were from the University of Surrey, being part of the Cryptography Group. Nine from the University of southampton from Electronic and Software Systems GroupThe experts were first given a seminar about 3D printing and then asked to comment within focus groups (a group of 3 and another of 4) after the seminar, senior experts were interviewed individually.

The qualitative data was captured from open-ended questions, and on their response to fixed questions. The expert participants were also asked their opinion on the suitability of each component. The expert review set out to:

- Confirm the components in the framework.

- Record findings of discussion in the expert review to uncover any overlooked aspects in the components of the framework.

## 7.2 Quantitative Results of the First Expert Review

A brief presentation was first given about additive manufacturing and the participants were then given a questionnaire of 19 questions. Qualitative data was collected using a 5-point Likert scale from, strongly disagreed to strongly agree (see Appendix 2). The quantitative data was collated, and analysed against a mean rating of 3, representing a natural answer, as presented in Table 7.1. All the components were statistically significant since all the power calculation for sigma were less than 0.5 for the type one error, therefore confirming that the refined GQM components of the framework are correct.

The power calculation used, implemented a one sample one tailed t-test to show the difference from the constant. The effect size type was large, therefore the effect size was 0.8. Type I error probability was 0.05, and type II was 0.2, which gives a power value of 0.8

Table 7.1: First Expert Review results for component confirmation

| **Properties** | **Components** | **Mean** | **Mean Diff** | **Std. Dev** | **Sig.(2-tailed)** |
|---|---|---|---|---|---|
| Accounting | Accounting Identity | 4.63 | 1.63 | 0.5 | <0.001 |
| | Accounting Protocol | 4.25 | 1.25 | 0.93 | <0.001 |
| | Accounting Timestamp | 4.13 | 1.13 | 0.81 | <0.001 |
| Authentication | Strength of authentication protocol | 4.19 | 1.19 | 0.75 | <0.001 |
| | Authenticity of data source | 4.31 | 1.31 | 0.7 | <0.001 |
| | Authenticity of information | 4.19 | 1.19 | 0.91 | <0.001 |
| Authorisation | Authorisation for resources | 3.94 | 0.94 | 0.85 | 0.001 |
| | Authorisation of confidential information | 4.38 | 1.38 | 0.62 | <0.001 |
| Availability | Availability of resources | 3.94 | 0.94 | 0.85 | 0.001 |
| | Availability of information | 4.06 | 1.06 | 0.93 | <0.001 |
| | Availability of services | 4.06 | 1.06 | 0.85 | <0.001 |
| | Recovery rate of failed resources | 3.94 | 0.94 | 0.85 | 0.001 |
| Confidentiality | Disclosure of confidential information | 4.06 | 1.06 | 1 | 0.001 |
| | Strength of confidentiality measures. | 4.13 | 1.13 | 0.72 | <0.001 |
| Integrity | Data Maintenance | 4.13 | 1.13 | 0.72 | <0.001 |
| | Secure disposal | 4 | 1 | 0.82 | <0.001 |
| | Data backup | 4.38 | 1.38 | 0.81 | <0.001 |
| Non-Repudiation | Data accuracy | 4.13 | 1.13 | 0.72 | <0.001 |
| | Data consistency | 4.06 | 1.06 | 0.77 | <0.001 |

## 7.3 Qualitative Results of the First Expert Review

The purpose of the first expert review was to confirm the components of the framework. The experts were presented with the background to the research gap as well as some security definitions. The experts were then asked to complete a task sheet and questioned on their responses. The experts' responses were anonymised, digitised and summarised into several categories.

The expert responses were themed around three points of discussion.

### 7.3.1 The Provenance Framework

The first set of comments were regarding the nature of the provenance of 3D objects and 3D prints, whether using the framework will be to secure 3D objects or using 3D objects to hide sensitive information.

> "What is the provenance for, the object or the message using the object just as a carrier?" (**Expert A**)

As discussed in chapter 3, there is an array of security solutions for 3D objects and 3D prints that fit some threat scenarios with varying degrees of monetary value, dependant on the value of intellectual property or trade secret. When asked about the value of the 3D object vs. the 3D print, one comment was

> "If the information about the 3D object is more valuable than the 3D print, then the security methods fall under the steganography definition. However, if the 3D print is as important as the 3D object than the security methods fall under the watermarking umbrella." (**Expert B**)

This is why the 3DOI is proposed as part of the framework and this 3D object identifier can be added to the physical 3D print. However, the 3DOI as part of the framework cannot be properly evaluated until the entire framework is validated, which lies beyond the scope of the current work, and this engendered the comment

> "The disadvantages for this framework are unclear." (**Expert C**)

In the opinion of the experts, this work is completely novel and there is nothing to compare it with.

### 7.3.2 The Provenance Framework Properties

The comments about the seven properties of the framework are as follows. **Expert D** questioned whether digital signing is a good measure for digital integrity.

> "Digital signing should be a measure for integrity." (Expert D)

A good example of this is IEEE Publishing who digitally sign publications to confirm the authenticity of publication. Additionally, IEEE publications store two copies of their digital papers, one that is text searchable and the second an image version. When they want to check for authenticity, they check both to see if they match. Arguably, even if

digital signing was used to confirm integrity, it cannot be used to reflect on the physical integrity of a 3D printed object.

**Expert E** commented on the usage of confidentiality and authorisation properties in the framework.

> "The confidentiality and authorisation are not so different so why have both." (Expert E)

The two properties are included in the framework because they have different relationships. Confidentiality is associated with the disclosure and protection mechanisms of information, while Authorisation is an associated resource rather than information. Both can be explained by the term *access*. For example, if you have a shared folder on your network, you will first need to request authorisation before you can access it. When you have been authorised to open the folder, you can create, read, or edit confidential information. Therefore, you can choose what to disclose to your colleagues and the network administrator decides who can access it. This discussion leads on to **Expert F** who questioned why there was:

> "No mention of access control policies." (Expert F)

Access control is not mentioned in the framework because it relates to authorised to view, edit or delete confidential information. Although it was initially proposed as a metric for non-repudiation, it was later removed as redundant information during the refine stage. **Expert G** discussed the importance of the properties and whether some are more important than others. If some are more important than others, is it because of inherited dependencies? Is there an order of priority of components?

> "The authentication property is more important than non-repudiation because without authentication there is no non-repudiation." (Expert G)

Another expert suggested that some properties are nested. For example, authorisation precedes confidentially because one authorises for confidential information.

> "A ranking of the properties is important to show these dependencies as well as nested properties." (Expert H)

Because of comments by **Expert G and Expert H**, an analysis was carried on the principles, properties and components using the quantitative data collected in the expert review. This found that ranking the proposed security properties to provide provenance to 3D objects and 3D prints gives a realistic reflection of the needs of the additive

manufacturing scene for security solutions. Such a ranking will uncover where the users of 3D printers are leaning towards and where this technology is trending in the future.

Table 7.2: Principles and Properties Ranking

| **Principles** | **Mean** | **Principles** | **Mean** | **Principles** | **Mean** |
|---|---|---|---|---|---|
| Information Transmission | 4.24 | Information Authenticity | 4.16 | Information Security | 4.09 |
| Accounting | 4.33 | Authentication | 4.23 | Integrity | 4.17 |
| Authentication | 4.23 | Integrity | 4.17 | Confidentiality | 4.09 |
| Authorization | 4.16 | Non Repudiation | 4.09 | Availability | 4 |

Table 7.2 shows that the ranking will be geared towards one or more of the following: exchange and sharing of 3D objects first, ownership and 3D object economy second, and information security measures for 3D objects and 3D prints third. These results agree with emerging market technologies for additive manufacturing, as a number of solutions focus on protecting the transmission of 3D objects for the purpose of 3D printing.

1. Accounting (Mean = 4.33)
2. Authentication (Mean = 4.23)
3. Integrity (Mean = 4.17)
4. Authorisation (Mean = 4.16)
5. Confidentiality (Mean = 4.09)
6. Non-Repudiation (Mean = 4.09)
7. Availability (Mean = 4.00)

Accounting has the highest priority as it is probably the most important to achieve provenance of 3D objects and 3D prints because of the difficulty of accounting for changes from digital to physical and back. Since Accounting precedes Authentication in importance, the ranking also conformed to the security standards for identification, because identification is a passive process while authentication is an active process. Confidentiality and Non-repudiation have the same score, which is interesting because it reflects **Expert G**'s comment that you cannot have one without the other.

### 7.3.3 Components of Provenance Framework Properties

One expert commented on the redundancy of the components of a property in the framework, as they may have already been covered under other properties:

> "Under the Integrity metric, secure disposal was thought not to be a requirement since there already exists the Accountability and Authorisation properties and their metrics." (Expert I)

It is true that Accountability and Authorisation are included in the framework. However, the component is focused on disposal of information to maintain integrity of the 3D objects, as old versions could conflict with new changes. Secondly, it must be done in a secure manner, where accountability and authorisation will hold sway.

The last point made by the experts was regarding the possible customisation of the framework to suit different customer needs.

> "The metrics and measurement should be tailored to a specific solution or a scenario that is based on the customer needs." (Expert J)

The properties and components are comprehensive and have covered the provenance needs for 3D objects and 3D prints in the framework. The framework, once completed, can be customised based on the relationships that the organisation has with information when using additive manufacturing. This is why this work has dedicated Chapter 5 to model the threats to additive manufacturing.

## 7.4 Component Priority

The component ranking showing the oder of importance will help prioritise the order of the questions as they also show the order of importance for the second expert review for better data collection, as shown in Table 7.3.

The purpose of the component confirmation was to prove that the components are correct using statistical data and showing their statistical significance. The ranking (Up, Same and Down) shows the reordered components. The ranking will help restructure the benchmarking process of assessing the security of additive manufacturing process as well as addressing the comment by **Expert G**.

## 7.5 Summary

The object of the expert review was to confirm the refined 19 components from chapter 6 are the right components for ensuring provenance for 3D printed objects. The experts examined the components and scored them by importance on a scale of 1 to 5, 3 being neutral. The experts were then asked to justify the score they gave for each component to gather the qualitative data.

Table 7.3: Components Ranked by Priority

| **Components (original)** | **Mean AVG** | **Ranking** | **Components (Ranked)** | **MeanAVG** |
|---|---|---|---|---|
| Accounting | | | | |
| Accounting Identity | 3.5 | Down | Accounting Protocol | 3.93 |
| Accounting Protocol | 3.93 | Up | Accounting Timestamp | 3.81 |
| Accounting Timestamp | 3.81 | Up | Accounting Identity | 3.5 |
| Authentication | | | | |
| Strength of authentication protocol | 3.75 | Down | Authenticity of information | 3.91 |
| Authenticity of data source | 3.7 | Down | Strength of authentication protocol | 3.75 |
| Authenticity of information | 3.91 | Up | Authenticity of data source | 3.7 |
| Authorization | | | | |
| Authorisation for resources | 3.85 | Same | Authorisation for resources | 3.85 |
| Authorization of confidential information | 3.62 | Same | Authorization of confidential information | 3.62 |
| Availability | | | | |
| Availability of resources | 3.85 | Down | Availability of information | 3.93 |
| Availability of information | 3.93 | Up | Availability of resources | 3.85 |
| Availability of services | 3.85 | Same | Availability of services | 3.85 |
| Recovery rate of failed resources | 3.85 | Same | Recovery rate of failed resources | 3.85 |
| Confidentiality | | | | |
| Disclosure of confidential information | 4 | Same | Disclosure of confidential information | 4 |
| Strength of confidentiality measures. | 3.72 | Same | Strength of confidentiality measures. | 3.72 |
| Integrity | | | | |
| Data Maintenance | 3.72 | Down | Secure disposal | 3.82 |
| Secure disposal | | Up | Data backup | 3.81 |
| Data backup | 3.81 | Up | Data Maintenance | 3.72 |
| Non-Repudiation | | | | |
| Data accuracy | 3.72 | Down | Data consistency | 3.77 |
| Data consistency | 3.77 | Up | Data accuracy | 3.72 |

The result confirmed the refined components, as all scored an average above 3.5. Therefore, the components proposed for the framework was sufficient coverage for providing provenance of 3D objects. Additionally, the components were ranked by importance to show where the current security trends for 3D objects are headed. It showed that sharing of 3D objects and 3D prints will be important in the near future.

The ranking showed that the security of transmitted information was the most important aspect of the system, according to the experts. Next came the Authenticity of the information, and then general information security. This ranking also helped to predict future trends in security procedures protecting 3D content. This ranking is shown in Table 7.3. Finally, the expert review prepared for the second expert review to confirm the metrics to measure the components. In summary, the framework was confirmed using an expert review preceded by these preparation stages:

**First stage** an initial set of components was proposed using GQM as illustrated in Framework version 1.0 in Chapter 6;

**Second stage** refine the initial components by the using six processes listed in section 6.2.

**Third stage** conducting the first expert review to confirm the components through interviews and focus groups to gather quantitative and qualitative data.

**Conclusion** A confirmed set of components for the framework.

Therefore, this research concludes that these components and the framework are correct and can be used to achieve a successful transition of provenance for 3D printed objects.

# Chapter 8

# Second Expert Review

This chapter addresses the third research objective which is:

> From the confirmed components, appropriate metrics will be proposed to complete the framework. These will be confirmed using expert interviews.

The objective is aimed at answering the third research question **"What metrics are required to measure the components of the provenance AM framework properties?"**.

A second expert review was conducted to confirm the metrics put forward to measure the components. The metrics are grouped by three principles: information transmission, information security, and information authenticity. The expert review was conducted through focus groups and interviews, using mixed methods to gather qualitative and quantitative results and so maximise the benefit.

In the following section the properties of the metric are listed by principle in three-sub sections: Component, Metric, and (Measurement and Scale). The findings and results from the second expert review on the metrics are in the form of qualitative and quantitative data. The expert comments are anonymised.

## 8.1 Information Transmission Principle

This principle depends on three properties: **authentication, authorisation and accounting**.

### 8.1.1 Authentication

The authentication property looks at three components, each of which has a two-dimensional metric to cover as much as possible of the property.

**The strength of authentication protocol**: The authenticity of the identity metric for the strength of the authentication protocol component is **How strong are the authentication methods for 3D objects and 3D prints?** It is a two-dimensional metric that answers

- **"What type of objects are created?"**
- **"How are the users who created them authenticated?"**

A number of experts commented on the Authenticity of identity in the light of the proposed metrics, the first being that the strength of the authentication protocol is subject to the importance of the information being protected.

> "The strength of the authentication protocol for exchanging 3D prints is completely dependent on the value of the object and material". (Authentication-Expert 1)

Some experts viewed the component as more important in the case of exchange of 3D objects and 3D prints.

> "The authentication strength is not a very important factor. However, the existence of the authentication process is necessary for the exchange of 3D prints." (Authentication-Expert 2)

Although experts said that this component is essential to the provenance of 3D printed objects, they were concerned with applying digital authentication measures to physical objects.

> "The authentication process for 3D prints is questionable, because digital authentication can be performed on digital objects but we are unsure how it can be applied to 3D prints". (Authentication-Expert 3)

The summary of the previous comments is that the strength of the authentication is an important factor in the provenance procedure. However, there must be a balance between strength of authentication and availability of information, and that balance is subject to the importance of information and the state of the technology, in covering provenance for digital and physical objects, with greater emphasis on 3D printed objects.

The experts commented on the first item in the metric, which is the creation of 3D objects.

> "There shouldn't be any limitation on the creation of digital content". (Authentication-Expert 4)

This reflects their concern with development and implantation of security technologies for 3D objects, as it could have a negative impact on the creation of 3D content which could hinder the creative spirit. However, this framework is general and can be modified to adapt to organisational needs, since proposing authentication for creating 3D objects does not necessarily provide security, but providing Strong authentication procedures does.

**The authenticity of data source**: The metric for the authenticity of the data source component is **What type of entity access is used to verify identity? On what level is access granted?** This is a two-fold metric that asks:

- **"What type of entities are authenticated inside the organisation?"**
- **"How much information regarding authenticated actions are recorded about these entities?"**

The second metric in the expert review was for the authenticity of the data source component.

> "The importance of authenticity of data source can change, based on the role (sender or recipient)". (Authentication-Expert 5)

This shows that the importance of items can shift, based on the roles, sender or recipient, which is a critical comment on this component and will be addressed in a later section. One comment was that the (user level access) component was not necessary.

> "This item is not required as it is covered in the next item (Users using Services access level) because all users are associated with services" and "This item is not needed to verify authenticity". (Authentication-Expert 6)

However, these comments do not address individuals or organisations that have no 3D printing services or do commerce on 3D objects and 3D prints. Finally, the (Domain level access (Highest access level)) emphasises this item being very important in two ways. First, sharing information is important as a strong factor in promoting this technology.

> "This item is not needed as sharing should be limited to people working on the 3D objects in a secure system". (Authentication-Expert 6)

Secondly, a security expert said that this item is not needed for sharing of 3D objects as the exchange could be limited only to involved parties.

> "This item is critical as all information should be open to public for freedom of information". (Authentication-Expert 7)

However, the statistical data implies that the presence of the Domain level access provides a fuller and more complete metric, as shown in the results of confirmation, even if their results were low. However, the type one error of $p < 0.001$ was well below the threshold of 0.05.

**The authenticity of information**: The metric for the authenticity of information component is **Upon examination of 3D object or 3D print, can you tell if changes occurred to the object if the object was not in its native state? At what level is access granted?** This is a two-fold metric that asks:

- **"What type of objects are handled by the organisation?"**
- **"How useable is the object for functional objects, and how recoverable for non-functional objects?"**

The third metric in the expert review was for the authenticity of information component. The expert review expanded on the initial assumptions on some items in this metric; the following assumptions are included in the metric.

1. All 3D objects and 3D prints are confidential, differing only in their classification of confidential, as this could vary from being top secret to unclassified.
2. 3D objects and 3D prints can also mean the origin of the 3D object and 3D print.

These assumptions are derived from the following comments:

> "Confidential 3D objects and confidential 3D prints should be added to the items in the metric" and "Origin of the 3D object and 3D print should be included as it can emphasise the value of the object". (Authentication-Expert 8)

The expert review revealed the importance of the documentation of the type and extent of damage to 3D objects and 3D prints as it can reflect on the best course for restoration, and is also a good measure of printability by a 3D printer.

> "Information such as type of damage is important as it can help in the process of information recovery" and "Information such as type of damage is important as it is a good reflection of printability of a 3D object, because content providers can provide a measure of success for published 3D content". (Authentication-Expert 9)

The expert review also revealed possible future work as it uncovered a need in 3D printing technology.

> "Value analysis method for 3D objects is an overlooked area of study as it can show the importance of 3D objects/3D prints and damaged 3D objects/3D prints, as replaceable/damaged items could potentially have important intellectual property". (Authentication-Expert 10)

**Statistical data for authorisation in the second expert review**: The statistical data in tables Table 8.1, Table 8.2, and Table 8.3, confirms the proposed metrics for the above components, as none of the items or scale in the metrics have a type one error of $p > 0.05$, as shown in the tables under Sig. (2-tailed). The test for the metric was based on 4 points on a Likert scale, therefore the mean was 2, the number of participants was *N*, the Mean was the average on a scale of 4, the mean difference is the average above the mean of 2, standard deviation from the mean and Sig. (2-tailed) stands for type one error.

Table 8.1: Expert review for authenticity of identity metric

| Test Value for the statistical mean = 2 | | | | | | |
|---|---|---|---|---|---|---|
| **Measure** | **Items** | **N** | **Mean** | **Mean Diff.** | **Std. Dev.** | **Sig. (2-tailed)** |
| | Creating 3D objects | 12 | 3.33 | 1.33 | 0.65 | <0.001 |
| | Exchange 3D Objects | 12 | 3.67 | 1.67 | 0.49 | <0.001 |
| | Printing 3D objects | 12 | 3.42 | 1.42 | 0.52 | <0.001 |
| | Exchange 3D prints | 12 | 3.08 | 1.08 | 0.67 | <0.001 |
| Scale | | 12 | 3.25 | 1.25 | 0.45 | <0.001 |

Table 8.1 shows that the lowest two values are (Exchange 3D prints) and (Scale), having mean differences of 1.08 and 1.25 respectively. The (Exchange 3D prints) item had a low score because some experts wondered how this process could be authenticated. Others equated it to the loan procedures from libraries or stores. The type one error was below 0.5 and it therefore remained in the metric. The score of 1.25 for (Scale) resulted from the experts having some comments on the scales, as shown in in the next section.

Table 8.2: Expert review for authenticity Data Source metric

| Test Value for the statistical mean = 2 | | | | | | |
|---|---|---|---|---|---|---|
| **Measure** | **Items** | **N** | **Mean** | **Mean Diff.** | **Std. Dev.** | **Sig. (2-tailed)** |
| | Users level access | 12 | 3.42 | 1.42 | 0.79 | <0.001 |
| | Users using Services access level | 12 | 3.67 | 1.67 | 0.49 | <0.001 |
| | Group level access | 12 | 3.5 | 1.5 | 0.52 | <0.001 |
| | Sub-domain level access | 12 | 3.5 | 1.5 | 0.52 | <0.001 |
| | Domain level access | 12 | 3.5 | 1.5 | 0.67 | <0.001 |
| Scale | | 12 | 3.25 | 1.25 | 0.45 | <0.001 |

Table 8.2 shows that the lowest two values are for (Users level access) and (Scale), having mean differences of 1.42 and 1.25 respectively. The score of 1.42 for (Users level access) was because some experts believed they did need to know who extracted the information on a user level, while others did not want to know, since they preferred open access. However, the presence of the (Users level access) item provides a fuller and more complete metric, as shown in the results of confirmation. Even if their results were low, the type one error of $p < 0.001$ was well below the type one threshold of 0.5. The score of 1.25 for (Scale) resulted from the experts having some comments on the scales, as shown in the next section.

Table 8.3: Expert review for authenticity of information metric

| Test Value for the statistical mean = 2 | | | | | | |
|---|---|---|---|---|---|---|
| **Measure** | **Items** | **N** | **Mean** | **Mean Diff.** | **Std. Dev.** | **Sig. (2-tailed)** |
| | 3D Objects | 12 | 3.42 | 1.42 | 0.52 | <0.001 |
| | Damaged 3D objects | 12 | 3.25 | 1.25 | 0.45 | <0.001 |
| | 3D Prints | 12 | 3.17 | 1.17 | 0.39 | <0.001 |
| | Damaged 3D print | 12 | 3.17 | 1.17 | 0.39 | <0.001 |
| Scale | | 12 | 3.25 | 1.25 | 0.62 | <0.001 |

Table 8.3 shows that the lowest two values are for (3D Prints) and (Damaged 3D Prints), having a mean difference of 1.17 for both. This is concerned with tracking authenticity for 3D prints and tracking damaged 3D prints, as previously commented on.

**Refined metric for authenticity of identity**: The metric for authenticity of identity has been refined using the expert review comments by making three modifications to the metrics, as shown in Table 8.4.

- No authentication protocol is added to the top of the scale, to change it from (Something you know, Something you have, Something you are, Hybrid of two or Hybrid of three) to (No authentication, protocol, Secure hardware, Something you know, Something you have, Something you are, Hybrid of two or Hybrid of three). Basically mean how many factor authentication the assessed uses.
- Digital certificates and secure hardware is included for services (not users) so this will also be added to the scale as secure hardware.
- Licensing 3D objects and 3D prints is added to the metric to cover licensing procedures.

Table 8.4: Refined metric and measure for strength of authentication protocol

| Component: Authenticity of identity "Refers to the strength of authentication protocol used to secure 3D objects and a 3D printed object." | |
|---|---|
| Metric: How strong are the authentication methods for 3D objects and 3D prints? | |
| **Measure item** | **Scale** |
| Creating 3D objects | No authentication protocol |
| Licencing 3D object | Something you know |
| Exchange 3D Objects | Something you have |
| Printing 3D objects | Something you are |
| Licencing 3D prints | Hybrid of two or Hybrid of three |
| Exchange 3D prints | |

**Refined metric for the authenticity of data source**: The metric for the authenticity of data source has been refined using the expert review comments by making three modifications to the metric, as shown in Table 8.5.

- More is needed to explain that not all services are in one system and not all services are digital services.
- The scale seems binary between (Rarely, sometimes, most of the time) meaning it is not adequate and (All the time) which is adequate.
- The Scale should change from (Rarely, Sometimes, Most of the time, All the time) to (Never 0%, sometimes 01%-49%, most of the time 50%-99%, all the time 100%).

Table 8.5: Refined metric and measure for authenticity of data source

<table>
<tr><td colspan="2">Component: Authenticity of source identity “Refers to the authenticity of data source (i.e.: museums, universities or users) of 3D objects and a 3D printed object.”</td></tr>
<tr><td colspan="2">Metric: What is the type of allowed entity access is used to verify identity? On what level access is granted?</td></tr>
<tr><td>Measure item</td><td>Scale</td></tr>
<tr><td>Users level access</td><td rowspan="5">No information is recorded 0%<br>Some information is recorded 01%-49%<br>Most information is recorded 50%-99%<br>Information is recorded all the time 100%</td></tr>
<tr><td>Users using Services access level (i.e.: 3D printing users, computing resources users)</td></tr>
<tr><td>Group level access</td></tr>
<tr><td>Sub-domain level access</td></tr>
<tr><td>Domain level access (Highest access level)</td></tr>
</table>

**Refined metric for the authenticity of information**: The metric for authenticity of information has been refined using the expert review comment by making four modifications to the metric, as show in Table 8.6.

- The scale should change from (Identifiable, Recoverable, Partially recoverable, Unidentifiable) to (Unrecoverable 0%, Partially recoverable 01%-49%, Recoverable 50%-99%, Acceptable 100%) for non-functional objects.
- The scale should change from (Identifiable, Recoverable, Partially recoverable, Unidentifiable) to (Unusable 0%, Mostly unusable 01%-49%, Mostly usable 50%-99%, Usable 100%) for functional objects.
- Partially Recoverable should provide a range of recoverability.
- The Scale should be based on usability percentages for functional objects.

Table 8.6: Refined metric and measure for authenticity of information

| Components: Authenticity of information ?Refers to the authenticity of information (i.e.: the object is genuine) of 3D objects and a 3D printed object.? | | |
|---|---|---|
| Metric: Upon examination of 3D digital object or 3D printed object can you tell if changes occurred to the object if the object was not in its native state? | | |
| **Measure item** | **Functional objects scale** | **Non-Functional object scale** |
| 3D Objects | Unusable 0% | Unrecoverable 0% |
| Damaged 3D objects | Partially unusable 01%-49% | Partially recoverable 01%-49% |
| 3D Prints | Mostly usable 50%-99% | Recoverable 50%-99% |
| Damaged 3D print | Usable 100% | Acceptable 100% |

Table 8.4, Table 8.5 and Table 8.6 are the final refined set of components and metrics for the authentication component of the framework.

### 8.1.2 Authorisation

The authorisation property has two confirmed components from the first expert review. **The authorisation for resources**: The metric for the authorisation for resources component is **What is the access type for resources used in the 3D object creation and printing?** This is a two-fold metric that asks:

- **"What type of recourses are available?"**
- **"What kind of authorisation is provided?"**

There was a good discussion about the (Allocated 3D printing time) item and its applicability to the current state of technology of 3D printers. The experts believed 3D printing time will not be an issue in future as the technology is advancing rapidly and the printing time will be so shortened that this problem will go away.

> "This item is not necessary in the metric for authorisation for resources because allocating print time is not applicable to users". (Authorisation-Expert 1)

> "This item is not necessary in the metric for authorisation because having a print queue is sufficient to provide information about the print time". (Authorisation-Expert 2)

> "Limiting usage time for 3D printers could seriously hinder the object availability". (Authorisation-Expert 3)

One expert was positive and believed it is important in a rapid prototyping environment.

> "This item is important when producing rapid prototypes to help in the product development cycles". (Authorisation-Expert 4)

But since there were more cons than pros, the metric for (Allocated 3D printing time) was excluded due to the low mean difference of 0.58, and the following comment on the scale for authorisation for resources metric.

> "Item (Identification exists but not required) is not required in the scale". (Authorisation-Expert 5)

The expert was unaware that some systems have an identification capability, but some organisations do not implement them. Also, the statistical data does not agree with that comment, so the scale is unchanged.

**The authorisation to access confidential information**: The metric for the authorisation for resources component is **What security levels are accommodated to restrict access to confidential 3D object/3D prints?** This is a two-fold metric that asks:

- **"What information is available about 3D objects and 3D prints?"**
- **"What kind of access is provided?"**

The authorisation of confidential information metrics has two items that the experts believed are vague, which are **Information about the digital object** and **Information about the physical object**. Therefore, this item will be expanded to include metadata explanation when using the case study. Examples will also be added to the items to make the metric clearer.

**Statistical data for authorisation**: The statistical data in Table 8.7 and Table 8.8 confirms the proposed metrics for the above components, as none of the items or scale in the metrics have a type one error of $p > 0.05$ as shown in the tables under Sig. (2-tailed) as all of them were $< 0.001$ with the exception of the last item (Allocated 3D printing time) that was 0.046 but it still less than 0.05 type one error so the item remained in the framework. The test for the metric was based on 4 points on a Likert scale; therefore, the mean was 2, the number of participants was $N$, the Mean was the average on a scale

of 1 to 4, the mean difference is the average above the mean of 2, standard deviation from the mean, and Sig. (2-tailed) stands for type one error.

Table 8.7: Expert review for authorisation for resources metric

| Test Value for the statistical mean = 2 | | | | | | |
|---|---|---|---|---|---|---|
| **Measure** | **Items** | **N** | **Mean** | **Mean Diff.** | **Std. Dev.** | **Sig. (2-tailed)** |
| | 3D computing resources | 12 | 3.5 | 1.5 | 0.52 | <0.001 |
| | 3D digitization equipment | 12 | 3.42 | 1.42 | 0.52 | <0.001 |
| | 3D Printing material | 12 | 3.33 | 1.33 | 0.49 | <0.001 |
| | 3D Printing Equipment | 12 | 3.33 | 1.33 | 0.49 | <0.001 |
| | Allocated 3D printing time | 12 | 2.58 | 0.58 | 0.9 | 0.046 |
| Scale | | 12 | 3.25 | 1.25 | 0.45 | <0.001 |

Table 8.7 shows that the lowest two values are for (Allocated 3D printing time) and (Scale) having mean differences of 0.58 and 1.25 respectively. The Justification for the Allocated 3D printing time item was discussed earlier and resulted in removal of the item. The score of 1.25 for (Scale) resulted from the experts having some comments on the scales shown in the next section.

Table 8.8: Expert review for authorisation of confidential information metric

| Test Value for the statistical mean = 2 | | | | | | |
|---|---|---|---|---|---|---|
| **Measure** | **Items** | **N** | **Mean** | **Mean Diff.** | **Std. Dev.** | **Sig. (2-tailed)** |
| | 3D object | 12 | 3.33 | 1.33 | 0.49 | <0.001 |
| | Source of 3D object | 12 | 3.5 | 1.5 | 0.52 | <0.001 |
| | Information about the digital object | 12 | 3.42 | 1.42 | 0.52 | <0.001 |
| | 3D Print | 12 | 3.25 | 1.25 | 0.45 | <0.001 |
| | Source of 3D Print | 12 | 3.33 | 1.33 | 0.49 | <0.001 |
| | Information about the physical object | 12 | 3.33 | 1.33 | 0.49 | <0.001 |
| Scale | | 12 | 3 | 1 | 0.85 | 0.002 |

Table 8.8 shows the lowest two values are for (3D Print) and (Scale) having mean differences of 1.25 and 1.00 respectively. Most experts agreed with (3D Prints) but they questioned the value of a 3D printed object that has a digital copy; therefore, they were mostly not Strongly agreed. However, this item remained in the metric as the presence of (3D Prints) provides a more complete metric as shown in the results of confirmation, even if their results were low. However, the type one error of $p < 0.001$ was below the

0.5 threshold. The results from the expert review show that the mean difference for the scale of authorisation of confidential information was 1.00, therefore the following modification has been added.

**Refined metric for the authorisation for resources**: The metric for the authenticity of data source has been refined using the expert review comments by making three modifications to the metric, as shown in Table 8.9. The experts agreed that (3D computing resources, 3D Printing material, and 3D Printing Equipment) should change so that:

- 3D computing resources would be expanded to include storage, 3D object library, software licensing, software versions, and minimum requirements.
- 3D Printing material would be expanded to include multi-material technology, type of material, thickness, and other material specification.
- Printing equipment should be expanded to include hazardous equipment and safety restrictions.

Table 8.9: Metric for authorisation for resources

<table>
<tr><td colspan="2">Component: Authorisation for resources “Refers to authorisation for 3D objects and 3D printed object resources.”</td></tr>
<tr><td colspan="2">Metric: What is the access type for resources used in the 3D object creation and printing?</td></tr>
<tr><td>Measure item</td><td>Scale</td></tr>
<tr><td>3D computing resources</td><td rowspan="4">No identification<br>Identification exists but not required<br>Identification exists and required<br>Identification and authentication exists and required</td></tr>
<tr><td>3D digitization equipment</td></tr>
<tr><td>3D Printing material</td></tr>
<tr><td>3D Printing Equipment</td></tr>
<tr><td colspan="2">Explanations</td></tr>
<tr><td colspan="2">3D computing resources include storage, 3D object library, software licensing, software versions and minimum requirements.</td></tr>
<tr><td colspan="2">3D Printing materials include multi-material technology, type of material, thickness and other material specification.</td></tr>
<tr><td colspan="2">Printing equipment include hazardous equipment and safety restrictions</td></tr>
</table>

**Refined metric for the authorisation to access confidential information**: The metric for accounting identification has been refined using the expert review comments by making two additions to the metric, as shown in Table 8.10.

**Digital information scale** The scale should change from (No, Low Level, Mid level, High level Access) to (Read, Read and write, Read, write and delete, Read, Write, Delete and 3D Print).

**Physical objects or physical records scale** The scale should change from (No Access, Low Level Access, Mid level Access, High level Access) to (Mandatory Access Control, Discretionary Access Control, Role-Based Access Control, Rule-Based Access Control, Lattice-based Access Control, Access control list)

Table 8.10: Metric for authorisation of confidential information

<table>
<tr><td colspan="3">Component: Authorisation of confidential information “Refers to the authorisation for confidential information access of 3D objects and a 3D printed object?</td></tr>
<tr><td colspan="3">Metric: What security levels are accommodated to restrict access to confidential 3D object/3D prints?</td></tr>
<tr><td>Item</td><td colspan="2">Scale</td></tr>
<tr><td>3D object (STL file format)</td><td colspan="2" rowspan="2">Read,<br>Read & write<br>Read, write & delete<br>Read, Write, Delete & 3D Print</td></tr>
<tr><td>Information about the digital object (metadata)</td></tr>
<tr><td>Item</td><td>Scale for Digital records:</td><td>Scale for Physical records:</td></tr>
<tr><td>Source of 3D object (3D scanned object)</td><td rowspan="2">Read<br>Read & write<br>Read, write & delete<br>Read, Write, Delete & 3D Print</td><td rowspan="2">Mandatory Access Control<br>Discretionary Access Control<br>Role-Based Access Control<br>Rule-Based Access Control<br>Lattice-based Access Control<br>Access control list</td></tr>
<tr><td>Source of 3D Print</td></tr>
<tr><td>Item</td><td colspan="2">Scale</td></tr>
<tr><td>Information about the physical object (metadata)</td><td colspan="2" rowspan="2">Mandatory Access Control<br>Discretionary Access Control<br>Role-Based Access Control<br>Rule-Based Access Control<br>Lattice-based Access Control<br>Access control list</td></tr>
<tr><td>3D Print</td></tr>
<tr><td colspan="3">Information about the digital object and the physical object include metadata such as where the original object was located, who designed the original 3D object, similar derivative works and the like.</td></tr>
</table>

Table 8.9 and Table 8.10 are the final refined set of components and metrics for the authorisation component of the framework.

### 8.1.3 Accounting

This property looks at three basic actions (Who did What, and When). **The identification component**: The metric for the identification component is **How strong are the identification methods?** This is a two-fold metric that asks:

- **"What is the identification method?"**
- **"How strong is the identification method?"**

The first metric is for the identification component. Concern was expressed with the technology of information sharing of a 3D object. There was also concern with hybridisation and biometric technologies, as some experts believed these could complicate the identification procedures.

> "Using biometrics for identification is excessive for accounting for identity when dealing 3D object/3D prints". (Accounting-Expert 1)

> "A hybrid of three methods is excessive for an identification method". (Accounting-Expert 2)

> "A hybrid of three methods could limit sharing and hinders the sharing process". (Accounting-Expert 3)

Table 8.11 shows that the biometric and hybridisation items (Hybrid of three) and (Something you are) achieved a relatively low score having mean differences of 0.92 and 1.00 respectively. However, the presence of the biometric and hybridisation provides a more complete metric, as shown in the results of confirmation even if their results were low. The type one errors of 0.001 and 0.002 were below the threshold, $p < 0.5$.

> "The need for hybrid methods is subject to the importance of the protected information". (Accounting-Expert 4)

**The protocol component**: The metric for the protocol component is **Are the actions listed being audited (recorded)?** This is a two-fold metric that asks:

- **"What type of actions being performed?"**
- **"How much of that information is being recorded?"**

The second metric in the expert review is for the protocol component; there were concerns with this metric regarding reading 3D objects.

> "Reading 3D objects should not be audited and tracked because if the object is available to read, then it can be exploited and altered". (Accounting-Expert 5)

This comment might sound contradictory but what the expert meant is the idea is that even viewing a 3D object could compromise the information about it. Although this is an issue, the research of provenance is about enabling an individual who wants to share the object with the public or a few selected individuals. Therefore, being able to read/view the object is a minimum requirement. This comment is also subject to the importance of the information.

> "The strength of the accounting is subject to the importance of the information being protected". (Accounting-Expert 6)

The expert review added two overlooked items in the metric:

> "Item one is copying 3D objects and Item two is printing 2D schematics for 3D objects". (Accounting-Expert 7)

The above items are believed to be of importance and were added to the items in the metrics.

**The timestamp component**: The metric for the timestamp component is **What timestamps are being audited (recorded)?** This is a two-fold metric that asks:

- **"What actions are being timestamped and recorded?"**
- **"How much of that information is being recorded?"**

The third metric in the expert review is for the timestamp component.

> "This item is important as different timestamps means we end up with different objects. Therefore, a comparative study of 3D objects constructed at different times might shed more light on the matter". (Accounting-Expert 8)

This raised the interesting issue of divergence of identity from the same object. This will be added to the future research work. The review added two overlooked items in the metric:

> "Add Timestamp Copying of 3D objects, and for Printing 2D schematics for 3D objects". (Accounting-Expert 9)

Table 8.12: Expert review for accounting protocol metric

| Test Value for the statistical mean = 2 | | | | | | |
|---|---|---|---|---|---|---|
| **Measure** | **Items** | **N** | **Mean** | **Mean Diff** | **Std. Dev.** | **Sig. (2-tailed)** |
| | Read 3D objects. | 12 | 3.25 | 1.25 | 0.45 | <0.001 |
| | Write to 3D objects | 12 | 3.5 | 1.5 | 0.52 | <0.001 |
| | Create new 3D object. | 12 | 3.5 | 1.5 | 0.52 | <0.001 |
| | Delete 3D object. | 12 | 3.5 | 1.5 | 0.67 | <0.001 |
| | Print 3D object | 12 | 3.33 | 1.33 | 0.49 | <0.001 |
| Scale | | 12 | 3.25 | 1.25 | 0.62 | <0.001 |

The above items are believed to be important and were added to the items in the metrics.

**Statistical data for accounting**: The statistical data in Table 8.11, Table 8.12 and Table 8.13 confirms the proposed metrics for the above components, as none of the items or scale in the metrics have a type one error of $p > 0.05$ as shown in the tables under Sig. (2-tailed). The test for the metric was based on 4 points on a Likert scale. Therefore, the mean was 2, the number of participants was *N*, the Mean was the average on a scale of 4, the mean difference is the average above the mean of 2, standard deviation from the mean, and Sig. (2-tailed) stands for type one error.

Table 8.11: Expert review for accounting identification metric

| Test Value for the statistical mean = 2 | | | | | | |
|---|---|---|---|---|---|---|
| **Measure** | **Items** | **N** | **Mean** | **Mean Diff** | **Std. Dev.** | **Sig. (2-tailed)** |
| | Something you know (passwords). | 12 | 3.33 | 1.33 | 0.49 | <0.001 |
| | Something you have (ID card). | 12 | 3.33 | 1.33 | 0.49 | <0.001 |
| | Something you are (fingerprint biometric). | 12 | 3 | 1 | 0.74 | 0.001 |
| | Hybrid of two (password with an ID card). | 12 | 3.42 | 1.42 | 0.52 | <0.001 |
| | Hybrid of three: is a combination first three | 12 | 2.92 | 0.92 | 0.79 | 0.002 |
| Scale | | 12 | 3.5 | 1.5 | 0.52 | <0.001 |

Table 8.11 shows that the lowest two values are for (Hybrid of three) and (Something you are) having mean differences of 0.92 and 1.00 respectively.

Table 8.12 shows that the lowest two values are (Read 3D objects) and (Scale) having a mean difference of 1.25 for both. The value is 1.25 for reading because the expert

Table 8.13: Expert review for accounting timestamp metric

| Test Value for the statistical mean = 2 | | | | | | |
|---|---|---|---|---|---|---|
| **Measure** | **Items** | **N** | **Mean** | **Mean Diff** | **Std. Dev.** | **Sig. (2-tailed)** |
| | Read 3D objects. | 12 | 3.17 | 1.17 | 0.84 | 0.001 |
| | Write to 3D objects | 12 | 3.5 | 1.5 | 0.67 | <0.001 |
| | Create new 3D object. | 12 | 3.58 | 1.58 | 0.52 | <0.001 |
| | Delete 3D object. | 12 | 3.42 | 1.42 | 0.67 | <0.001 |
| | Print 3D object | 12 | 3.42 | 1.42 | 0.52 | <0.001 |
| Scale | | 12 | 3.33 | 1.33 | 0.49 | <0.001 |

from Cultural Heritage believed that any restrictions on the reading of 3D objects could hinder the process of sharing 3D content.

The scale mean difference of 1.25 is accounted for since the expert felt the scale could be improved by adding more clarification.

Table 8.13 shows that the lowest two values are (Read 3D objects) and (Scale) having mean differences of 1.17 and 1.33 respectively. The value of 1.17 is the same as the previous section with the comment on the reading of 3D objects.

The scale mean difference of 1.33 is accounted for since the expert felt the scale could be improved by adding more clarification, as suggested in their comments below on the refined metric for the protocol component.

**Refined metric for the identification component**: The metric for accounting identification was refined using the expert review comments, by making two additions to the metric, as shown in Table 8.14.

- No identification method is added to the items in the metric.
- The scale should change from (Weak, Medium, Strong, very strong) to (Null, Very Weak, Weak, Medium, Strong, Very Strong)

Table 8.14: Refined metric for accounting identification

| Component: Identification "Refers to establishing an Identification procedure of (users/Services) for computer generated 3D objects & 3D printed objects." | |
|---|---|
| Metric: How strong are the identification methods? | |
| **Measure item** | **Scale** |
| No Identification Method | Null |
| Something you know (passwords). | Very Weak |
| Something you have (ID card). | Weak |
| Something you are (fingerprint biometric). | Medium |
| Hybrid of two (password with an ID card). | Strong |
| Hybrid of three: is a combination first three | Very Strong |

**Refined metric for the protocol component**: The metric for accounting protocol was refined using the expert review comments, by making two additions to the metric, as shown in Table 8.15.

- The scale seems a choice between (Rarely, sometimes, most of the time) meaning that it is not adequate, and (All the time) which means adequate.
- The Scale should change from (Rarely, Sometimes, Most of the time, All the time) to (Never 0%, sometimes 01%-49%, most of the time 50%-99%, all the time 100%).

Table 8.15: Refined metric for accounting protocols

| Component: Protocols ?Refers to accounting for processes and protocols acted upon 3D objects & 3D prints? | |
|---|---|
| Metric: Are the actions listed being audited (recorded)? | |
| **Measure item** | **Scale** |
| Read 3D objects. | No information is recorded 0% |
| Write to 3D objects | Some information is recorded 01%-49% |
| Copy 3D object | Most information is recorded 50%-99% |
| Create new 3D object. | Information is recorded all the time 100% |
| Delete 3D object. | |
| Print 2D schematics | |
| Print 3D object | |

**Refined metric for the timestamp component**: The metric for accounting timestamp was refined using the expert review comments, by making two additions to the metric, as shown in Table 8.16. This is the final refined version that will be used in future work. The scale was addressed by adding more clarification as suggested.

- The scale seems a choice between (Rarely, sometimes, most of the time) meaning not adequate, and (All the time) which is adequate.
- The Scale should change from (Rarely, Sometimes, Most of the time, All the time) to (Never 0%, sometimes 01%-49%, most of the time 50%-99%, all the time 100%)

Table 8.16: Refined metric for accounting timestamp

| Component: Timestamp "Refers to recording the time when an action has been acted upon 3D objects and 3D prints. | |
|---|---|
| Metric: What timestamps that are being audited (recorded)? | |
| **Measure item** | **Scale** |
| Read 3D objects. | No information is recorded 0% |
| Write to 3D objects | Some information is recorded 01%-49% |
| Copy 3D object | Most information is recorded 50%-99% |
| Create new 3D object. | Information is recorded all the time 100% |
| Delete 3D object. | |
| Print 2D schematics | |
| Print 3D object | |

Table 8.14, Table 8.15 and Table 8.16 are the final refined set of components and metrics for the accounting component of the framework.

## 8.2 Information Security Principle

This principle depends on three properties: **Confidentiality, integrity, and availability**. The following sections discuss each property in detail.

### 8.2.1 Confidentiality

The experts viewed information and 3D objects as not necessarily at the same confidentially levels. For example, a person may have good information about the object freely given, and thus can make a decision to purchase a 3D object from a digital library:

> "The 3D object or 3D print without its source and information about the object is meaningless; therefore, the objects and information don't need to be secured at the same level". (Confidentiality-Expert 1)

The same 3D object may have different values, based on the type of licensing.

> "Should there be different types of licence, such as (to own, to print, to distribute)?" (Confidentiality-Expert 2)

However, this research is about confidentiality values, not monetary values. The confidentiality property has two components based on the first expert review.

**Disclosure of confidential information**: The metric for the disclosure of confidential information component is **What is the confidentiality of information about 3D objects/3D prints?** This is a two-fold metric that asks:

- **"What type of confidential information does the organisation disclose?"**
- **"What kind of confidentiality disclosure does the organisation support?"**

The experts commented on the scale that some public information disclosure is different across international borders, because different countries have different standards for information confidentiality.

> "With public access, there are still international restrictions for information sharing". (Confidentiality-Expert 3)

Public disclosure is not necessary since the parties involved can exchange information as end-users, groups, and organisations.

> "The Public shouldn't be restricted, but they don't need to know". (Confidentiality-Expert 4)

There is a debate about the borders of public access, which falls outside the scope of this research. However, public disclosure is really important for open source and open access to 3D objects.

**Strength of confidentiality measures**: The metric for the strength of confidentiality measures component is **How strong are the security measures to protect the information confidentiality of 3D objects/3D prints?** This is a two-fold metric that asks:

- **"What type of confidential information does the organisation secure?"**
- **"How strong are the confidentiality measures?"**

**Statistical data for confidentiality**: The statistical data in Table 8.17 and Table 8.18 confirms the proposed metrics for the above components, since none of the items or scale in the metrics have a type one error $p > 0.05$, as shown in the tables under Sig. (2-tailed). The test for the metric was based on 4 points on a Likert scale. Therefore, the mean was 2, the number of participants was *N*, the Mean was the average on a scale of 4, the mean difference is the average above the mean of 2, standard deviation from the mean, and Sig. (2-tailed) stands for type one error.

Table 8.17: Expert review for Disclosure of confidential information metrics

| Test Value for the statistical mean = 2 | | | | | | |
|---|---|---|---|---|---|---|
| **Measure** | **Items** | **N** | **Mean** | **Mean Diff.** | **Std. Dev.** | **Sig. (2-tailed)** |
| | 3D object | 12 | 3.33 | 1.33 | 0.49 | <0.001 |
| | Source of 3D object | 12 | 3.58 | 1.58 | 0.52 | <0.001 |
| | Information about the digital object | 12 | 3.58 | 1.58 | 0.52 | <0.001 |
| | 3D Print | 12 | 3.17 | 1.17 | 0.58 | <0.001 |
| | Source of 3D Print | 12 | 3.58 | 1.58 | 0.52 | <0.001 |
| | Information about the physical object | 12 | 3.42 | 1.42 | 0.52 | <0.001 |
| Scale | | 12 | 3.5 | 1.5 | 0.52 | <0.001 |

Table 8.17 shows the lowest two values are (3D object) and (3D Print) having mean differences of 1.33 and 1.17 respectively. The results show that (3D objects) and (3D prints) have the lowest of the mean differences because the expert's view that confidentiality measures should not be equal in importance, as discussed in the previous section.

> "The 3D object or 3D print without its source and information about the object is meaningless; therefore, the objects and information don't need to be secured at the same level". (Confidentiality-Expert 5)

The experts valued the information about the 3D object and 3D prints more than the objects themselves.

Table 8.18: Expert review for Strength of confidentiality metric

| Test Value for the statistical mean = 2 | | | | | | |
|---|---|---|---|---|---|---|
| **Measure** | **Items** | **N** | **Mean** | **Mean Diff.** | **Std. Dev.** | **Sig. (2-tailed)** |
| | 3D object | 12 | 3.25 | 1.25 | 0.45 | <0.001 |
| | Source of 3D object | 12 | 3.58 | 1.58 | 0.52 | <0.001 |
| | Information about the digital object | 12 | 3.5 | 1.5 | 0.52 | <0.001 |
| | 3D Print | 12 | 3.42 | 1.42 | 0.52 | <0.001 |
| | Source of 3D Print | 12 | 3.5 | 1.5 | 0.52 | <0.001 |
| | Information about the physical object | 12 | 3.42 | 1.42 | 0.52 | <0.001 |
| Scale | | 12 | 3.25 | 1.25 | 0.45 | <0.001 |

Table 8.18 shows that the lowest two values are for (3D objects) and (Scale) having a mean difference of 1.25 for both. As before, the low mean for (3D object) is due to the concerns with sharing 3D objects. The score of 1.25 for (Scale) resulted from the experts having some comments on the scales, shown in the next section.

**Refined metric for disclosure of confidential information**: The metric for accounting identification has been refined using the expert review comments by making one addition to the metric, as shown in Table 8.19. Disclosure of confidential information and strength of confidentiality measures metrics have two items that the experts believed were vague.

- **Information about the digital object**
- **Information about the physical object**

This item will therefore be expanded to include metadata explanation when using the case study. Examples will also be added to the items to make the metric clearer.

Table 8.19: Metric for disclosure of confidential information

| Component: Disclosure of confidential information "Refers to disclosure of confidential information of 3D objects and a 3D printed object." | |
|---|---|
| Metric: What is the confidentiality of information for and about 3D objects/3D prints? | |
| **Measure item** | **Scale** |
| 3D object (STL file format) | Individuals<br>Groups<br>Internal organisation<br>Public |
| Source of 3D object (3D scanned object) | |
| Information about the digital object (metadata) | |
| 3D Print | |
| Source of 3D Print | |
| Information about the physical object (metadata) | |
| Information about the digital object and the physical object include metadata such as where was the original object located, who designed the original 3D object, similar derivatives works and alike. | |

**Refined metric for strength of confidentiality measures**: The metric for accounting identification has been refined using the expert review comments, by making one addition to the metric, as shown in Table 8.20.

Disclosure of confidential information and strength of confidentiality measures metrics contain two items that the experts believed were vague.

- **Information about the digital object**
- **Information about the physical object**

This item will therefore be expanded to include metadata when using the case study. Examples will also be added to the items to make the metric clearer.

Table 8.20: Metric for strength of confidentiality measures

| Component: Strength of confidentiality measures ?Refers to the strength of confidentiality measures used to secure 3D objects and a 3D printed object.? | |
|---|---|
| Metric: How strong are the security measures to protect the information confidentiality of 3D objects/3D prints? | |
| **Measure item** | **Scale** |
| 3D object<br>(STL file format) | No confidentiality measures |
| Source of 3D object<br>(3D scanned object) | Weak confidentiality measures |
| Information about the digital object<br>(metadata) | Medium confidentiality measures |
| 3D Print | Strong confidentiality measures |
| Source of 3D Print | Very Strong confidentiality measures |
| Information about the physical object<br>(metadata) | |
| Information about the digital object and the physical object include metadata such as where the original object was located, who designed the original 3D object, similar derivative works and like. | |

Table 8.19 and Table 8.20 are the final refined set of components and metrics for the confidentiality component of the framework.

### 8.2.2 Integrity

The integrity of information property has three components to maintain integrity. **Data maintenance for data integrity**: The metric for the data maintenance for data integrity component is **How secure is the storage of 3D object/3D prints?** This is a two-fold metric that asks:

- **"What type of information the organisation maintain?"**
- **"How strong is the protection of these assets?"**

The experts reviewed the metric for the first component of the integrity property and agreed that the items should be expanded for (Information about the digital object) and (Information about the physical object) to specify what information should be included.

> "This item should be expanded to include versions, revisions, and derivatives. & The expansion should be limited as the potential information is limitless". (Integrity-Expert 1)

**Secure disposal of information**: The metric for secure disposal of information component is **How secure is the disposal of 3D objects/3D prints?** This is a two-fold metric that asks:

- **"What type of information the organisation that needs to be securely disposed off?"**
- **"How strong is the disposal of these assets?"**

The disposal of 3D objects or 3D prints is really important as a security metric; the experts also noted that recycling should also be included.

> "Consider environmental concerns in the scale, i.e. green technology". (Integrity-Expert 2)

**Backup frequency**: The metric for the Backup frequency component is (How frequent is the backup process of 3D object/3D prints?) This is a two-fold metric that asks:

- **"What type of organisation assets needs to be backed up?"**
- **"How resilient is the backup procedures?"**

The backup frequency is dependent on the organisation requirement of the backup process, based on time (every 24 hours, 48 hours, etc.), and the metric could be expanded to fit the organisation needs.

> "The backup frequency should be divided into two types frequency of backups based on actions preformed on objects, and frequency of backups based on time. And the items in this metric should be expanded to specify what information is covered". (Integrity-Expert 3)

Also the metric of backing up 3D prints could use further discussion and study as it can be very costly; however, for the time being the metric is sufficient.

> "Backup of 3D prints by printing more 3D prints could be costly and not economically feasible". (Integrity-Expert 4)

**Statistical data for integrity**: The statistical data in Table 8.21, Table 8.22 and Table 8.23, confirms the proposed metrics for the above components, as none of the items or scale in the metrics have $p > 0.05$ as shown in the tables under Sig. (2 Tailed). The test for the metric was based on 4 points on a Likert scale therefore the mean was

2, the number of participants was N, the Mean was the average on scale of 4, the mean difference is the average above the mean of 2, standard deviation from the mean, and Sig. (2-tailed) stands for type one error.

Table 8.21: Expert review for integrity metrics - data maintenance

| Test Value for the statistical mean = 2 | | | | | | |
|---|---|---|---|---|---|---|
| **Measure** | **Items** | **N** | **Mean** | **Mean Diff.** | **Std. Dev.** | **Sig. (2-tailed)** |
| | 3D object | 12 | 3.5 | 1.5 | 0.52 | <0.001 |
| | Source of 3D object | 12 | 3.58 | 1.58 | 0.52 | <0.001 |
| | Information about the digital object | 12 | 3.5 | 1.5 | 0.52 | <0.001 |
| | 3D Print | 12 | 3.33 | 1.33 | 0.49 | <0.001 |
| | Source of 3D Print | 12 | 3.58 | 1.58 | 0.52 | <0.001 |
| | Information about the physical object | 12 | 3.5 | 1.5 | 0.52 | <0.001 |
| Scale | | 12 | 3.25 | 1.25 | 0.45 | <0.001 |

Table 8.21 shows the lowest two values are (3D Print) and (Scale) having mean differences of 1.33 and 1.25 respectively. The scale mean difference of 1.25 is accounted for by the expert who felt the scale could be improved by adding more clarification as suggested in comments in the refined metric for protocol component. The experts were not sure how 3D prints could be maintained or if they should. However, it is important in the metric because sometimes manufacturers use 3D printing to create the first stage of an object, the initial stage for completing a project. Therefore, it is important to keep the mould in good condition prior to processing, or glazing in the case of 3D printed pottery. And since $p < 0.001$, below type one error of 0.5, the item remained unchanged.

Table 8.22: Expert review for integrity metrics - secure disposal of information

| Test Value for the statistical mean = 2 | | | | | | |
|---|---|---|---|---|---|---|
| **Measure** | **Items** | **N** | **Mean** | **Mean Diff.** | **Std. Dev.** | **Sig. (2-tailed)** |
| | 3D object | 12 | 3.5 | 1.5 | 0.52 | <0.001 |
| | Source of 3D object | 12 | 3.58 | 1.58 | 0.52 | <0.001 |
| | Information about the digital object | 12 | 3.58 | 1.58 | 0.52 | <0.001 |
| | 3D Print | 12 | 3.33 | 1.33 | 0.65 | <0.001 |
| | Source of 3D Print | 12 | 3.5 | 1.5 | 0.52 | <0.001 |
| | Information about the physical object | 12 | 3.5 | 1.5 | 0.52 | <0.001 |
| Scale | | 12 | 3.33 | 1.33 | 0.49 | <0.001 |

The statistical result, similar to the previous metric in availability of services as shown in Table 8.22, shows that the lowest two values are for (3D Print) and (Scale) having a mean difference of 1.33 for both. The score of 1.08 on the (Scale) resulted from the experts having some comments on the scales shown in the next section.

Table 8.23: Expert review for integrity metrics - backup frequency

| Test Value for the statistical mean = 2 | | | | | | |
|---|---|---|---|---|---|---|
| **Measure** | **Items** | **N** | **Mean** | **Mean Diff.** | **Std. Dev.** | **Sig. (2-tailed)** |
| | 3D object | 12 | 3.67 | 1.67 | 0.49 | <0.001 |
| | Source of 3D object | 12 | 3.5 | 1.5 | 0.52 | <0.001 |
| | Information about the digital object | 12 | 3.42 | 1.42 | 0.52 | <0.001 |
| | 3D Print | 12 | 3.25 | 1.25 | 0.45 | <0.001 |
| | Source of 3D Print | 12 | 3.5 | 1.5 | 0.52 | <0.001 |
| | Information about the physical object | 12 | 3.33 | 1.33 | 0.49 | <0.001 |
| Scale | | 12 | 3.17 | 1.17 | 0.39 | <0.001 |

The statistical result, similar to the previous metric in availability of services as shown in Table 8.23, shows that the lowest two values are for (3D Print) and (Scale) having mean differences of 1.25 for (3D Print) and 1.17 for (Scale). The score of 1.17 for (3D Print Storage) arose from discussions in the focus group about the feasibility of allocating dedicated 3D print storage. The score of 1.25 for (Scale) resulted from the experts having some comments on the scales shown in the next section.

**Refined metric for data maintenance for data integrity**: The metric for data maintenance for data integrity has been refined using the expert review comments by making one modification to the metrics as shown in Table 8.24.

- Extra strong should be added to the scale to be (No, Weak, Medium, Strong, Extra Strong secure storage) to accommodate for high-level security for priceless and one-of-a-kind objects.

Table 8.24: Metric for Data maintenance for data integrity

| Component: Data Maintenance "Refers to having properly maintained data (3D objects, 3D prints)." | |
|---|---|
| Metric: How secure is the storage of 3D object/3D prints? | |
| **Measure item** | **Scale** |
| 3D object | No secure storage |
| Source of 3D object | Weak secure storage |
| Information about the digital object | Medium secure storage |
| 3D Print | Strong secure storage |
| Source of 3D Print | Extra Strong secure storage |
| Information about the physical object | |

**Refined metric for secure disposal of information**: The metric for backup frequency for integrity has been refined using the expert review comments as shown in Table 8.25.

Table 8.25: Metric and measure for secure disposal of information

| Component: Secure disposal ?Refers to secure disposal of previous versions of (3D objects, 3D prints).? | |
|---|---|
| Metric: How secure is the disposal of 3D objects/3D prints? | |
| **Measure item** | **Scale** |
| 3D object | No secure disposal |
| Source of 3D object | Weak secure disposal |
| Information about the digital object | Medium disposal storage |
| 3D Print | Strong secure disposal |
| Source of 3D Print | |
| Information about the physical object | |

**Refined metric for backup frequency**: The metric for backup frequency for integrity has been refined using the expert review comments as shown in Table 8.26.

Table 8.26: Metric and measure for backup frequency

| Component: Data backup "Refers to data backup of (3D objects, 3D prints)." | |
|---|---|
| Metric: How frequent is the backup process of 3D object/3D prints? | |
| **Measure item** | **Scale** |
| 3D object | No backup |
| Source of 3D object | Low frequency backup |
| Information about the digital object | Medium frequency backup |
| 3D Print | Strong frequency backup |
| Source of 3D Print | |
| Information about the physical object | |

Table 8.24, Table 8.25 and Table 8.26 are the final refined set of components and metrics for the confidentiality component of the framework. Please note the scales the components were explained in the expert review also the reason the scales were incremental in strength and frequency because measuring integrity as a property for additive manufacturing is subjective and depends on the domain.

### 8.2.3 Availability

The availably property has four components. **Availability of resources**: The metric for the availability of resources component is **What is the availability of resources for 3D objects/printing?** This is a two-fold metric that asks:

- **"Types of resources in an organisation?"**
- **"How often are these resources are available?"**

There was the same discussion in the authorisation property about the item (Allocated 3D printing time) and its applicability in the current state of technology of 3D printers. The experts believed 3D printing time will not be an issue in future as the 3D printing technology is advancing quite rapidly and the time for printing will be shortened.

**Availability of information**: The metric for the availability of information component is **What is the availability of information for 3D objects/printing?** This is a two-fold metric that asks:

- **"What type of support for 3D printing services?'**
- **"How often are these features are available?"**

The availability of information expert review commented on the metadata that

> "Metadata is not important as the current state of the technology provides little support for this feature". (Availability-Expert 1)

At the time this research is written, the metadata support is not fully developed in STL and AMF (STL 2.0). However, the item will not be removed and future explanation will be added.

**Availability of services**: The metric for the availability of services component is **What is the availability of services for 3D objects/printing?** This is a two-fold metric that asks:

- **"What type of services/facilities the organisation own?"**
- **"How often are these services are available?"**

The availability of services had experts comment on 3D print storage that

> "This point is a bit vague and the item should be renamed to 3D printing storage size". (Availability-Expert 2)

This comment has been addressed and metric renamed.

**Recovery rate of failed resources**: The metric for the recovery rate of failed resources component is **What is the recovery period of failed resources for 3D objects/printing?** This is a two-fold metric that asks:

- **"What type of maintained services/facilities?"**
- **"How well maintained are these services by reflecting on the recovery rate?"**

The recovery rate of failed resources expert review commented on 3D print storage that

> "This item is vague as its not clear how storage can fail and also recover". (Availability-Expert 3)

Therefore,3D print storage was changed to 3D print storage size and added to the metric. When the experts were asked about the scale of the metric and whether frequency over time should be included in the scale, one expert had the following comment

> "Time should not be included in the scale as it is relative to size of organisation and importance of information". (Availability-Expert 4)

**Statistical data for availability**: The statistical data in tables Table 8.27, Table 8.28, Table 8.29 and Table 8.30 confirms the proposed metrics for the above components, as none of the items or scale in the metrics have $p > 0.05$ as shown in the tables under Sig. (2-tailed) as all of them were $< 0.001$. The test for the metric was based on 4 points on a Likert scale therefore the mean was 2, the number of participants was N, the Mean was the average on scale of 4, the mean difference is the average above the mean of 2, standard deviation from the mean, and Sig. (2-tailed) stands for type one error.

Table 8.27: Expert review for availability of resources metric

| Test Value for the statistical mean = 2 | | | | | | |
|---|---|---|---|---|---|---|
| **Measure** | **Items** | **N** | **Mean** | **Mean Diff.** | **Std. Dev.** | **Sig. (2-tailed)** |
| | 3D computing resources | 12 | 3.67 | 1.67 | 0.49 | <0.001 |
| | 3D digitization equipment | 12 | 3.58 | 1.58 | 0.52 | <0.001 |
| | 3D Printing material | 12 | 3.58 | 1.58 | 0.67 | <0.001 |
| | 3D Printing Equipment | 12 | 3.67 | 1.67 | 0.49 | <0.001 |
| | Allocated 3D printing time | 12 | 3.17 | 1.17 | 0.94 | 0.001 |
| Scale | | 12 | 3.08 | 1.08 | 0.67 | <0.001 |

Table 8.27 shows that the lowest two values are for (Allocated 3D printing time) and (Scale) having mean differences of 1.17 and 1.08 respectively. The Justification for the Allocated 3D printing time item was discussed earlier and resulted in removal of the item. Even though the (Allocated 3D printing time) was slightly higher than for authorisation for resources metric of 0.58, the score of 1.08 for (Scale) resulted from the experts having some comments on the scales shown in the next section.

Table 8.28: Expert review for availability of information metric

| Test Value for the statistical mean = 2 | | | | | | |
|---|---|---|---|---|---|---|
| **Measure** | **Items** | **N** | **Mean** | **Mean Diff.** | **Std. Dev.** | **Sig. (2-tailed)** |
| | Print material | 12 | 3.67 | 1.67 | 0.49 | <0.001 |
| | Print colour | 12 | 3.42 | 1.42 | 0.67 | <0.001 |
| | Print texture | 12 | 3.5 | 1.5 | 0.52 | <0.001 |
| | Print constellation | 12 | 3.5 | 1.5 | 0.52 | <0.001 |
| | Meta-data | 12 | 3.5 | 1.5 | 0.67 | <0.001 |
| Scale | | 12 | 3.33 | 1.33 | 0.65 | <0.001 |

Table 8.28 shows that the lowest two values are for (Print colour) and (Scale) having mean differences of 1.42 and 1.33 respectively. The Justification for the Allocated 3D

printing time item was discussed earlier and resulted in removal of the item. The justification for the mean of 1.42 for (Print colour) is due to only one type of 3D printer supporting this feature, which is the Granular material binding. However, the $p < 0.001$ was below the type one threshold of 0.5 therefore the item will remain in the metric.

Table 8.29: Expert review for availability of services metric

| Test Value for the statistical mean = 2 | | | | | | |
|---|---|---|---|---|---|---|
| **Measure** | **Items** | **N** | **Mean** | **Mean Diff.** | **Std. Dev.** | **Sig. (2-tailed)** |
| | 3D Digitization service | 12 | 3.42 | 1.42 | 0.52 | <0.001 |
| | 3D Computing service | 12 | 3.5 | 1.5 | 0.52 | <0.001 |
| | 3D object Storage | 12 | 3.5 | 1.5 | 0.52 | <0.001 |
| | 3D Printing services | 12 | 3.5 | 1.5 | 0.52 | <0.001 |
| | 3D Print Storage | 12 | 3.17 | 1.17 | 0.39 | <0.001 |
| Scale | | 12 | 3.17 | 1.17 | 0.58 | <0.001 |

Table 8.29 shows that the lowest two values are for (3D Print Storage) and (Scale) having a mean difference of 1.17 for both. The score of 1.17 for (3D Print Storage) was due to the vagueness of the item as mentioned in the previous section. The score of 1.17 for (Scale) resulted from the experts having some comments on the scales shown in the next section.

Table 8.30: Expert review for recovery rate of failed resources metrics

| Test Value for the statistical mean = 2 | | | | | | |
|---|---|---|---|---|---|---|
| **Measure** | **Items** | **N** | **Mean** | **Mean Diff.** | **Std. Dev.** | **Sig. (2-tailed)** |
| | 3D Digitization service | 12 | 3.58 | 1.58 | 0.52 | <0.001 |
| | 3D Computing service | 12 | 3.58 | 1.58 | 0.52 | <0.001 |
| | 3D object Storage | 12 | 3.75 | 1.75 | 0.45 | <0.001 |
| | 3D Printing services | 12 | 3.5 | 1.5 | 0.52 | <0.001 |
| | 3D Print Storage | 12 | 3.17 | 1.17 | 0.58 | <0.001 |
| Scale | | 12 | 3.08 | 1.08 | 0.52 | <0.001 |

The statistical result is similar to the previous metric in availability of services as shown in Table 8.30. The expert review showed that the lowest two values were for (3D Print Storage) and (Scale) having mean differences of 1.17 and 1.08 respectively. The score of 1.17 for (3D Print Storage) was due to the vagueness of the item as mentioned in the previous section. The score of 1.08 for (Scale) resulted from the experts having some comments on the scales shown in the next section.

**Refined metric for availability of resources**: The metric for availability of resources has been refined using the expert review comments by making five modifications to the metric as shown in Table 8.31. The availability of resources expert review comments agreed that (3D computing resources, 3D Printing material, and 3D Printing Equipment) should be expanded thus:

- 3D computing resources would be expanded to include storage, 3D object library, software licensing, software versions, and minimum requirements.
- 3D Printing material would be expanded to include multi-material technology, type of material, thickness, and other material specification.
- Printing equipment should be expanded to include hazardous equipment and safety restrictions.
- The item available should be changed to always available.
- The scale should change from (Unavailable, Sometime Available, Often Available, Available) to (Unavailable 0%, Sometime Available 01%-49%, Often Available 50%-99%, Always Available 100%) to accommodate percentages of availability.

Table 8.31: Metric and measure for availability of resources

| Component: Availability of resources ?Refers to the availability of resources for 3D objects and 3D prints.? | |
|---|---|
| Metric: What is the availability of resources for 3D objects/printing? | |
| **Measure item** | **Scale** |
| 3D computing resources | Unavailable 0% |
| 3D digitization equipment | Sometime Available 01%-49% |
| 3D Printing material | Often Available 50%-99% |
| 3D Printing Equipment | Always Available 100% |
| Explanations | |
| 3D computing resources include storage, 3D object library, software licensing ,software versions, and minimum requirements. | |
| 3D Printing materials include multi-material technology, type of material, thickness, and other material specification. | |
| Printing equipment include hazardous equipment, and safety restrictions | |

**Refined metric for availability of information**: The metric for the availability of information has been refined using the expert review comments by making two modifications to the metric as shown in Table 8.32.

- The item available should be changed to always available.

- The scale should change from (Unavailable, Sometime Available, Often Available, Available) to (Unavailable 0%, Sometime Available 01%-49%, Often Available 50%-99%, Always Available) to accommodate percentages of availability.

Table 8.32: Metric for availability of information

| Component: Availability of information "Refers to the availability of information about 3D objects and a 3D print (i.e. print colour, material, texture and meta data)." | |
|---|---|
| Metric: What is the availability of information for 3D objects/printing? | |
| **Measure item** | **Scale** |
| Print material | Unavailable 0% |
| Print colour | Sometime Available 01%-49% |
| Print texture | Often Available 50%-99% |
| Print constellation | Always Available 100% |
| Meta-data | |
| Explanations | |
| Meta-data such as access dates, author name , time stamps and other meta data. | |

**Refined metric for availability of services**: The metric for the availability of services has been refined using the expert review comments by making two modifications to the metric as shown in Table 8.33.

- The item available should be changed to always available.
- The scale should change from (Unavailable, Sometime Available, Often Available, Available) to (Unavailable 0%, Sometime Available 01%-49%, Often Available 50%-99%, Always Available) to accommodate percentages of availability.

Table 8.33: Metric for availability of services

| Component: Availability of Services ?Refers to the availability of services (i.e.: 3D scanners, 3D software, 3D printers) for 3D objects and 3D prints.? | |
|---|---|
| Metric: What is the availability of services for 3D objects/printing? | |
| **Measure item** | **Scale** |
| 3D Digitization service | Unavailable 0% |
| 3D Computing service | Sometime Available 01%-49% |
| 3D object Storage size | Often Available 50%-99% |
| 3D Printing services | Always Available 100% |
| 3D Print Storage size | |

**Refined metric for recovery rate of failed resources**: The metric for authenticity of identity has been refined using the expert review comments by making one modification to the metrics as shown in Table 8.34.

- 3D print storage was changed to 3D print storage size.

Table 8.34: Metric for recovery rate of failed resources

| Component: Availability of Services "Refers to the recovery rate of failed resources while producing 3D objects and 3D prints." | |
|---|---|
| Metric: What is the recovery period of failed resources for 3D objects/printing? | |
| **Measure item** | **Scale** |
| 3D Digitization service | Very Slow |
| 3D Computing service | Slow |
| 3D object Storage | Acceptable |
| 3D Printing services | Fast |
| 3D Print Storage size | Very Fast |

Table 8.31, Table 8.32, Table 8.33 and Table 8.34 are the final refined set of components and metrics for the availability component of the framework. Please note the scales the components were explained in the expert review also the reason the scales were incremental in percentages because measuring availability as a property for additive manufacturing is subjective and depends on the domain.

## 8.3 Information Authenticity Principle

This principle depends on three properties **authentication, integrity, and non-repudiation**. Since authentication and integrity have already been discussed in the previous sections, that leaves the non-repudiation property, to be discussed next.

### 8.3.1 Non-repudiation

The non-repudiation property has two components. **Data accuracy**: The metric for the data accuracy is **Is the information accuracy within objects enough to prove involvement in case of deniable actions against a lawful allegation?** This is a two-fold metric that asks:

- **"What kind of information is used as evidence to prove a claim?"**
- **"How accurate are these records?"**

The 3D printing technology and 3D printing material is a strong factor in the accuracy and consistency of a 3D print item. However, this metric is about measuring the non-repudiation, not establishing it. **Data consistency**: The metric for data consistency is **Is the information consistency within objects sufficient to prove involvement in case of deniable actions against a lawful allegation?** This is a two-fold metric that asks:

- **"The number information to provide as evidence?'**
- **"How consistent are these pieces of information?"**

**Statistical data for non-repudiation**: The statistical data in Table 8.35 and Table 8.36 confirms the proposed metrics for the above components, as none of the items or scale in the metrics have $p > 0.05$ as shown in the tables under Sig. (2-tailed) as all of them were $< 0.001$. The test for the metric was based on 4 points on a Likert scale therefore the mean was 2, the number of participants was N, the Mean was the average on scale of 4, the mean difference is the average above the mean of 2, standard deviation from the mean, and Sig. (2-tailed) stands for type one error.

Table 8.35: Expert review for Non-repudiation metrics - data accuracy

| Test Value for the statistical mean = 2 | | | | | | |
|---|---|---|---|---|---|---|
| **Measure** | **Items** | **N** | **Mean** | **Mean Diff.** | **Std. Dev.** | **Sig. (2-tailed)** |
| | 3D object | 12 | 3.58 | 1.58 | 0.52 | <0.001 |
| | Source of 3D object | 12 | 3.67 | 1.67 | 0.49 | <0.001 |
| | Information about the digital object | 12 | 3.5 | 1.5 | 0.52 | <0.001 |
| | 3D Print | 12 | 3.5 | 1.5 | 0.52 | <0.001 |
| | Source of 3D Print | 12 | 3.5 | 1.5 | 0.52 | <0.001 |
| | Information about the physical object | 12 | 3.58 | 1.58 | 0.52 | <0.001 |
| Scale | | 12 | 3.42 | 1.42 | 0.52 | <0.001 |

Table 8.36: Expert review for Non-repudiation metrics - data consistency

| Test Value for the statistical mean = 2 | | | | | | |
|---|---|---|---|---|---|---|
| **Measure** | **Items** | **N** | **Mean** | **Mean Diff.** | **Std. Dev.** | **Sig. (2-tailed)** |
| | 3D object | 12 | 3.58 | 1.58 | 0.52 | <0.001 |
| | Source of 3D object | 12 | 3.67 | 1.67 | 0.49 | <0.001 |
| | Information about the digital object | 12 | 3.58 | 1.58 | 0.52 | <0.001 |
| | 3D Print | 12 | 3.42 | 1.42 | 0.52 | <0.001 |
| | Source of 3D Print | 12 | 3.67 | 1.67 | 0.49 | <0.001 |
| | Information about the physical object | 12 | 3.58 | 1.58 | 0.52 | <0.001 |
| Scale | | 12 | 3.42 | 1.42 | 0.52 | <0.001 |

In Table 8.35 and Table 8.36, the lowest value was for (Scale) having mean difference of 1.42. Although the scale was confirmed, the review comments were taken into account and slight modification was made to the scale. Also in Table 8.35, the value of (3D Print) was the lowest at 1.42. Discussion in the focus group commented (on 3D Print) that

> "consistency is subject to the type of 3D printer to give consistent results". (Non-repudiation-Expert 1)

This research predicts that this will become less relevant in the future, as 3D printers become more accurate.

**Refined metric for data accuracy**: The metric for data accuracy for non-repudiation has been refined using the expert review comments by making one modification to the metrics, as shown in Table 8.37.

- The scale was changed from (No, Weak, Medium, Strong accuracy) to (Weak, Medium, Strong accuracy).

Table 8.37: Metric and measure for data accuracy

| Component: Data accuracy "refers to data accuracy when trying to establish non-repudiation". | |
|---|---|
| Metric: Is the information accuracy within objects enough to prove involvement in case of deniable actions against a lawful allegation? | |
| **Measure item** | **Scale** |
| 3D object | Weak accuracy |
| Source of 3D object | Medium accuracy |
| Information about the digital object | Strong accuracy |
| 3D Print | |
| Source of 3D Print | |
| Information about the physical object | |

**Refined metric for data consistency**: The metric for data consistency for non-repudiation has been refined using the expert review comments by making one modification to the metrics, as shown in Table 8.38.

- The was changed from (No, Weak, Medium, Strong consistency) to (Weak, Medium, Strong consistency).

Table 8.38: Metric and measure for data consistency

| Component: Data consistency "Refers to data consistency when trying to establish non-repudiation" | |
|---|---|
| Metric: Is the information consistency within objects is sufficient to prove involvement in case of deniable actions against a lawful allegation? | |
| **Measure item** | **Scale** |
| 3D object | Weak consistency |
| Source of 3D object | |
| Information about the digital object | Medium consistency |
| 3D Print | |
| Source of 3D Print | Strong consistency |
| Information about the physical object | |

Table 8.37 and Table 8.38 are the final refined set of components and metrics for the non-repudiation component of the framework.

## 8.4 Summary of the metric confirmation

The framework was built on seven security properties defined earlier. Through a GQM and refinement process, a number of components were extrapolated and later evaluated by the first expert review. The second expert review was longer and more comprehensive, and its main objective was to confirm and refine the proposed metrics. Through a refinement process similar to that used in section 6.2, the initial GQM metrics in 6 were refined and a task sheet was compiled. The task sheet was later given to the experts to rate the metrics and the scales. After completing the task sheet, the experts were then questioned on their responses. Their responses were recorded, then transcribed, anonymised, and grouped into expert points. The experts' transcribed comments, with the statistical data, were used to evaluate the initial proposed metrics in 7. The quantitative findings uncovered some overlooked metrics and refined the remainder in a similar way to the first expert review.

This objective was carried successfully and the result confirmed that the metrics were appropriate, sufficient, and complete, to measure the implementation of the components in a system that preserves the provenance of a 3D printed Object as it moves from the digital to the physical world and *vice-versa*. Combined with the first expert review, the results completed the triangulation of the research to achieve a confirmed framework. Evidence to support this claim are in sections 8.1, 8.2, and refinfor-auth, for component confirmation, as well as the data collected from the first expert review which is in 7.

# Chapter 9

# Prototyping and Validation

This chapter addresses the Fourth research objective:

> Validate the research by using the framework to build a software tool to assess the provenance of manufacturing operations.

This objective aims at answering the fourth research question "**Can the framework be used to provide a software requirement specification for provenance of additive manufacturing?**" This chapter builds on the result of the second expert review in chapter 8.

The findings of the second expert review will help in constructing the software requirement validation for the framework using prototyping. First, a paper-based prototype as shown in 9.2 is written to discover the software requirements from the stakeholders. This prototype is considered a skeleton for building a provenance tool this is described and built in section **??**. This chapter will address each security property described in 2.5, and explain how the tool operates to provide provenance. This prototype is the first step to building a functioning provenance system.

## 9.1 Prototyping additive manufacture tool - Dataflow

This research addressed cyber security procedures for AM and found a number of approaches, analysed in chapter 3, that work for some scenarios and fail for others. The data flow diagrams in Figure 3.1, Figure 3.2, Figure 3.3 and Figure 3.4 illustrated the process of satisfying the security principles. Figure 9.1 was generated from the analysis. Ideally, the combined data flows will satisfy the provenance requirements in fulfilling all the cyber security principles at the same time, and provide the overall functions for the theoretical framework.

The framework will provide the tools for the user to selectively benchmark provenance. If applied generally, it can be used to discriminate between authorised printing of 3D objects and unauthorised replicas, as well as benchmarking the security of the business that uses additive manufacturing. Also, if a new type of electronic tagging is needed, a single string can encapsulate the digital identity of the 3D object that can be added to the object's metadata for the 3D object file and fabricated with the 3D printed object, using methods described in the literature review, such as RFIDs, which also makes the framework domain-independent. The encapsulation takes the first class data, then the processed data secondly, then third class relationships, and assigns a special identifier, referred to as 3DOI.

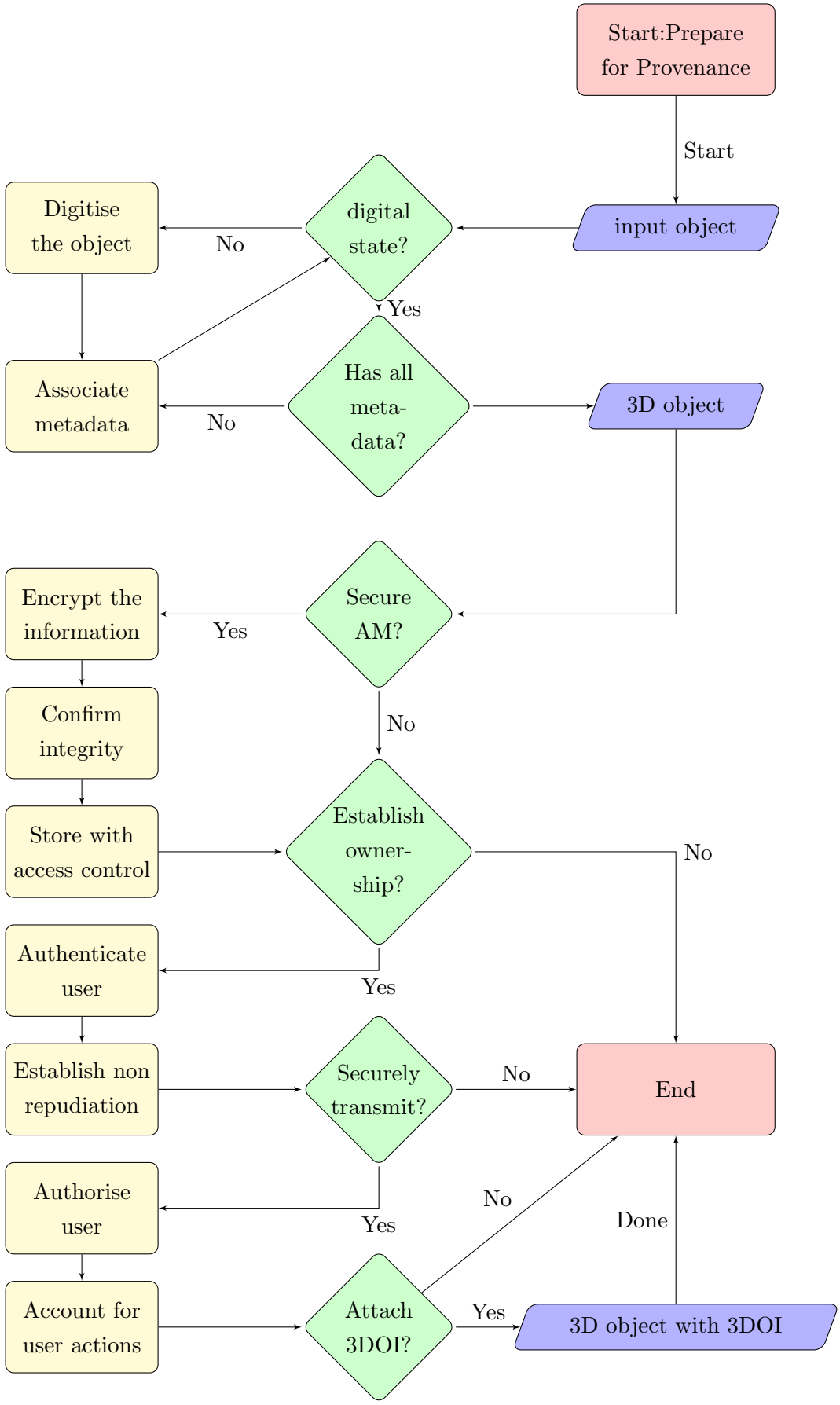



Figure 9.1: Provenance process for 3D objects and 3D prints

To understand the data flow and disambiguate how the use of security properties, the following scenario will explain how the security properties of the framework come into play when used to handle a product that has additive manufacturing as part of its production process. Security is like a building a wall: it needs the right foundation and building plan to have the right security measures in place.

**Analogy**

Imagine a scenario were Bob works for a military contractor that makes water safety valves. Bob is asked to get the new military valve specifications from a military base. The process of obtaining the information and the logical placement or usage of security properties can be summarised in seven steps.

**Step 1** When Bob arrives at the military base's gate he is asked to show identificationto **Authenticate** himself as Bob.

**Step 2** Bob is directed to the right facility based on his **Authorisation**.

**Step 3** Bob is assigned a military escort that accompanies him throughout his visit to watch over him and make sure that all of his actions are **Accounted** for.

**Step 4** Bob reaches the right facility and he is handed the new security valve designs in a briefcase with digital locks, to make sure that the information stays **Confidential**.

**Step 5** The briefcase is very strong and sturdy. The design of the briefcase makes sure anything inside remains intact and its **Integrity** is maintained.

**Step 6** Bob returns to his company and puts the briefcase in a safe where his superiors have access to it when they need it, as it has be **Available** at all times.

**Step 7** When the design documents are finally in the hands of the engineers, they inspect the schematics and verify the authenticity of the document through the military stamps and signatures on it, to make sure that these documents were undeniably from the military and the documents were **Non-Repudiated**.

Now imagine this process digitally handling 3D objects and 3D prints. The case study here is that bob needs to be able to protect any IP that is given and not leak any information that could compromise the agreement. At the same time bob supervisor is able to verify the IP was secure and trackable.

The following sections will build an initial paper-based prototype using the framework as the basis for the tool. This paper-based tool helps the stakeholders grasp the provenance system for additive manufacturing.

## 9.2 Prototyping additive manufacture tool

The research output described in chapters 7 and 8 is turned into a tool to investigate security of additive manufacturing. This tool has two interface:

**The inputs**: is a form that has process on one side and a scale of how good or how strong the security property for that process is.

**The outputs**: is a spider diagram that describes the overall strength/coverage of a security property. The figures described in Appendix B are drawn by semantic modelling using PROV-N with cyber-to-physical taxonomy. These figures will act as a template to map the additive manufacturing process, threats, and hardening measures, to protect an organisation. There are three sets for each security property.

- The First set is a description of the additive manufacturing process.
- The Second set is the additive manufacturing process with possible attacks highlighted in red.
- The Third set is the threatened additive manufacturing process with the framework highlighted in green.

### 9.2.1 Authentication

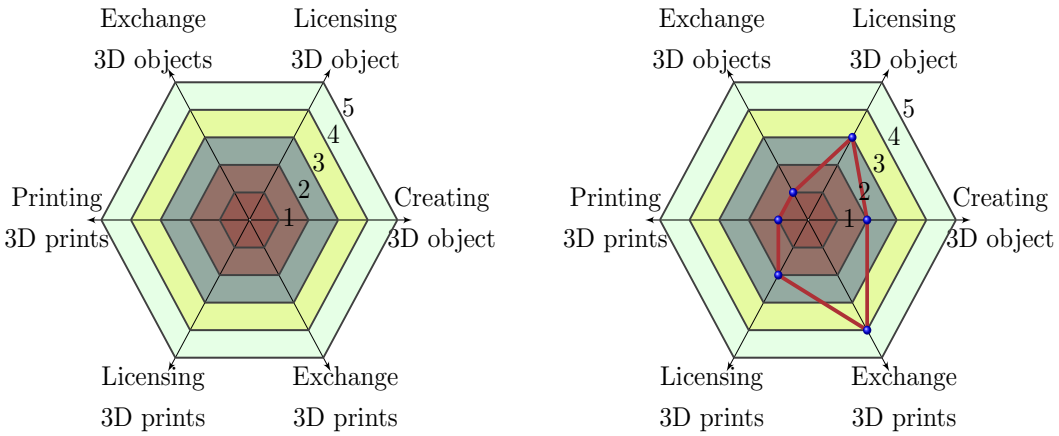
The authentication property, described in 2.5, briefly means to validate a claim of identity (I am who I claim to be). In additive manufacturing, the authentication property is required for three types of process creating, exchanging, and licensing of 3D objects or 3D printed objects. As described in chapter 7, this authentication has three components:

**Strength of the authentication protocol** means the type of authentication that is used for creating, exchanging, and licensing 3D objects and 3D prints. The metric for this component will provide: the type of authentication, and what type of objects are created, exchanged and licensed. The user of the tool will employ Table 9.1 to input the data.

Table 9.1: Tool for measuring the strength of authentication protocol

| How strong are the authentication for | No authentication | Something you know | Something you have | Something you are | Hybrid of previous |
|---|---|---|---|---|---|
| Creating 3D object? | 1 | 2 | 3 | 4 | 5 |
| Licensing 3D object? | 1 | 2 | 3 | 4 | 5 |
| Exchange 3D objects? | 1 | 2 | 3 | 4 | 5 |
| Printing 3D prints? | 1 | 2 | 3 | 4 | 5 |
| Licensing 3D prints? | 1 | 2 | 3 | 4 | 5 |
| Exchange 3D prints? | 1 | 2 | 3 | 4 | 5 |

Once the data is entered, a spider diagram is generated to reflect the strength of the authentication, as shown in Figure 9.2. The further away from the centre of the spider diagram, the stronger the authentication.




(a) Spider diagram visual tool

(b) Spider diagram example

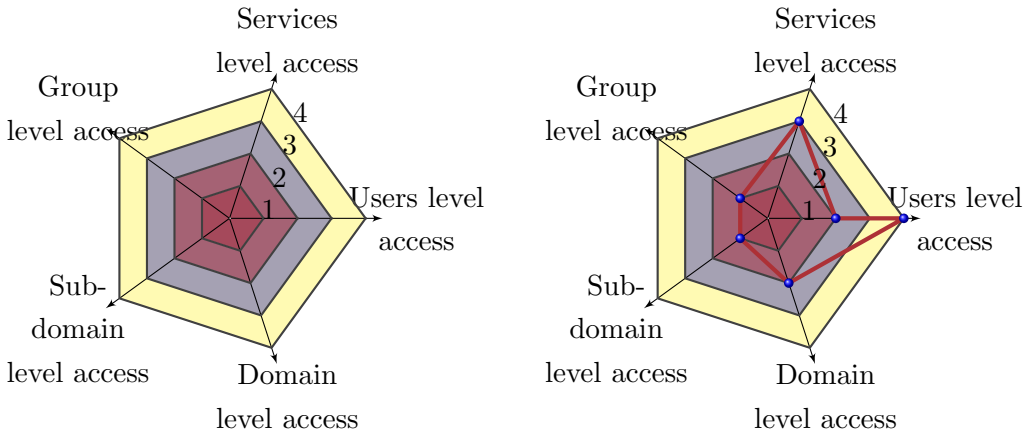
Figure 9.2: Strength of the authentication protocol spider diagram

**Authenticity of data source** means the direct access to raw material, computing power or physical resources. Typically, access to resources within an organisation or a company is classified and access provided on a personal, group or corporate level. The metric for this component will provide the authenticated party (can be a person, a service, group of people, group of people belonging to a sub-domain or open access to anyone in a certain domain), and the percentage of employees that are required to authenticate. The user of the tool will employ Table 9.2 to input the data.

Table 9.2: Tool for measuring the authenticated access to resources

| Is authenticationto access resources recorded on | 0% information recorded | 01%–49% Some information recorded | 50%–99% Most information recorded | 100% Information recorded |
|---|---|---|---|---|
| Users level access? | 1 | 2 | 3 | 4 |
| Users using Services access level [1]? | 1 | 2 | 3 | 4 |
| Group level access? | 1 | 2 | 3 | 4 |
| Sub-domain level access? | 1 | 2 | 3 | 4 |
| Licensing 3D prints? | 1 | 2 | 3 | 4 |
| Domain level access (Highest access level) ? | 1 | 2 | 3 | 4 |

Once the data is entered, a spider diagram is generated to reflect the authentication of resources, as shown in Figure 9.3. The further away from the centre the stronger the authentication of resources.




(a) Spider diagram visual tool

(b) Spider diagram example

Figure 9.3: Authenticated access to resources spider diagram

**Authenticity of information** means being able to prove the origin of a 3D object or 3D print, even if its damaged or faulty. The metric for this component will provide whether the organisation handles 3D object or 3D print or both, and how valuable the object is in terms of information that it could give about its origin or usage. Table 9.3 is the input form to help confirm the authenticity of functional and non-functional objects, and it

[1](i.e.: 3D printing users, computing resources users)

has two sub-tables, depending on the nature of what is produced: if it is a functional or a non-functional object. Non-functional objects that have aesthetic properties that make them unique.

Table 9.3: Tool for measuring the authenticity of information

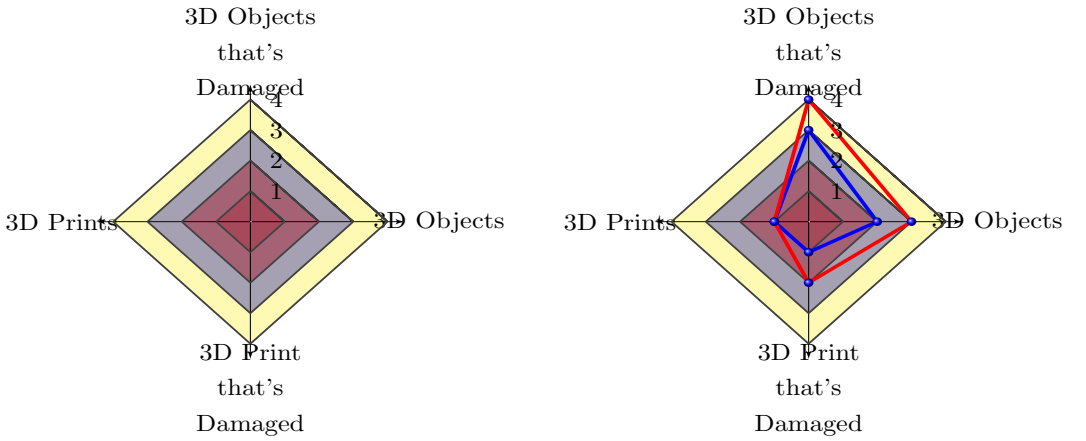
(a) Functional objects and prints

| In what state can you still confirm the authenticity of a functional | 0% Unusable | 01%-49% Partially Unusable | 50%-99% Mostly Unusable | 100% Usable |
|---|---|---|---|---|
| 3D Objects? | 1 | 2 | 3 | 4 |
| 3D Objects that's Damaged? | 1 | 2 | 3 | 4 |
| 3D Prints? | 1 | 2 | 3 | 4 |
| 3D Print that's Damaged? | 1 | 2 | 3 | 4 |

(b) Non-Functional objects and prints

| In what state can you still confirm the authenticity of a non-functional | 0% Unrecoverable | 01%-49% Partially recoverable | 50%-99% Mostly recoverable | 100% Recoverable |
|---|---|---|---|---|
| 3D Objects? | 1 | 2 | 3 | 4 |
| 3D Objects that's Damaged? | 1 | 2 | 3 | 4 |
| 3D Prints? | 1 | 2 | 3 | 4 |
| 3D Print that's Damaged? | 1 | 2 | 3 | 4 |

Once the data is entered, a spider diagram is generated to reflect the authentication of information, as shown in Figure 9.4. The further away from the centre of the spider diagram, the more information could be retrieved.




(a) Spider diagram visual tool

(b) Spider diagram example, Blue for functional and red for non functional

Figure 9.4: Authenticated access to information spider diagram

The results from the abovementioned components are mapped onto the template in Appendix Figure B.3, which is a graphical presentation of threats and placement of recommendations.

### 9.2.2 Authorisation

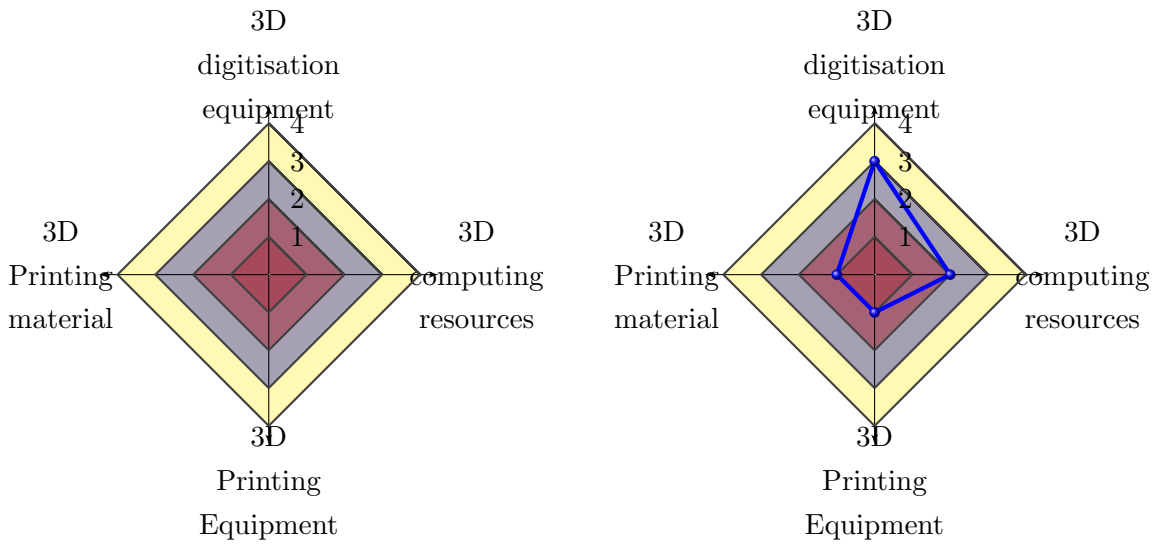
The authorisation property, described in 2.5, briefly means giving authority to people, a group of people, or service, to do something. In additive manufacturing, the authorisation property is required for three types of process: 3D scanning, 3D printing, and 3D design of 3D objects or 3D printed objects. As described in chapter 7, the authentication has two components.

**Authorisation of resources** means to authorise someone or something to use hardware or physical resources to 3D scan, 3D print, and 3D design, to create any 3D object or 3D print. The metric for this component will provide data identifying the type of resources used, and the state of authorisation policies in place. Table 9.4 is the input form to help identify the kind of authorisation of resources.

Table 9.4: Tool for measuring the authorisation of resources

| What kind of authorisation is required for | No identification | Identification exists but not required | Identification exists and required | Authorisation exists and required |
|---|---|---|---|---|
| 3D computing resources? | 1 | 2 | 3 | 4 |
| 3D digitisation equipment? | 1 | 2 | 3 | 4 |
| 3D Printing material? | 1 | 2 | 3 | 4 |
| 3D Printing Equipment? | 1 | 2 | 3 | 4 |

Once the data is entered, a spider diagram is generated to reflect the authorisation of resources, as shown in Figure 9.5. The further away from the centre of the spider diagram, the stricter the authorisation.




(a) Spider diagram visual tool

(b) Spider diagram example

Figure 9.5: authorisationto resources spider diagram

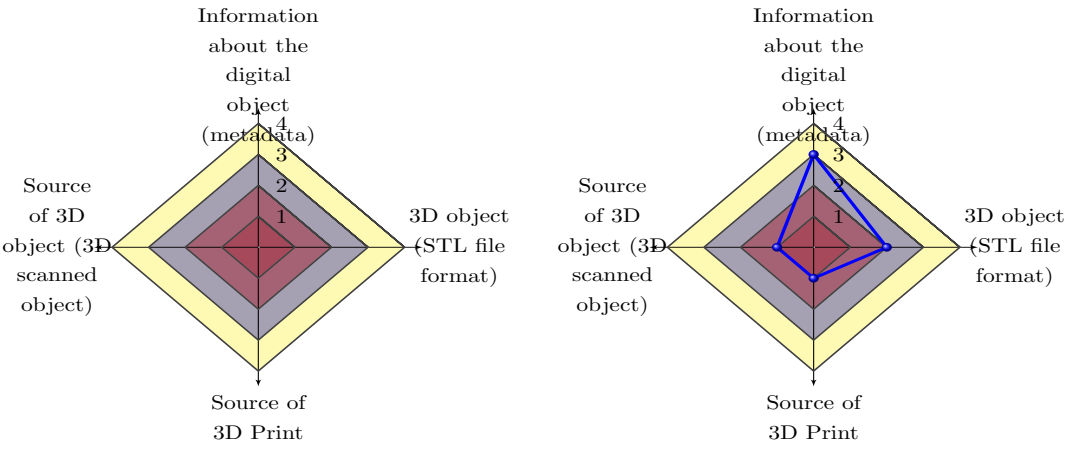
**Authorisationto access confidential information** means restrictions applied to entities that are either used or generated by additive manufacturing. The metric for this component will provide the type of entities and records that an organisation uses, and the restriction policies in place. This is split into two parts one for digital records and

one for physical records, as the restrictions are different. Table 9.5 is the input form for the digital entities and Table 9.6 for physical entities.

Table 9.5: Tool for measuring the authorisation for resources

| What kind of restrictions for | Read, Write, Delete & 3D Print | Read, Write & Delete | Read & Write | Read |
|---|---|---|---|---|
| 3D object (STL file format)? | 1 | 2 | 3 | 4 |
| Information about the digital object (metadata)? | 1 | 2 | 3 | 4 |
| Source of 3D object (3D scanned object)? | 1 | 2 | 3 | 4 |
| Source of 3D Print? | 1 | 2 | 3 | 4 |

Once the data is entered, a spider diagram is generated to reflect the authorisationto access **digital** confidential information, as shown in Figure 9.6. The further away from the centre of the spider diagram, the stricter the authorisation for digital assets.




(a) Spider diagram visual tool

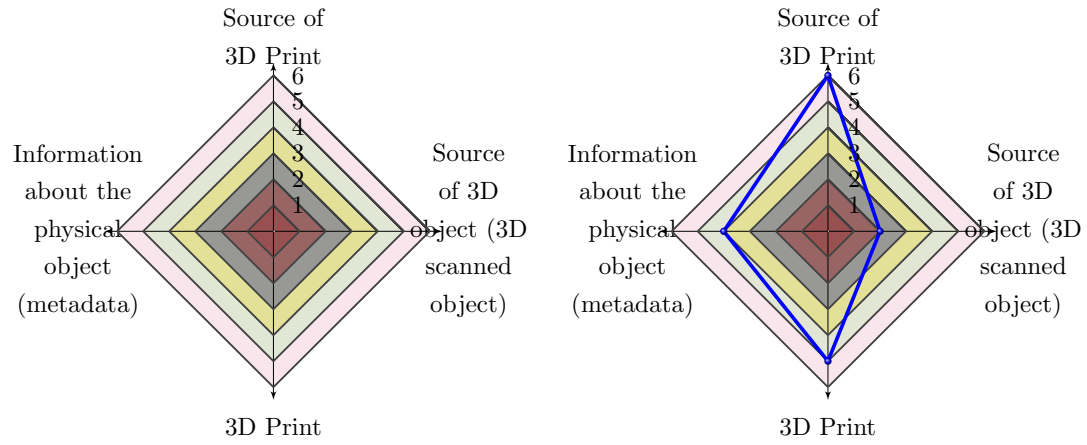
(b) Spider diagram example

Figure 9.6: authorisationto access confidential information spider diagram

Table 9.6: Tool for measuring the authorisation of confidential information

| What kind of restrictions for | Access control list | Lattice-based Access Control | Rule-Based Access Control | Role-Based Access Control | Discretionary Access Control | Mandatory Access Control |
|---|---|---|---|---|---|---|
| Source of 3D object (3D scanned object)? | 1 | 2 | 3 | 4 | 5 | 6 |
| Source of 3D Print? | 1 | 2 | 3 | 4 | 5 | 6 |
| Information about the physical object (metadata)? | 1 | 2 | 3 | 4 | 5 | 6 |
| 3D Print? | 1 | 2 | 3 | 4 | 5 | 6 |

Once the data is entered, a spider diagram is generated to reflect the authorisationto access **physical** confidential information, as shown in Figure 9.7. The further away from the centre of the spider diagram, the stricter the authorisation for physical assets.




(a) Spider diagram visual tool

(b) Spider diagram example

Figure 9.7: authorisation of confidential information spider diagram

The results from the abovementioned components are mapped onto the template in Appendix Figure B.6 which is a graphical presentation of threats and placement of recommendations.

### 9.2.3 Accounting

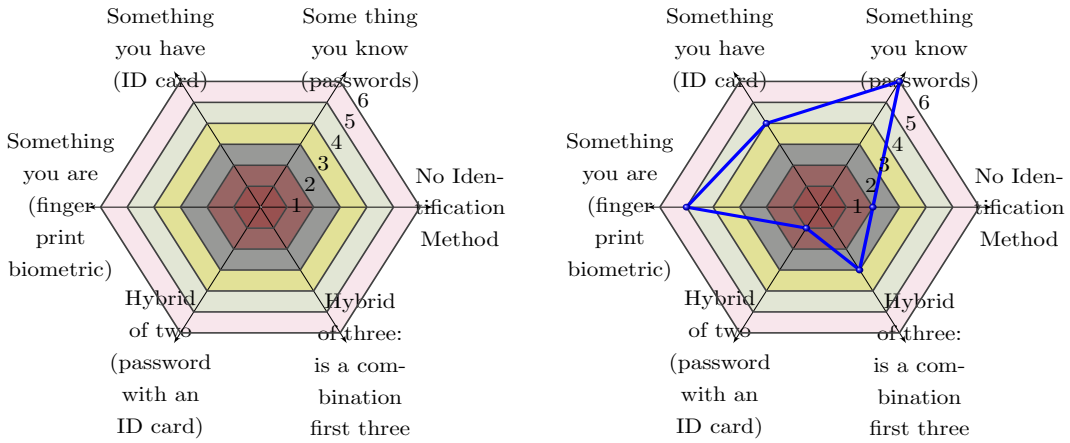
The accounting process, described in 2.5, briefly means finding out who did what and when. In additive manufacturing, the accounting property is required for two types of process CRUD "create, read, update, and delete" for digital functions, and 3D printing for physical functions. As described in chapter 7, the accounting has three components.

**The identification component** means being able to identify who did something to an entity. The metric for this component will provide what identification method is used, and how strong the identification is. Table 9.7 is the input form to help identify the accounting type.

Table 9.7: Tool for measuring the strength of accounting identification

| How strong is the identification for | Null | Very Weak | Weak | Medium | Strong | Very Strong |
|---|---|---|---|---|---|---|
| Some thing you know (passwords)? | 1 | 2 | 3 | 4 | 5 | 6 |
| Something you have (ID card)? | 1 | 2 | 3 | 4 | 5 | 6 |
| Something you are (finger print biometric)? | 1 | 2 | 3 | 4 | 5 | 6 |
| Hybrid of two (password with an ID card)? | 1 | 2 | 3 | 4 | 5 | 6 |
| Hybrid of three: is a combination first three? | 1 | 2 | 3 | 4 | 5 | 6 |

Once the data is entered, a spider diagram is generated to reflect the accounting for identity, as shown in Figure 9.8. The further away from the centre of the spider diagram, the stronger the accounting for identity.




(a) Spider diagram visual tool

(b) Spider diagram example

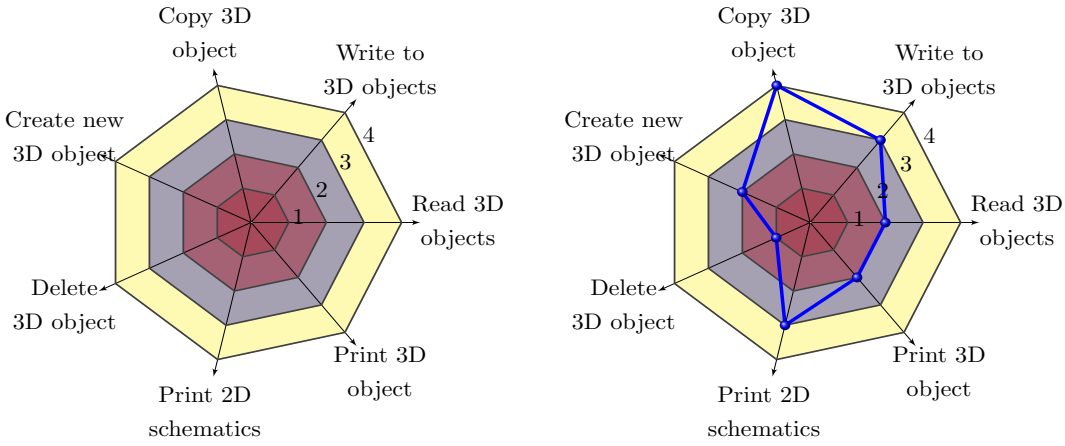
Figure 9.8: accounting identification strength spider diagram

**The protocol component** means to account for an action operating on 3D objects and 3D prints. The metric for this component will provide for identifying the actions performed, and how well information taken are recorded. Table 9.8 is the input form to help measure the accounting protocol's strength.

Table 9.8: Tool for measuring the accounting protocols strength

| What kind of restrictions for | 0% No information is recorded | 01%-49% Some information is recorded | 50%-99% Most information is recorded | 100% Information is recorded all the time |
|---|---|---|---|---|
| Read 3D objects | 1 | 2 | 3 | 4 |
| Write to 3D objects | 1 | 2 | 3 | 4 |
| Copy 3D object | 1 | 2 | 3 | 4 |
| Create new 3D object | 1 | 2 | 3 | 4 |
| Delete 3D object. | 1 | 2 | 3 | 4 |
| Print 2D schematics | 1 | 2 | 3 | 4 |
| Print 3D object | 1 | 2 | 3 | 4 |

Once the data is entered, a spider diagram is generated to reflect the accounting protocol's strength, as shown in Figure 9.9. The further away from the centre of the spider diagram, the more information is recorded and accounted for.




(a) Spider diagram visual tool

(b) Spider diagram example

Figure 9.9: accounting protocols strength spider diagram

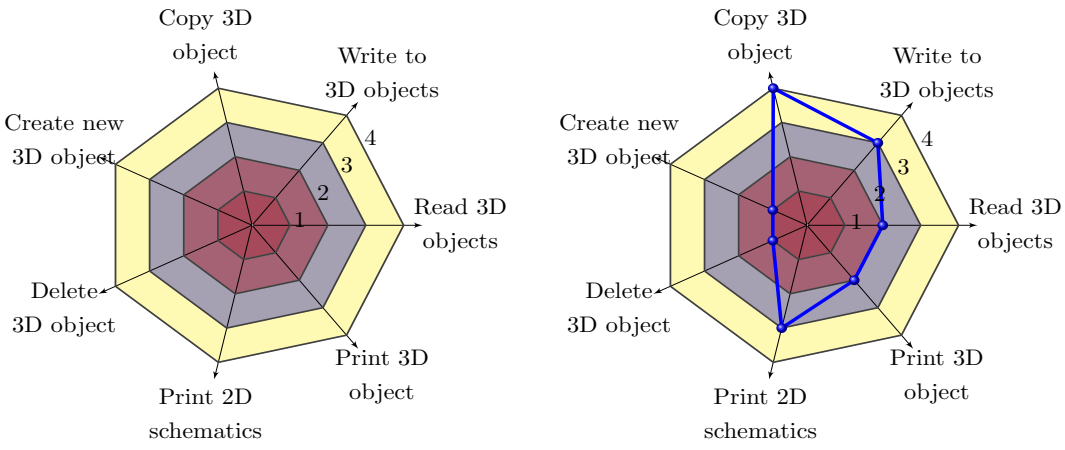
**The timestamp component** means to account for when an action acted on 3D objects and 3D prints. The metric for this component will provide the type of assets that timing is accounted for, and how well information taken are recorded. Table 9.9 is the input form to help measure the accounting protocol's strength.

Table 9.9: Tool for measuring the accounting timestamp

| What are the timestamps that are being audited (recorded) for | 0% No information is recorded | 01%-49% Some information is recorded | 50%-99% Most information is recorded | 100% Information is recorded all the time |
|---|---|---|---|---|
| Read 3D objects | 1 | 2 | 3 | 4 |
| Write to 3D objects | 1 | 2 | 3 | 4 |
| Copy 3D object | 1 | 2 | 3 | 4 |
| Create new 3D object | 1 | 2 | 3 | 4 |
| Delete 3D object. | 1 | 2 | 3 | 4 |
| Print 2D schematics | 1 | 2 | 3 | 4 |
| Print 3D object | 1 | 2 | 3 | 4 |

Once the data is entered, a spider diagram is generated to reflect accounting timestamp, as shown in Figure 9.10. The further away from the centre of the spider diagram, the

more information could be retrieved.




(a) Spider diagram visual tool

(b) Spider diagram example

Figure 9.10: accounting timestamp spider diagram

The results from the abovementioned components are mapped onto the template in Appendix Figure B.9 which is a graphical presentation of threats and placement of recommendations.

### 9.2.4 Availability

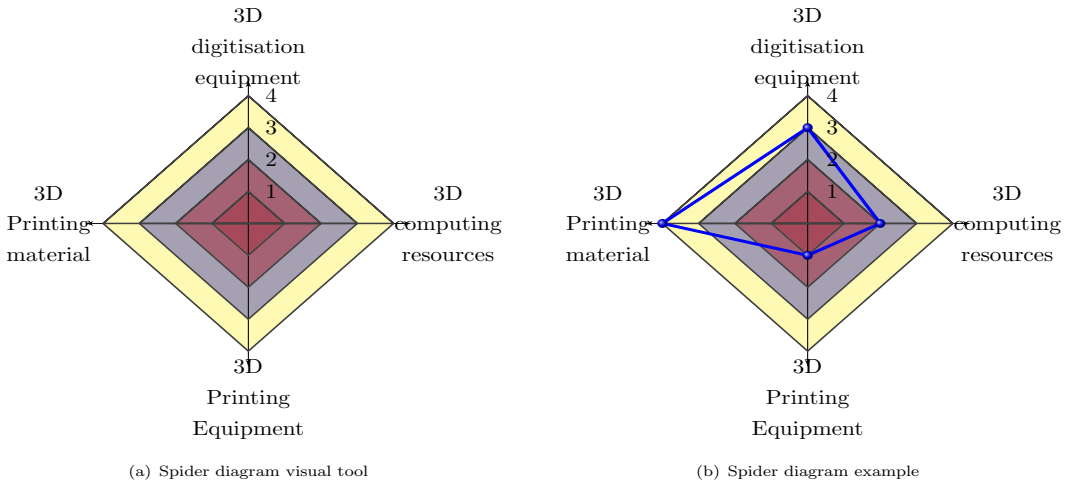
The availability property, described in 2.5, briefly means making sure that the information is present when needed. It also refers to the availably of services. In additive manufacturing, the accounting property is required for four types of process: 3D scanning, 3D design, 3D printing, and storage for 3D objects and 3D prints. As described in chapter 7, the accounting has four components.

**Availability of resources** means to make additive manufacturing resources available when needed. The metric for this component will provide the type of resources available in the organisation, and how often these resource are available. Table 9.10 is the input form to help identify availability of resources.

Table 9.10: Tool for measuring the availability of resources

| What is the availability of resources for | 0% Unavailable | 01%-49% Sometime Available | 50%-99% Often Available | 100% Always Available |
|---|---|---|---|---|
| 3D computing resources | 1 | 2 | 3 | 4 |
| 3D digitisation equipment | 1 | 2 | 3 | 4 |
| 3D Printing material | 1 | 2 | 3 | 4 |
| 3D Printing Equipment | 1 | 2 | 3 | 4 |

Once the data is entered, a spider diagram is generated to reflect the availability of resources, as shown in Figure 9.11. The further away from the centre of the spider diagram, the more available the resources are.




(a) Spider diagram visual tool

(b) Spider diagram example

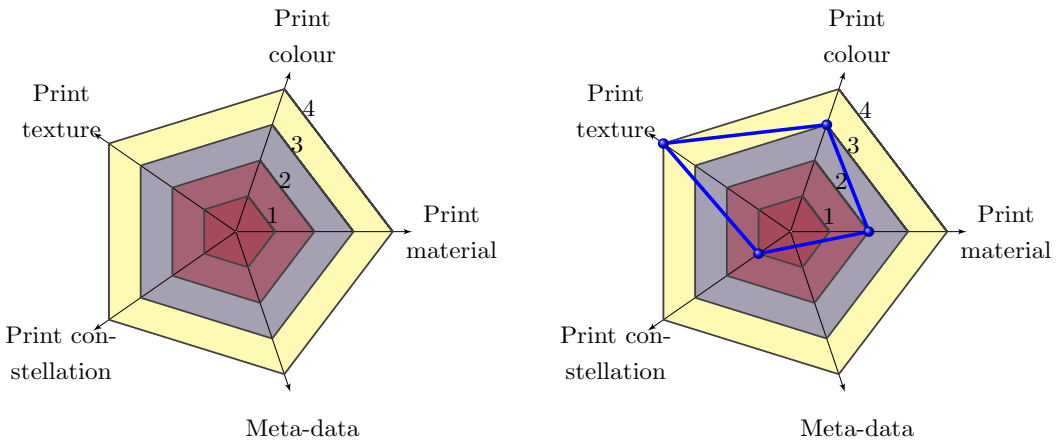
Figure 9.11: availability of resources spider diagram

**Availability of information** means to make additive manufacturing information available when needed. The metric for this component will provide the type of information available for additive manufacturing, and how often these pieces of information are available. Table 9.11 is the input form to help identify availability of information.

Table 9.11: Tool for measuring the availability of information

| What is the availability of information for | 0% Unavailable | 01%-49% Sometime Available | 50%-99% Often Available | 100% Always Available |
|---|---|---|---|---|
| Print material | 1 | 2 | 3 | 4 |
| Print colour | 1 | 2 | 3 | 4 |
| Print texture | 1 | 2 | 3 | 4 |
| Print constellation | 1 | 2 | 3 | 4 |
| Meta-data | 1 | 2 | 3 | 4 |

Once the data is entered, a spider diagram is generated to reflect the availability of information, as shown in Figure 9.12. The further away from the centre of the spider diagram, the more available the information is.




(a) Spider diagram visual tool

(b) Spider diagram example

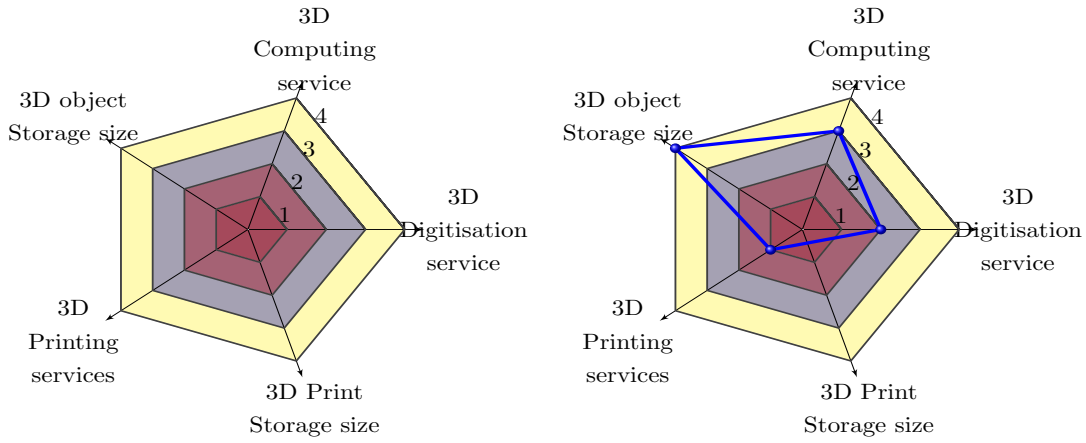
Figure 9.12: Availability of information spider diagram

**Availability of services** means to make additive manufacturing services available when needed. The metric for this component will provide the type of services available for additive manufacturing, and how often these services are available. Table 9.12 is the input form to help identify availability of services.

Table 9.12: Tool for measuring the availability of services

| What is the availability of services for | 0% Unavailable | 01%-49% Sometime Available | 50%-99% Often Available | 100% Always Available |
|---|---|---|---|---|
| 3D Digitisation service | 1 | 2 | 3 | 4 |
| 3D Computing service | 1 | 2 | 3 | 4 |
| 3D object Storage size | 1 | 2 | 3 | 4 |
| 3D Printing services | 1 | 2 | 3 | 4 |
| 3D Print Storage size | 1 | 2 | 3 | 4 |

Once the data is entered, a spider diagram is generated to reflect the availability of services, as shown in Figure 9.13. The further away from the centre of the spider diagram, the more available the services are.




(a) Spider diagram visual tool

(b) Spider diagram example

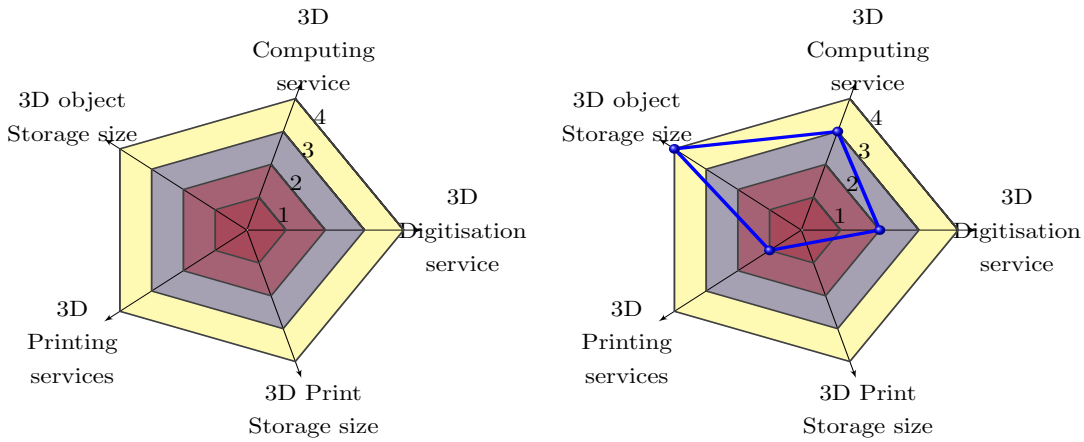
Figure 9.13: Availability of services spider diagram

**Recovery rate of failed resources** means the ability to recover after a failure of a service that is part of the additive manufacturing process. The metric for this component will provide the services that have recovery mechanisms that are part of additive manufacturing, and how fast these services recover. Table 9.13 is the input form to help measure the recovery rate of failed resources.

Table 9.13: Tool for measuring the recovery rate of failed resources

| What is the availability of services for | Very Slow | Slow | Acceptable | Fast | Very Fast |
|---|---|---|---|---|---|
| 3D Digitisation service | 1 | 2 | 3 | 4 | 5 |
| 3D Computing service | 1 | 2 | 3 | 4 | 5 |
| 3D object Storage size | 1 | 2 | 3 | 4 | 5 |
| 3D Printing services | 1 | 2 | 3 | 4 | 5 |
| 3D Print Storage size | 1 | 2 | 3 | 4 | 5 |

Once the data is entered, a spider diagram is generated to reflect the recovery of services, as shown in Figure 9.14. The further away from the centre of the spider diagram, the faster services recover.




(a) Spider diagram visual tool

(b) Spider diagram example

Figure 9.14: Recovery rate of failed resources spider diagram

The results from the abovementioned components are mapped onto the template in Appendix Figure B.12, which is a graphical presentation of threats and placement of recommendations.

### 9.2.5 Confidentiality

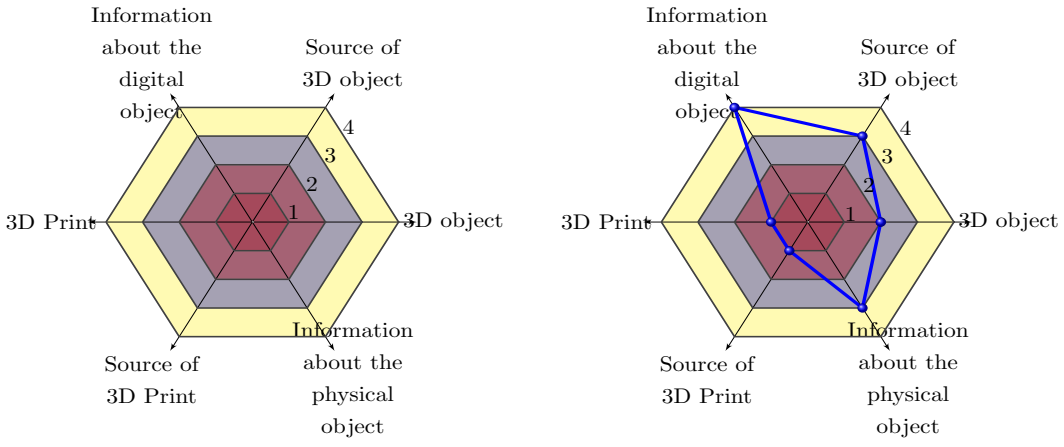
The confidentiality property, described in 2.5, briefly means to make sure that nothing is disclosed without permission. In additive manufacturing, the confidentiality property is required for two types of process: sharing, and storing 3D objects and 3D prints. As described in chapter 7, the authentication has two components.

**Disclosure of confidential information** means how to disclose information that is part of the additive manufacturing process. The metric for this component will provide the type of confidential information types the organisation discloses, and the kind of confidentiality disclosure the organisation supports. Table 9.14 is the input form to help identify the strength of disclosure of confidential information.

Table 9.14: Tool for measuring the disclosure of confidential information

| To whom confidential information is disclosed for | Individuals | Groups | Internal organisation | Public |
|---|---|---|---|---|
| 3D object (STL file format) | 1 | 2 | 3 | 4 |
| Source of 3D object (3D scanned object) | 1 | 2 | 3 | 4 |
| Information about the digital object (metadata) | 1 | 2 | 3 | 4 |
| 3D Print | 1 | 2 | 3 | 4 |
| Source of 3D Print | 1 | 2 | 3 | 4 |
| Information about the physical object (metadata) | 1 | 2 | 3 | 4 |

Once the data is entered, a spider diagram is generated to reflect the disclosure of confidential information, as shown in Figure 9.15. The further away from the centre of the spider diagram, the more disclosure there is.




(a) Spider diagram visual tool

(b) Spider diagram example

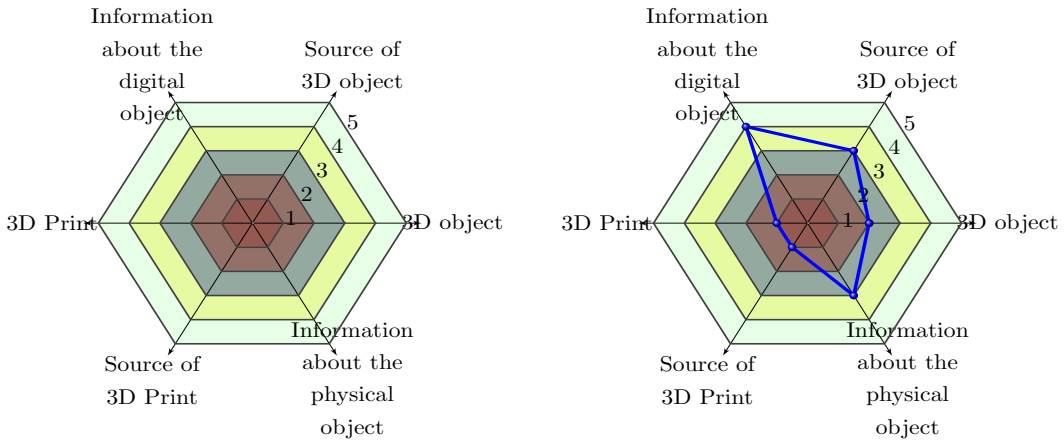
Figure 9.15: disclosure of confidential information spider diagram

**Strength of confidentiality measures** means the strength of security protocol that is used by the organisation to protect 3D objects and 3D prints. The metric for this component will provide the type of confidential information the organisation secures, and how strong the confidentiality measures are. Table 9.15 is the input form to help identify the strength of confidentiality measures.

Table 9.15: Tool for measuring the strength of confidentiality

| How strong are the security measures to protect | No confidentiality measures | Weak confidentiality measures | Medium confidentiality measures | Strong confidentiality measures | Very Strong confidentiality measures |
|---|---|---|---|---|---|
| 3D object (STL file format) | 1 | 2 | 3 | 4 | 5 |
| Source of 3D object (3D scanned object) | 1 | 2 | 3 | 4 | 5 |
| Information about the digital object (metadata) | 1 | 2 | 3 | 4 | 5 |
| 3D Print | 1 | 2 | 3 | 4 | 5 |
| Source of 3D Print | 1 | 2 | 3 | 4 | 5 |
| Information about the physical object (metadata) | 1 | 2 | 3 | 4 | 5 |

Once the data is entered, a spider diagram is generated to reflect the strength of confidentiality measures, as shown in Figure 9.16. The further away from the centre of the spider diagram, the stronger the confidentiality.




(a) Spider diagram visual tool

(b) Spider diagram example

Figure 9.16: Strength of confidentiality spider diagram

The results from the abovementioned components are mapped onto the template in Appendix Figure B.15, which is a graphical presentation of threats and placement of recommendations.

### 9.2.6 Integrity

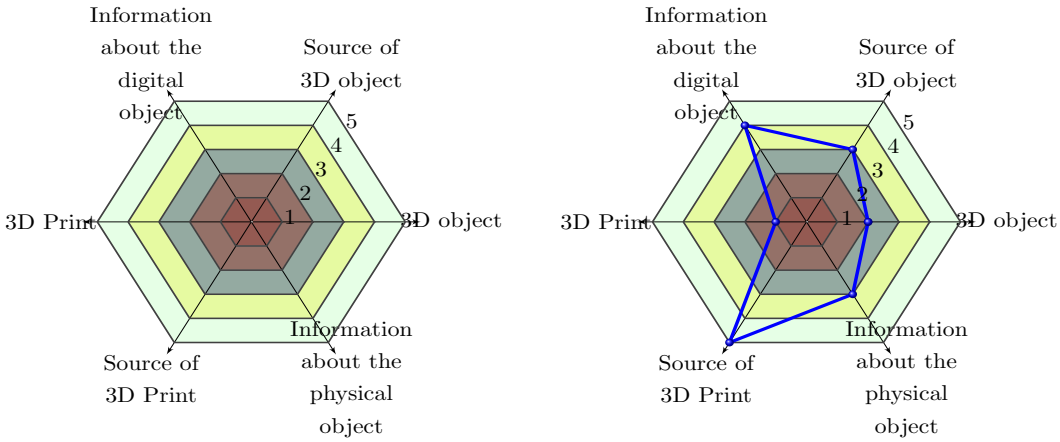
The integrity property, described in 2.5, briefly means to make sure that the information that is a part of the additive manufacturing process is maintained and disposed of properly. The integrity property is required for two types of process: backups, and disposal of 3D objects and 3D prints. As described in chapter 7, the integrity has three components.

**Data maintenance for data integrity** means maintaining valuable information whether the data is digital or physical. The metric for this component will provide the type of information the organisation maintains, and how well the assets are protected. Table 9.16 is the input form to help measure data maintenance.

Table 9.16: Tool for measuring data maintenance for data integrity

| How secure is the storage of | No secure storage | Weak secure storage | Medium secure storage | Strong secure storage | Extra Strong secure storage |
|---|---|---|---|---|---|
| 3D object (STL file format) | 1 | 2 | 3 | 4 | 5 |
| Source of 3D object (3D scanned object) | 1 | 2 | 3 | 4 | 5 |
| Information about the digital object (metadata) | 1 | 2 | 3 | 4 | 5 |
| 3D Print | 1 | 2 | 3 | 4 | 5 |
| Source of 3D Print | 1 | 2 | 3 | 4 | 5 |
| Information about the physical object (metadata) | 1 | 2 | 3 | 4 | 5 |

Once the data is entered, a spider diagram is generated to reflect the data maintenance, as shown in Figure 9.17. The further away from the centre of the spider diagram, the stronger the storage is.




(a) Spider diagram visual tool

(b) Spider diagram example

Figure 9.17: Data maintenance for data integrity spider diagram

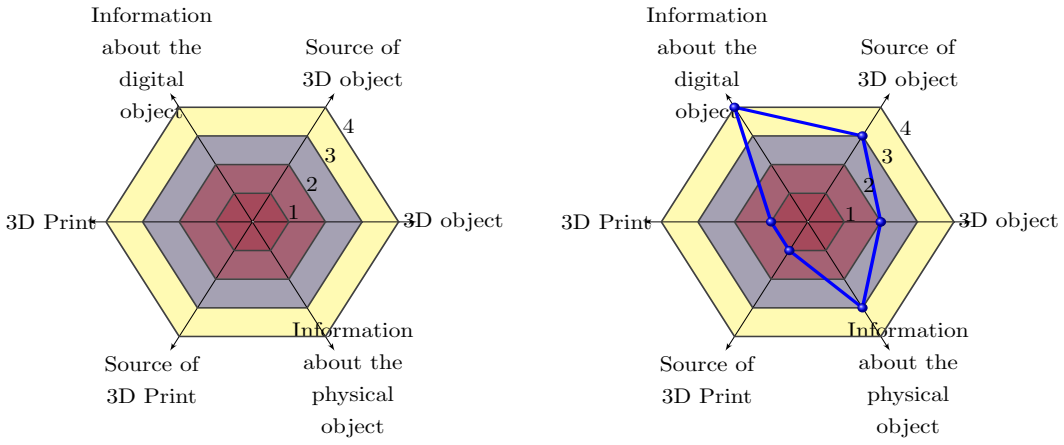
**Secure disposal of information** means making sure that nothing leaks out of the organisation, and having secure disposal policies in place. The metric for this component will provide the type of sensitive information that needs secure disposal, and how strong

the current disposal policies are. Table 9.17 is the input form to help show the strength of the disposal policies.

Table 9.17: Tool for measuring the secure disposal of information

| How secure is the disposal of | No secure disposal | Weak secure disposal | Medium disposal storage | Strong secure disposal |
|---|---|---|---|---|
| 3D object (STL file format) | 1 | 2 | 3 | 4 |
| Source of 3D object (3D scanned object) | 1 | 2 | 3 | 4 |
| Information about the digital object (metadata) | 1 | 2 | 3 | 4 |
| 3D Print | 1 | 2 | 3 | 4 |
| Source of 3D Print | 1 | 2 | 3 | 4 |
| Information about the physical object (metadata) | 1 | 2 | 3 | 4 |

Once the data is entered, a spider diagram is generated to reflect secure disposal of information, as shown in Figure 9.2. The further away from the centre of the spider diagram, the stronger the disposal.




(a) Spider diagram visual tool

(b) Spider diagram example

Figure 9.18: Secure disposal of information spider diagram

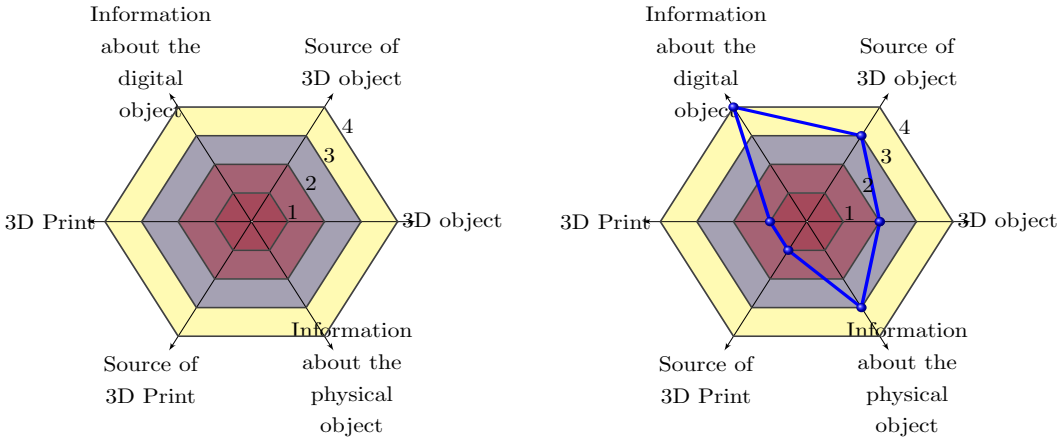
**Backup frequency** means how often regular backups of 3D objects and 3D prints are made. The metric for this component will provide the assets that need backups, and

how strong the backup policies are. Table 9.18 is the input form to help identify backup frequency.

Table 9.18: Tool for measuring the backup frequency

| How frequent is the backup process of | No backup | Low frequency backup | Medium frequency backup | Strong frequency backup |
|---|---|---|---|---|
| 3D object (STL file format) | 1 | 2 | 3 | 4 |
| Source of 3D object (3D scanned object) | 1 | 2 | 3 | 4 |
| Information about the digital object (metadata) | 1 | 2 | 3 | 4 |
| 3D Print | 1 | 2 | 3 | 4 |
| Source of 3D Print | 1 | 2 | 3 | 4 |
| Information about the physical object (metadata) | 1 | 2 | 3 | 4 |

Once the data is entered, a spider diagram is generated to reflect the backup frequency of assets, as shown in Figure 9.19. The further away from the centre of the spider diagram, the stronger the backup policy.




(a) Spider diagram visual tool

(b) Spider diagram example

Figure 9.19: backup frequency spider diagram

The results from the abovementioned components are mapped onto the template in Appendix Figure B.18, which is a graphical presentation of threats and placement of recommendations.

### 9.2.7 Non-repudiation

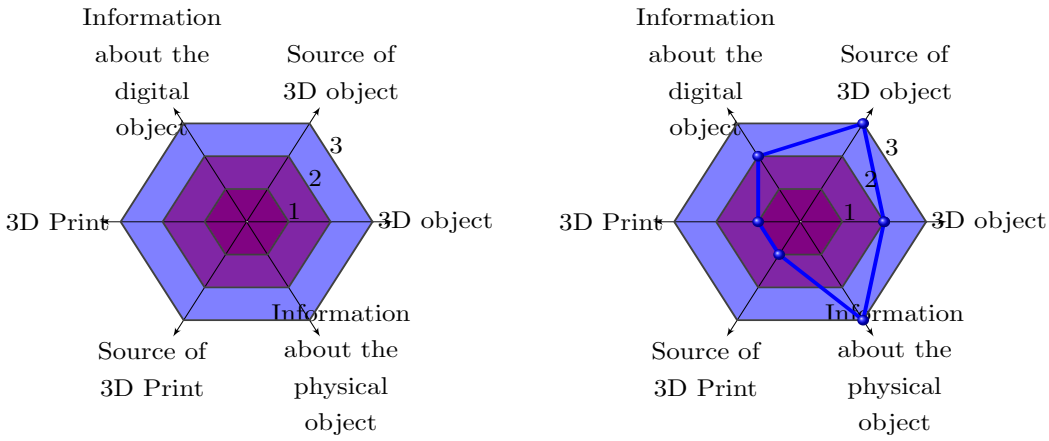
The non-repudiation property, described in 2.5, briefly means proving an event has undeniably happened, and was operated by a certain individual or service. In additive manufacturing, the non-repudiation property is required for two types of process: data consistency checks, and verification for 3D objects and 3D prints. As described in chapter 7, the accounting has two components.

**Data accuracy** means maintaining the accuracy of information when using additive manufacturing. The metric for this component will provide what kind of information is used as evidence to prove data accuracy, and how accurate the evidence record is. Table 9.19 is the input form to help measure data accuracy.

Table 9.19: Tool for measuring the data accuracy

| How accurate is the information for | Weak accuracy | Medium accuracy | Strong accuracy |
|---|---|---|---|
| 3D object (STL file format) | 1 | 2 | 3 |
| Source of 3D object (3D scanned object) | 1 | 2 | 3 |
| Information about the digital object (metadata) | 1 | 2 | 3 |
| 3D Print | 1 | 2 | 3 |
| Source of 3D Print | 1 | 2 | 3 |
| Information about the physical object (metadata) | 1 | 2 | 3 |

Once the data is entered, a spider diagram is generated to reflect the data accuracy, as shown in Figure 9.20. The further away from the centre of the spider diagram, the stronger the data accuracy.




(a) Spider diagram visual tool

(b) Spider diagram example

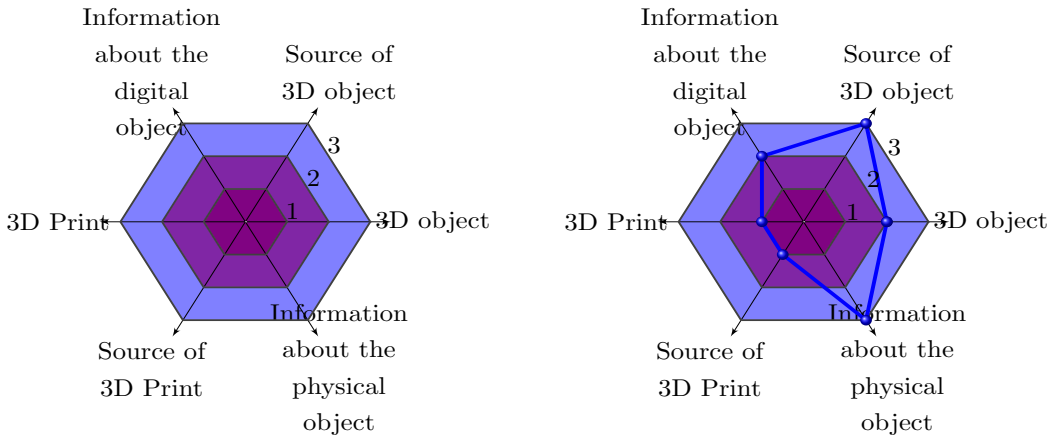
Figure 9.20: Data accuracy spider diagram

**Data consistency** means to maintain the consistency of information when using additive manufacturing. The metric for this component will provide the kind of information used as evidence to prove data consistency, and how accurate the evidence record is. Table 9.19 is the input form to help measure data accuracy.

Table 9.20: Tool for measuring the data consistency

| How accurate is the information for | Weak consistency | Medium consistency | Strong consistency |
|---|---|---|---|
| 3D object (STL file format) | 1 | 2 | 3 |
| Source of 3D object (3D scanned object) | 1 | 2 | 3 |
| Information about the digital object (metadata) | 1 | 2 | 3 |
| 3D Print | 1 | 2 | 3 |
| Source of 3D Print | 1 | 2 | 3 |
| Information about the physical object (metadata) | 1 | 2 | 3 |

Once the data is entered, a spider diagram is generated to reflect the data consistency, as shown in Figure 9.21. The further away from the centre of the spider diagram, the stronger the data consistency.




(a) Spider diagram visual tool

(b) Spider diagram example

Figure 9.21: data consistency spider diagram

The results from the abovementioned components are mapped onto the template in Appendix Figure B.21, which is a graphical presentation of threats and placement of recommendations.

## 9.3 System requirement validation by prototyping

System requirement validation by prototyping is good for validation by software engineers and clients, because it is a more accessible form of requirement specification, as it can visually demonstrate them and also simplifies fault-finding in the requirements. This process can use a paper prototype or a computerised version. The development of the model view controller can be horizontal or vertical, in an evolutionary process or just a throwaway.

It is important have use cases or scenarios to guide the software requirement discovery. The steps for prototype validation are:

- Prototype testers' selection for the prototyping sessions.
- Prototype testing using the scenarios as test cases.
- Prototype documentation as well as faults, bugs or any issues via a problem reporting tool.

This section is based on the work done on a EPSRC-funded grant to build a SECaaS tool for manufacturing in the supply chain, using my framework as the basis for software requirements.

### 9.3.1 Prototype Testers - Stakeholders

The testers were a part of a EPSRC funded grant to the University of Southampton with Dr Richard M Crowder as principal investigator. The grant proposal objective was to build a tool capable of finding faults and vulnerabilities in supply chains that have additive manufacturing as part of production process. Because Dr Crowder is the principal investigator, he will also be the prototype tester. The prototyping was built and implemented by Nawfal Fadhel and Zeyad Aber in several increments, and progress was examined by the principal investigator.

### 9.3.2 Prototype Testing - Test Cases

**Threat Scenarios** Chapter 5 has a comprehensive of set of scenarios used for building the prototype, and cover the selected security properties. The 22 scenarios comprise CVE data (8 cases), Real published cases (5 cases), and hypothetical cases (9 cases). The reasons for selecting these scenarios are:

1. CVE for testing the (CIA) Confidentiality, Integrity, and Availability. CVE are published incidents affecting information security of confidential data such as motorcar designs or Art.
2. Real cases. Testing the (AIN) Authentication, Integrity, and Non-repudiation. Real cases are IP thefts, where the published item is hijacked so these cases do not arise from vulnerabilities in IT systems.
3. Hypothetical cases testing the (AAA) Authentication, Authorisation, and Accounting. Network transmission hacking is not specific to AM (we do not use man in the middle just to attack AM), therefore a scenario where this is possible is more appropriate.

**Use Case Scenarios** The following scenarios illustrate how the framework is used for creating and protecting printable 3D content and is independent of the threat scenarios. 2.3.3 explained that uniqueness can be added to a 3D object either by using the metadata to attach a digital identifier, or by modifying the 3D object surface using steganography.

> Consider the following scenario: As described in the analogy earlier in section **??** Bob is an employee of a military contractor that is getting a design for a new valve that has certain design functions that the valve performs. If the design valve is compromised it could lead to loss in IP, reputation and possible sabotage if not detected.

This research investigates a solution using the provenance framework to protect the provenance of 3D content. This framework can operate hypothetically, even with 3D printed objects using steganographic methods for adding signatures that could be extracted digitally. The new signing methodology could be also employed in the manufacturing sector; a company would be able to sign an object from the inside or outside to establish provenance. The challenge is retaining the signature on the physical object after printing a 3D object. The following sections will define 3D data creation technology, 3D objects, 3D technologies and 3D printing.

**Digital Creation and Signing Scenario** Figure 9.22 represents a provenance scenario to address the concerns of intellectual property holders when publishing 3D digital content, including safe delivery and transferring ownership of the digital content when the object is purchased, and also providing licensed prints if the creator wishes to retain ownership of the intellectual property.

**Step 1** : Digital content creator, whether a designer, engineer, or digitiser, creates the content.

**Step 2** : 3D file is created to a digital file format.

**Step 3** : 3D file is converted to a file format that supports metadata.

**Step 4** : A digital object identifier (3DOI) is generated and added to the metadata.

**Step 5** : The 3D file that contains the (3DOI) is published, where information about the object is catalogued and stored.

**Step 6** : The content provider stores the secured 3D files available for free or purchased download.

**Step 7** : User/Customer Searches for an object that fulfils their requirement.

**Step 8** : User/Customer purchases object, or is given free access, and then downloads it.

**Step 9** : User/Customer 3D prints the object from the 3D file.

**Step 10** : The physical object is created with a physical object identifier on it that is readable using the naked eye, or is hidden steganographically and can only be read with special digital scanning methods.

**Step 11** : The extraction of the 3DOI depends on the method of signing, whether a steganographic method or a visible string of decimal numbers.

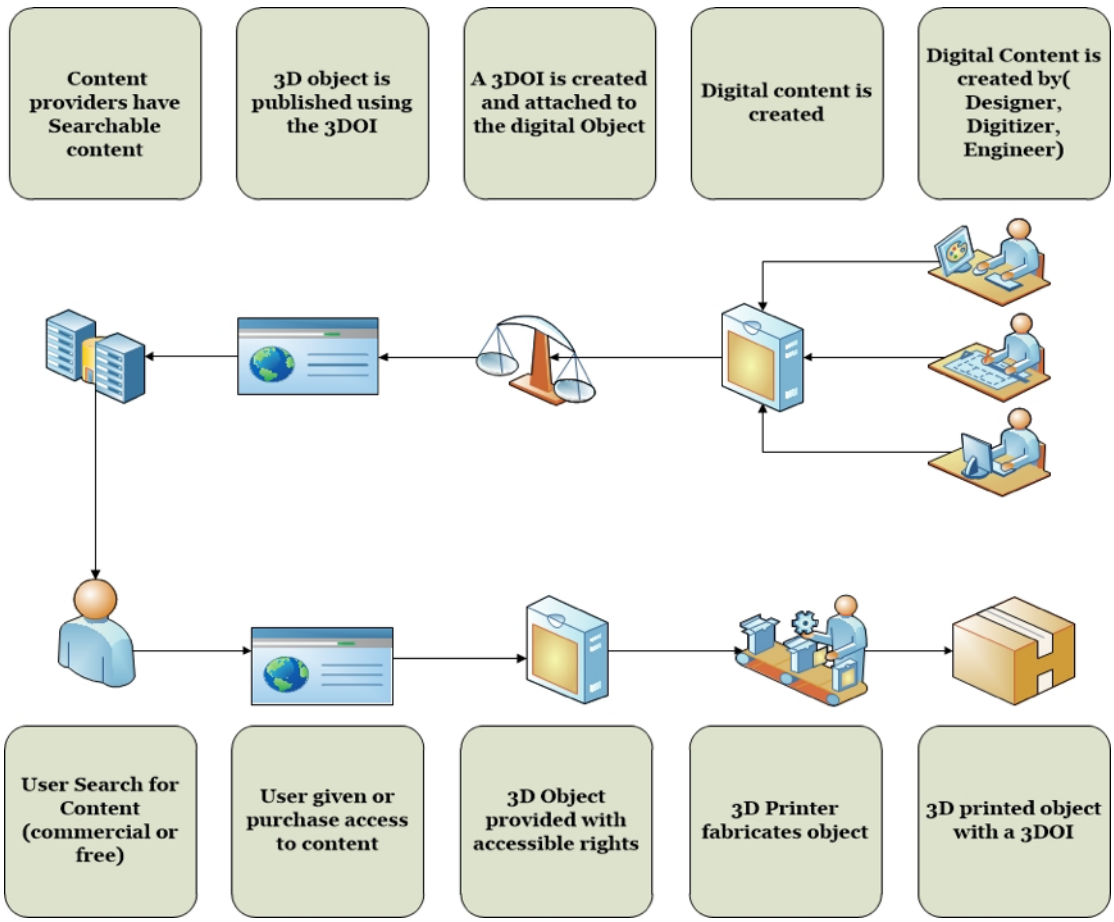



Figure 9.22: User checking 3DOI to provide authenticity of rights owned

**Read and Retrieve Scenario** Figure 9.23 is a scenario-proving claim of ownership or simply investigation of the object's origin, authenticity, and rights, for 3D printed objects. The rights associated with it can be extrapolated from the 3DOI.

**Step 1** : A 3D object is scanned for 3DOI, or read by naked eye if it was printed on the surface of the object.

**Step 2** : The 3DOI is searched for with the content provider to find the object.

**Step 3** : The data regarding access rights and privileges for that unique 3DOI is fetched, and at this step the provenance information is given back to the user.

**Step 4** : The original 3D file information is provided along with the file itself if the user purchased multiple accesses or is the owner of the content.

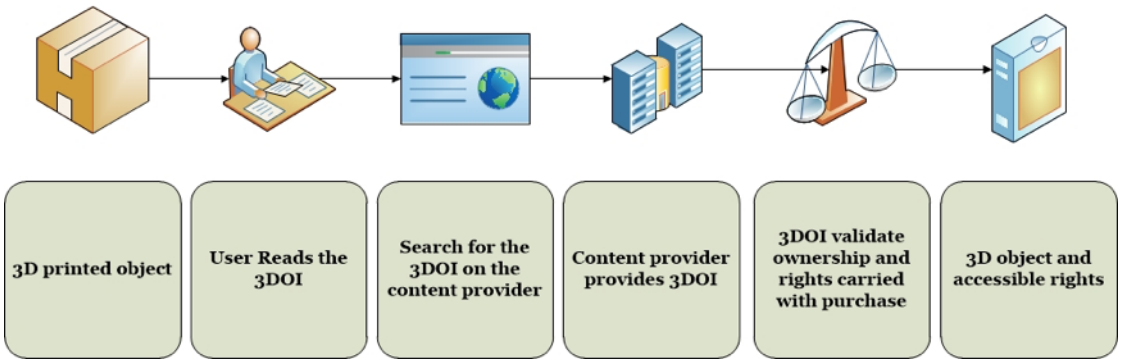



Figure 9.23: Validating a 3D object with an associated 3DOI

Note that, although it is possible to use the 3D object metadata to add security information to provide provenance if AMF or 3MF file formats are used, retaining the provenance information after 3D printing is not possible.

## 9.4 Software Requirement Specification for 3D Prov

With the paper based tool built, testing was carried with the stakeholders and the result of the software requirement is in this section. "3D Prov" a custom tool to measure security compliance within OEM that enables manufacturers to design their own cyber security benchmarks and push the benchmark to the supply chain. This section describes the software requirement specification for 3D Prov that will lead to design and implementation of a cloud-based Security as a Service (SECaaS).

**Purpose** 3D Prov is software that is a cloud-based service, specifically SECaaS. This software is built as a demonstration or proof of concept for research into the maintenance of provenance within the adaptive manufacturing process as well as validating the framework. A basic description of what the tool does is given below.

- Collect and analyse the manufacturing process that involves different suppliers in its supply chain.
- Map relationships between manufacturers and their suppliers, describing stakeholders, process and entities, which are (input/output) for making or delivering a product.
- Identify weaknesses and the vulnerabilities in the supply chain using sets of questions to uncover the current state of security.
- Provide feedback to patch the weak links in the supply chain, in the form of an action list to perform on their business process.

Generally, the continuous use of the software package will permit manufacturers using adaptive manufacturing processes to log all security-related information for all the contracted parties in their supply chain. This is important because it will provide a strong indicator of the state of security.

**Scope** This piece of software is a minimum viable product demonstrator. Therefore, this software requirement document will explore the minimal requirement for a SECaaS to protect manufacturers' handling of their supply chain. The tool can be described as being capable of undertaking the following tasks.

- A data collection tool that is able to collect evidence for government or corporate compliance.
- Analyse the evidence and data collected to map, identify faults and vulnerabilities, to a supply chain.
- Create threat scenarios from the collected data, mapping Stakeholders as agents, processes and entities that describe (input/output).
- Generate reports of the state of compliance using sets of questions based on the security mapping that identified the faults and vulnerabilities.

However, the software developed does not to provide the following features:

- Secure data storage service provider for sensitive security data.
- Is not meant to be liable for any digital privacy act, as this is the responsibility of the user.

The perceived benefit of using 3D Prov SECaaS software will be maintenance of security compliance, increased security assurance to customers, and up-to-date security mitigation policies. Therefore, the objective of building 3D Prov SECaaS software is meant to provide the following value propositions:

- Save time in data collection for security compliance, enabling the user to write compliance reports rapidly.
- Facilitate maintaining security compliance by providing customised feedback that is targeted, based on the manufacturer requirement.

Satisfying the above value propositions should help with

- Organizations building and distributing their own custom security benchmarks.

- Collecting data from the supply chain in a very short time.
- Building reports quickly using the 3D Prov research analysis and evaluation methods.

**Compliance** Government and organisational guidelines used to inform the development of the forms that should be constructed as part of the 3D Prov system include:

- ISO 27001
- Cyber Security Essential Scheme
- EN 9002

**Overview** The software requirement specification is a compilation of customer pains and gains, as well as the required features identified during a 3-month customer discovery programme by Set Squared, led by the University of Southampton. The Software Requirement Specification for 3D Prov describes an early version of a Security as a Service (SECaaS) cloud service that is able to be deployed between one organisation and any number of companies in the supply chain. The service is meant to be used by a security professional to build the initial security benchmark. The benchmark consists of questions and scales that are meant to be presented to the clients as forms. The forms are populated and sent back to the organisation where the cloud service will analyse the data and preform a vulnerability risk assessment.

### 9.4.1 System Design

The system design is based on the paper prototype described in 9.2. The functional and non-functional requirements are described in Appendix D and Appendix E. The database and relationship and system functions are based on these requirements. The full description of the database is in Appendix F

### 9.4.2 Database Design

The database design for 3D Prov is based on the interpretation of the additive manufacturing information model described in Figure 5.2, and the 3D Prov concept prototype in 9.2. Based on the requirements, several iterations of the database were built. Figure 9.24 is the final iteration of the database and has six containers.

**Scenario building** : This container is tasked with building relationship scenarios. The scenario has entities, process and stakeholders.

**Manufacturing management** : This container is responsible for describing the manufacturing process and steps required to manufacture something.

**Security standards** : This container is responsible for a standard that an organisation needs to comply with.

**Certificate management** : This container is responsible for awarding a certificate.

**Knowledge management** : This container holds the assessment data to build questionnaires to assess compliance.

**User management** : This container holds the users, groups and permission tables to support the system.

### 9.4.3 User Interface Design

The user interface mockups are shown in Appendix C, for the stakeholders to decide whether the interpretation of the requirement is correct. There are two modes of operation:

**Admin** The administrator is responsible for choosing the standard that the organisation needs to comply with, and has a dashboard of the compliance score.

**Client** The client is responsible for inputting the information then acting on the feedback.

## 9.5 Summary

In this chapter aimed to validate the framework by using it to build a tool capable of establishing provenance. The research method for validation is software requirement verification by prototyping. This method has three basic requirements: identify the stakeholders, have a list of use cases, and a prototype to show to the stakeholder. The process of validation is by first giving the system architect a paper-based tool to build the system architecture and requirement, and then use it as the basis for discussion with the stakeholder. Then the software-based prototype is shown to the stakeholders to build the requirements. The final tool is delivered to the stakeholder, based on the approved requirements what were built iteratively. In conclusion, the framework was successful in providing the information necessary to build a provenance system that serves the additive manufacturing process.

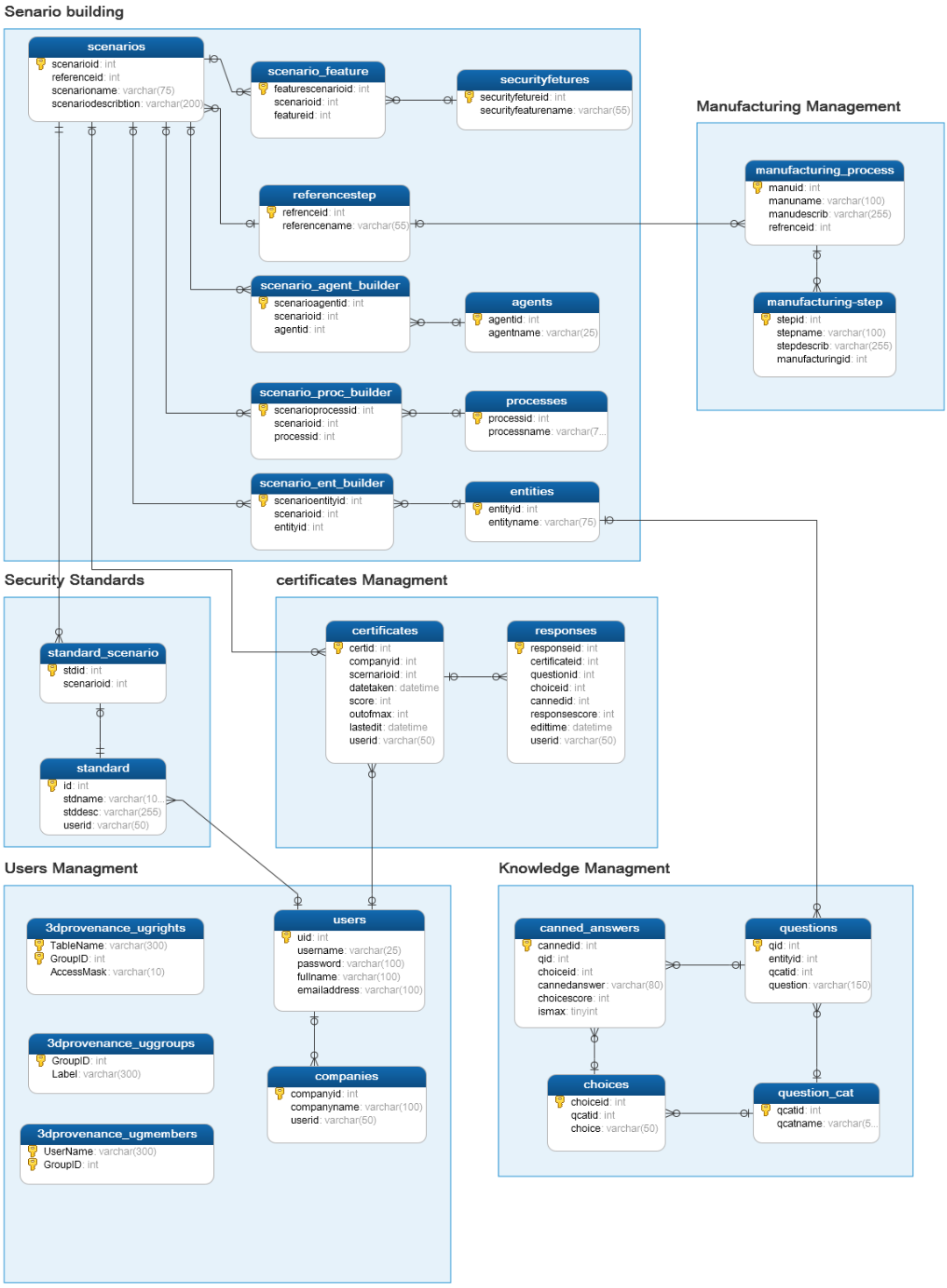



Figure 9.24: Database design based

# Chapter 10

# Conclusion

The literature review showed that 3D printers are available in different sizes, shapes, and additive manufacturing technology, and can vary from 200 to 20000 or more, depending on the type and the quality of the generated object. Some 3D objects can be made into physical objects using 3D printers from a number of materials such as ABS, PLA, ceramics, and metals, depending on the additive manufacturing technology. In 2017, the price dropped to 200 for entry-level 3D printers, and prices are expected to drop further as commercial retailers start to take an interest in this technology.

3D printers use a number of data sources, data creation methods, and data file types, for recording the object, with varied attribute support that may include 3D printing parameters. This research examined 3D digitisation from various data sources, a process with several components. The acquired 3D object has many purposes: educational, entertainment, or just digital preservation. The result of the digitisation process is a 3D object that has geometrical measurements, textured surface, colour, and sometimes material. Additionally, after the 3D object has been recorded and digitised some metadata is needed to describe the object, such as purpose, author, and location.

On the cyber security aspect, the research explored three security principles consisting of a set of properties (Accounting, Authentication, Authorisation, Availability, Confidentiality Integrity, Non-repudiation), and these properties are benchmarks for any security system. Authentication does not itself provide security, but a strong authentication protocol does, and likewise for the rest of the properties. These properties were broken down into components and metrics in later chapters.

The availability of 3D printers to anyone who can afford them introduced a disruptive effect on intellectual property rights, as with the introduction of affordable video cassette recorders (VCR), and when MP3 and E-Books were introduced, but that did not stop the technology being adopted. Because of disruptive effect on intellectual property rights, this could potentially discourage artists and innovators from sharing their intellectual

property, as 3D printed objects currently have no track of provenance and cannot be traced.

3D printers fabricate 3D objects, and illegal possession of unlicensed 3D objects is punishable by law - similar to illegal possession of MP3 and E-Books. But MP3 and the E-books are treated legally as objects rather than file formats, where the law punishes illegal possession of such files. However, when it comes to proving illegal possession of 3D objects, the law for 3D printed objects is loosely defined and hard to achieve. In conclusion, there is no unified 3D object file format nor has legislation caught up with additive manufacturing; moreover, there has been very little research in protecting 3D objects before or after fabrication.

For that reason, a research methodology was built as an important part of the work, and follows good scientific procedure that helps to provide concrete evidence to answer the research questions, which address the successful transferring of security properties from digital to physical objects and *vice versa*.

The security, exchange, and authenticity, of 3D objects and 3D prints is an issue that has been receiving increased attention because of the disruptive effect of additive manufacturing. And additive manufacturing infringements are scarce, while the technology adoption rate is only starting to pick up. The research analysed three types of dataset: documented threats, CVE threats, and hypothetical threat cases. This was done to answer the research question of building a unique threat model for additive manufacturing.

Following publication of the outline framework, the investigation focused on determining the components of the framework, using the goal question metric approach, from which framework version 1.0 was constructed describing the components and their metrics. The framework presented the security properties needed to provide provenance, but did not describe the components nor how to measure them. This led to an expert review that confirmed a refined set of 19 components are the right ones to ensure provenance for 3D printed objects. The expert review used mixed methods by gathering qualitative and qualitative data for the confirmation.

The components were also ranked by importance, to show where the current security trends for 3D objects are headed. This ranking also helps to predict future trends in security procedures protecting 3D content. The ranking showed that the security of transmitted information was the most important aspect of the system, according to the experts, as it showed that sharing 3D objects and 3D prints will be important in the near future. Next came Authenticity of the information, and then general information security.

In summary, at the conclusion of Chapter 7, the second research question had been answered using an expert review: First stage an initial set of components was proposed using GQM as illustrated in Framework version 1.0 in Chapter 6; Second stage refined

the initial components by the using several processes; Third stage conducting the first expert review to confirm the components through interviews and focus groups to gather quantitative and qualitative data.

The initial GQM metrics in Chapter 6 were refined and a task sheet was compiled. The task sheet was made available to the second expert review to rate the metrics and the scales, and the experts questioned on their responses after completing the task sheet. The quantitative findings uncovered some overlooked metrics, and the rest of the metrics refined in a similar way to the first expert review.

The second expert review was longer and more comprehensive, whose main objective was to answer research question three that confirmed and refined the proposed metrics for the components of the framework. The experts' transcribed comments, together with the statistical data, both evaluated the proposed metrics in Chapter 7. This objective of the second expert review was carried out successfully and the result confirmed the metrics were appropriate, sufficient, and complete, to measure the implementation of the components in a system that preserves the provenance of a 3D printed Object as it moves from the digital to the physical world and *vice versa*. Combined with the first expert review, the results completed the triangulation for the research to achieve a confirmed framework.

The objective of research question four was to validate the framework by using it to build a tool capable of establishing provenance. The process is called software validation by prototyping. This method has three basic requirements: identify the stakeholders, produce a list of use cases, and have a prototype to show the stakeholder. The validation started by giving the system architect a paper-based tool to build the system architecture and requirement list, and use it as the basis for discussion with the stakeholder. Then the software-based prototype is shown to the stakeholders to build the requirements. After agreement on the requirements, the final tool is delivered to the stakeholder, built iteratively. The framework was successful in answering research question four by providing the information necessary to build a provenance system that serves the additive manufacturing process.

## 10.1 Contribution

Intelectual property is not defined by the native state that it was founded upon, native state being digital or physical. Intelectual property is a transient property and a reflection of intelligent design. Intelligent assets are created on purpose such as 3D design or by chance, natural formations or bio structures are an example. It is not possible to box the intellectual property without boxing the individual or the phenomena that created it. If we do box them then we will have absolute security over the intelectual property but then it becomes unusable. To use any intellectual property is to disclose it and this

disclosure needs to be regulated. Film, music, art, manufacturing all have regulation or standards to manage accounablity in case of abuse to the intellectual property. However, 3D printing or additive manufacturing is unregulated and it is difficult to because of the nature of the designs/patent being both digital and physical forms.

The contribution to knowledge are in:

**Chapter 5:** Cyber to physical attack reference model that is able to describe vulnerableness and attacks on additive manufacturing.

**Chapter 8:** Provenance framework that is able to provide the tools to save, exchange and sign 3D objects.

**Chapter 9:** Additive manufacturing security analysis tool to find faults and vulnerabilities in organisations that use additive manufacturing part or its process.

## 10.2 Future Work

Provenance is a key aspect of additive manufacturing and no fabrication should be without it, as the intellectual property is of global significance of very high value to the world economy. However, the industrial systems, from big organisations to small enterprises, do not always have the support systems in place to provide provenance. Provenance for additive manufacturing is a collection of evidence to prove where, what, when, who, why, and how, something is fabricated. Unfortunately, not all these pieces of information are recorded.

Therefore, the next step in the research is investigate evidence collection support systems using a concept called Security as a Service (SECaaS), which is a cloud-based technology. The concept is illustrated in the 3D Prov tool that is the output of validation. There are several problem areas that will need further investigation that are summarised below.

- Bridge cyber security language to industrial manufacturing language.
- Build a mathematical model to test for scalability.
- Analyse infringement cases based on threats to quality that a typical attack has cost.
- Measure the effectiveness of the framework against existing cyber security compliances, such as cyber security essentials.
- Investigate the knowledge transfer of the research to apply it in the supply chain environment.

- Build a 3D certification authority for public distribution of global identifiers.
- Build a data mining model from 3D objects, identified by a global identifier.
- Publish analysed infringement cases and 3D objects in Data journals.
- Build a draft standard for IP of 3D objects for oil and gas, in collaboration with Lloyd's Register.

# Appendix A

# Goal Question Metric Approach

The following tables are goal question metric approach analysis, these table is this research initial attempt at creating additive provenance framework. This approached assessed the feasibility of such task.

Table A.1: Goal Question Metric analysis for accounting property

| | | |
|---|---|---|
| Goal | Purpose | Establish |
| | Issue | The Provenance of AM |
| | Object | Auditing 3D objects and 3D prints |
| | View Point | 3D printers users |
| Question (Q1) | How are the 3D printer users identified? | |
| This question inquires about the identity of digital content designer/provider so the action on 3D objects can be identified. This question is important because it will establish if there are any security identification polices in place. | | |
| Metric (M2) | Metric item | Measure |
| | Username & password | Binary |
| | ID cards readers | Binary |
| | Biometrics readers | Binary |
| | Hybrid of the above | Binary |
| | Non of the above | Binary |
| Question (Q2) | What are the attributes required for an audit trail for 3D printer operators? | |
| This question inquires about auditing of 3D printing services. Such as, who printed what and when? Answering this question is important, as it will allow to action association for 3D printing services. Services such as (3D Design tools, 3D printing application and 3D printing hardware). | | |
| Metric (M2) | Metric item | Measure |
| | Identity | User/ Service name |
| | Timestamp | Time |
| | 3D Object Action | Protocol |
| | 3D Print Action | Protocol |
| | Description | Description of the protocol |
| Question (Q3) | How long does it take to identify and report security violations? | |
| This question inquires about violation response time of security polices / Access control. Answering this question will assess response time to violation of security policies and procedures. | | |
| Metric (M3) | Metric item | Measure |
| | Violation instance | Integer |
| | Violation Report | Integer |
| | Rate of security updates | Integer |
| | Violation Response | Integer |

Table A.2: Goal Question Metric analysis for authentication property

| | | | |
|---|---|---|---|
| Goal | Purpose | Establish | |
| | Issue | The Provenance of AM | |
| | Object | Authenticating for 3D objects and 3D prints | |
| | View Point | 3D printers users | |
| Question (Q4) | How is authentication session managed for a 3D print operation? | | |
| "This question inquires about session timing and session time out. Answering this question will enable the measurement of the authentication session" | | | |
| Metric (M4) | Metric item | | Measure |
| | Max. Authentication session | | Time |
| | Time to print | | Time |
| | Timeout duration for inactive session | | Time |
| Question (Q5) | What are the authentication layers per session? | | |
| "This question inquires about authorization levels. Answering this question will indicate available services and their total authentication requests.? | | | |
| Metric (M5) | Metric item | | Measure |
| | Total authentication attempts | | Integer |
| | Authenticated application | | Boolean |
| | Authenticated service | | Boolean |
| | Authenticated 3D printing hardware | | Boolean |
| Question (Q6) | How are the 3D printer operators and 3D designers are authenticated? | | |
| "This question inquires about the authenticity of digital content designer/provider. Answering this question with provide bases for forming physical identity of 3D printed object using inherited digital attribute" | | | |
| Metric (M6) | Metric item | Scale | Measure |
| | Total authentication | Non | Integer |
| | Failed authentication | Non | Integer |
| | Authentication methods | Username & password | Binary |
| | | ID cards readers | Binary |
| | | Biometrics readers | Binary |
| | | Hybrid of the above | Binary |
| | | Non of the above | Binary |

Table A.3: Goal Question Metric analysis for authorisation property

| | | |
|---|---|---|
| Goal | Purpose | Establish |
| | Issue | The Provenance of AM |
| | Object | Authorization for 3D objects and 3D prints |
| | View Point | 3D printers users |
| Question (Q7) | What are the authorization layers per session? ”No of authorization layers per session (Application layer, Service layer, Hardware layer). Answering this question will enabling tailoring security policies according to system size/ scale? | |
| Metric (M7) | Metric item | Measure |
| | No. Of Authorized application | Integer |
| | No. Of Authorized service | Integer |
| | No. Of Authorized 3D printing hardware | Integer |
| | Total authorization attempts | Integer |
| Question (Q8) | How many resources are available for a single user on 3D printer in terms of time and material? ”This question examines the resources required for authorized personal/ services. Answering this question will gage the resources allocation for users with respect to size/ scale that was determined in the previous question.” | |
| Metric (M8) | Metric item | Measure |
| | Printing Time | Time |
| | Printing Material | Pounds |
| | Printing Cost | Sterling pounds |
| Question (Q9) | What are the authorization classes for access to 3D printers? ?This question inquires about the authorization type in the organization. Answering this question will provide organization policy needs according to authorization type.? | |
| Metric (M9) | Measure | Variable/Units |
| | Authorization type | Personal authorization/ Binary |
| | | Role based authorization/ Binary |
| | | Group based authorization/ Binary |
| | | Other type of authorization/ Binary |
| Question (Q10) | What is the number of failed / successful authorization attempts to use a 3D printer? ”This question examines allocation of resources to authenticated users. Answering this question will provide a real acceptance/ rejection ratio.” | |
| Metric (M10) | Metric item | Measure |
| | Total No. Of successful attempts | Integer |
| | Total No. Of failed attempts | Integer |

Table A.4: Goal Question Metric analysis for availabilty property

| | | |
|---|---|---|
| Goal | Purpose | Establish |
| | Issue | The Provenance of AM Availability for |
| | Object | 3D objects and 3D prints |
| | View Point | 3D printers users |
| Question (Q11) | How much time a 3D printer is available for normal operation? | |
| "This question investigates the efficiency of time using 3D printers. Answering this question will reflect availability of services by utilization of 3D printer time" | | |
| Metric (M11) | Metric item | Measure |
| | Total working hours | Time |
| | Total of 3D printing time | Time |
| Question (Q12) | How fast can a 3D printer recover? | |
| "This question investigates failure recovery time. Answering this question will reflect resilience of the system to recover from failures." | | |
| Metric (M12) | Metric item | Measure |
| | Fail time | Time |
| | Recovery time | Time |
| Question (Q13) | What are the possible failure points in a 3D printing process? | |
| "This question where the fail of availability of information occurs. Is failure in the transmission of information? Is the failure in the in software or the hardware?" | | |
| Metric (M13) | Metric item | Measure |
| | Rate of software failure | Integer |
| | Rate of hardware failure | Integer |
| | Rate of network failure. | Integer |
| Question (Q14) | How do you trust the acquired 3D objects? | |
| "This question reflect on the availability of information (in this case the information is a 3D printed object)" | | |
| Metric (M14) | Metric item | Measure |
| | Identity | User/ Service name |
| | 3D Design tools | Service name |
| | No. Of successful 3D prints | Integer |

Table A.5: Goal Question Metric analysis for confidentiality property

| | | | |
|---|---|---|---|
| Goal | Purpose | Establish | |
| | Issue | The Provenance of AM | |
| | Object | Confidentiality for 3D objects and 3D prints | |
| | View Point | 3D printers users | |
| Question (Q15) | How strong is the data transmission security for transmitting and sharing 3D objects? | | |
| "This question examines network securityprocedures that used to carry 3D content" | | | |
| Metric (M15) | Metric item | Measure | |
| | Cryptographic algorithm | Method | |
| | Algorithm to generate key | Method | |
| | Key length | Integer | |
| | Network security protocols | Protocol | |
| Question (Q16) | What are the method used generate random or unique identification No.? | | |
| "This question examines the number generation of 3D object identifier (3DOI) to be associated with 3D objects" | | | |
| Metric (M16) | Metric item | Measure | |
| | 3DOI no. generator | Protocol | |
| | Size of the 3DOI | Integer | |
| Question (Q17) | How is 3D data is stored? | | |
| "This question inquires about the quality of storage to maintain information integrity during the 3D object life cycle." | | | |
| Metric (M17) | Metric item | Measure | |
| | Storage Size | Integer | |
| | Encryption protocol | Protocol | |
| Question (Q18) | How are 3D printed objects are identified? | | |
| "This question inquires about the inspection of 3Dprinted objects to associate/ identify them." | | | |
| Metric (M18) | Metric item | Scale | Measure |
| | Physical object identification | Visual identification | Protocol |
| | | Tagged identification | Protocol |
| | | Serial number identification | Protocol |
| Question (Q19) | What is the classification/ Clearance levels for 3D object and 3D prints | | |
| "This question inquires about classification/ clearancelevels for personal, enterprise, legal or governmental to access 3D objects and 3D prints." | | | |
| Metric (M19) | Metric item | Scale | Measure |
| | Classification/ Clearance levels | Unclassified | Protocol |
| | | Confidential | Protocol |
| | | Secret | Protocol |
| | | Top Secret | Protocol |
| Question (Q20) | How are confidential 3D printed objects are protected in work place? | | |
| "This question inquires the protectionof 3D printed object in the workplace" | | | |
| Metric (M20) | Metric item | Scale | Measure |
| | Physical security for 3D objects | Unprotected | Protocol |
| | | Storage Cabinets | Protocol |
| | | Safe | Protocol |
| | | Safe and Guards | Protocol |

Table A.6: Goal Question Metric analysis for integrity property

| | | | |
|---|---|---|---|
| Goal | Purpose | Establish | |
| | Issue | The Provenance of AM | |
| | Object | Integrity for 3D objects and 3D prints | |
| | View Point | 3D printers users | |
| Question (Q21) | How many validation checks for a single 3D object? | | |
| "This question examines the validity of the 3D object before printing. User validation refers to validation by the user that the object integrity is complete and there are no (gaps/ breaks / holes) in the model and software validation refers to the 3D printing software using 3D objects." | | | |
| Metric (M21) | Metric item | Measure | |
| | Total Number of Validation checks | Integer | |
| | User validation | Integer | |
| | Software validation | Integer | |
| Question (Q22) | How many validation checks for a single 3D Print? | | |
| "This question examines the validity of the 3D object before printing. User validation refers to validation by the user that the object integrity will hold during the printing and software validation refers to the object requirement in terms of material, type of printer and type of object." | | | |
| Metric (M22) | Metric item | Measure | |
| | Number of Validation checks | Integer | |
| | User validation | Integer | |
| | Software validation | Integer | |
| Question (Q23) | How 3D prints are prioritized for 3D printer Queue? | | |
| "This question investigates the efficacy of printing queues to present a clearer prospective of 3D printing availability" | | | |
| Metric (M23) | Metric item | Measure | |
| | Time to print | Date | |
| | No. Of 3D Object in Queue | Integer | |
| Question (Q24) | How are 3D objects are backed up under legal requirements to compliance? | | |
| "This question inquires about the backup process to present a clearer prospective of 3D printing availability" | | | |
| Metric (M24) | Metric item | Measure | |
| | Backup Time | Date | |
| | Frequency of backup | Integer | |
| | Restoration Time | Date | |
| Question (Q25) | How application program ensure integrity? | | |
| "This question address the integrity of printable 3D objects as some objects require special conditions, which if met could result of higher availability of 3D prints." | | | |
| Metric (M25) | Metric item | Measure | |
| | Size of 3D print | Cubic CM | |
| | Type of print 3D | Type | |
| | Type of 3D printer | Type | |
| Question (Q26) | How are protected 3D printed objects are disposed of? | | |
| "This question inquires about the secure disposal of potentially confidential info." | | | |
| Metric (M26) | Metric item | Scale | Measure |
| | Recycling methods | Shredders | Protocol |
| | | Disposal company | Protocol |
| | | Recycling company | Protocol |

Table A.7: Goal Question Metric analysis for non-repudiation property

| | | | |
|---|---|---|---|
| Goal | Purpose | Establish | |
| | Issue | The Provenance of AM | |
| | Object | Non-Repudiation 3D objects and 3D prints | |
| | View Point | 3D printers users | |
| Question (Q27) | What attributes are considered as proof of digital / Physical transaction on 3D objects? | | |
| "This question examines the attributes used to prove fraudulent attempts on 3D objects/3D beyond reasonable doubt." | | | |
| Metric (M27) | Metric item | Measure | |
| | Entry number | Integer unit | |
| | Timestamp | Date | |
| | Identity | User/ Service name | |
| | Action | Protocol | |
| | Description | Description of the protocol | |
| Question (Q28) | How are the interactions checked in the entry log for 3D objects? | | |
| "This question inquires about how information is retrieved from the logs about the 3D objects/3D prints" | | | |
| Metric (M28) | Metric item | Measure | |
| | No. Of entries | Integer | |
| | No. Of interactions | Integer | |
| Question (Q29) | How are the log files accessed? | | |
| "This question examines the access control procedures for log files" | | | |
| Metric (M29) | Metric item | Scale of Access control | Measure |
| | Access control type | Mandatory | Protocol |
| | | Discretionary | Protocol |
| | | Role-Based | Protocol |
| | | Rule-Based | Protocol |
| | | Lattice-based | Protocol |
| | | List | Protocol |

# Appendix B

# Framework Template - Modelling and Function

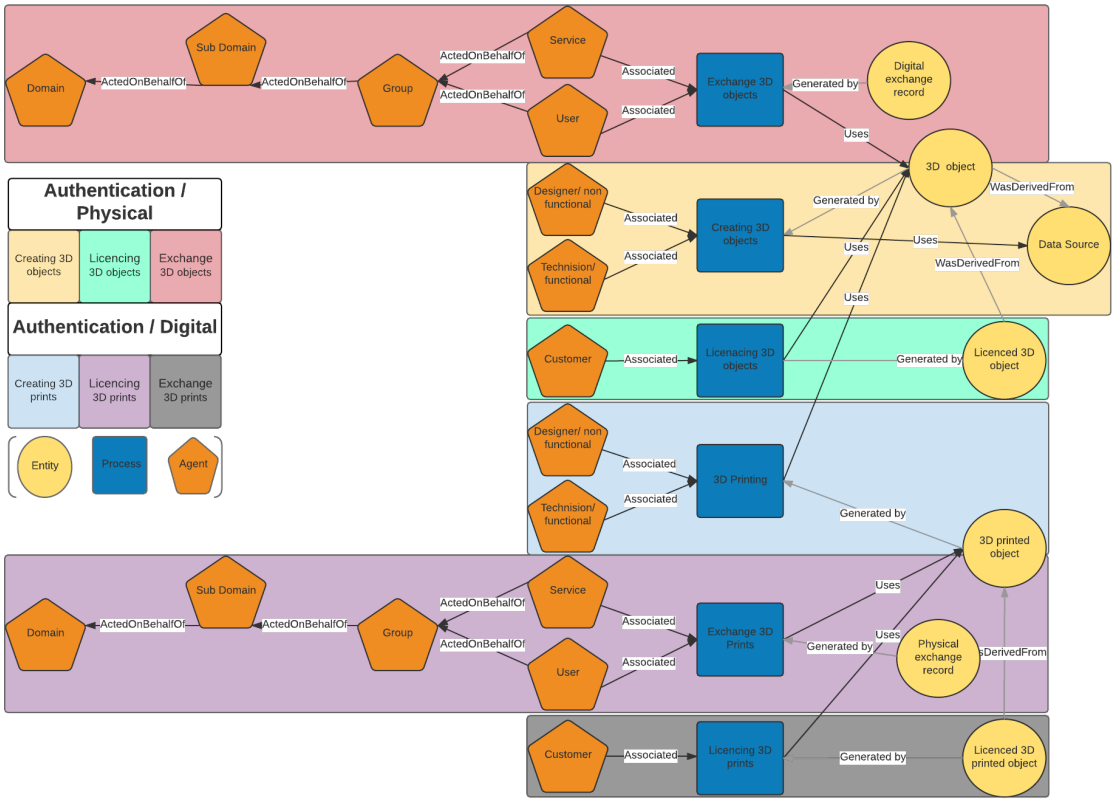



Figure B.1: What to authenticate in the additive manufacturing process

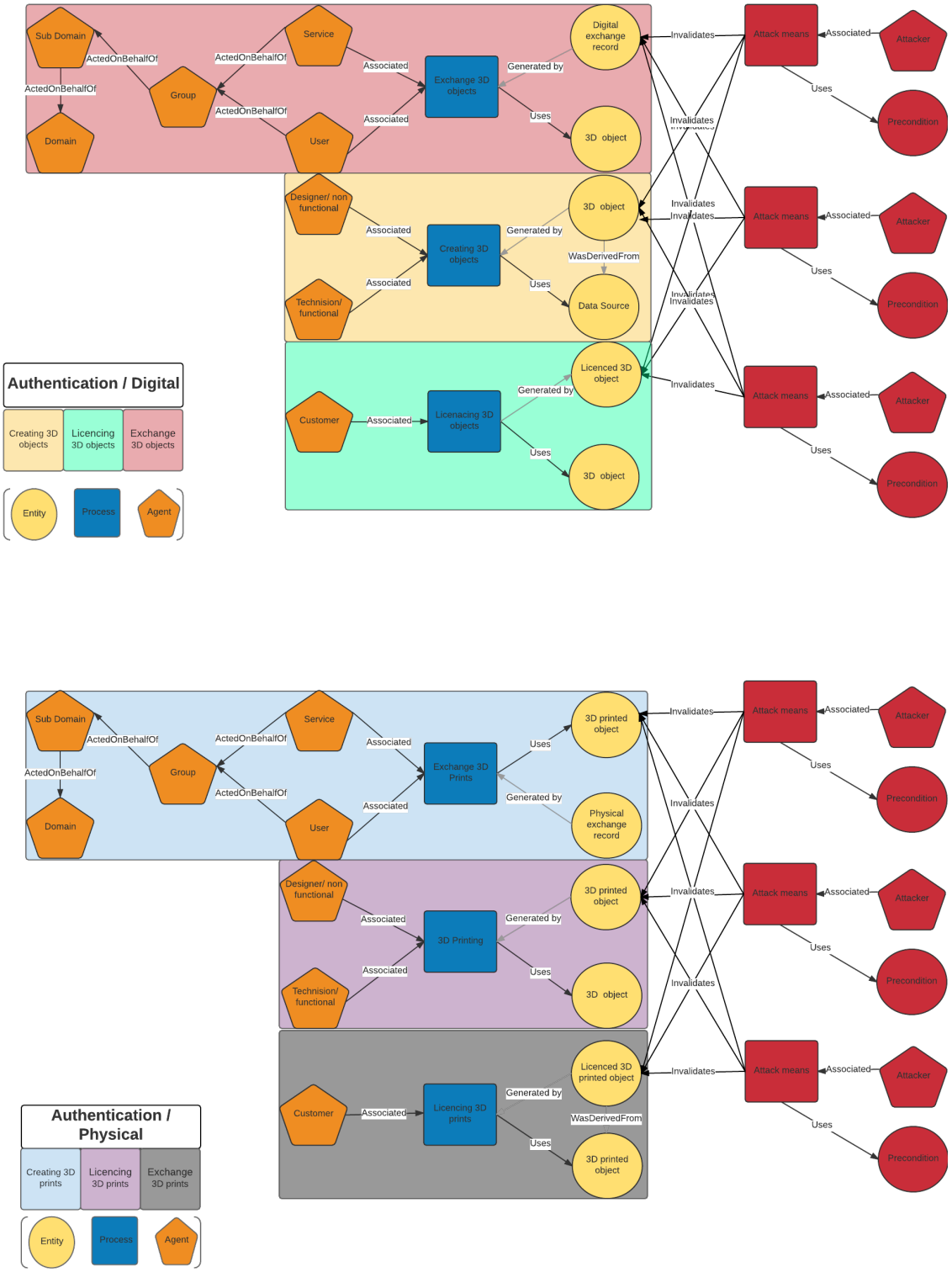



Figure B.2: Attack targets in the additive manufacturing process that will be exploited via authentication weakness

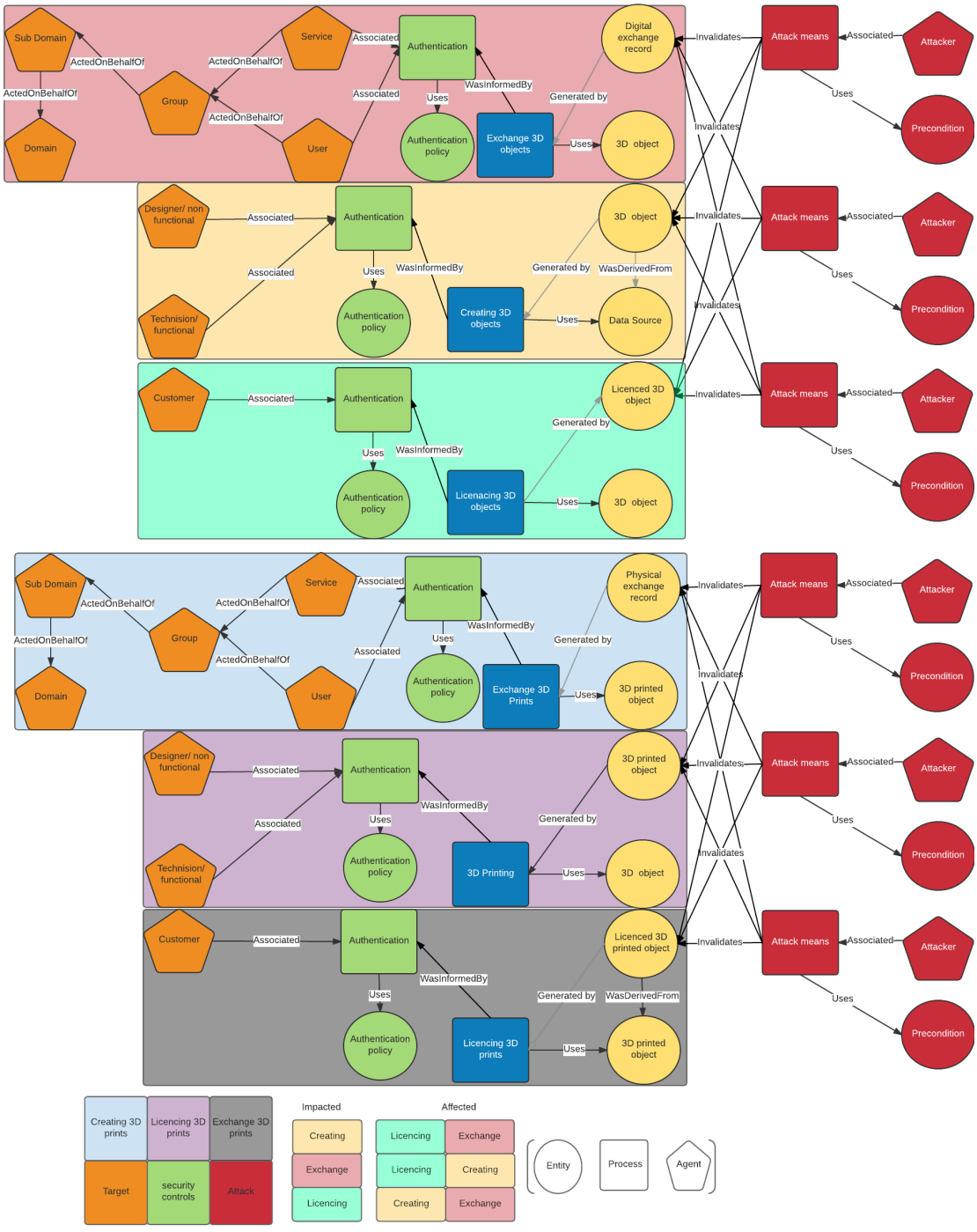



Figure B.3: Authentication hardening recommendations to patch threats to the additive manufacturing process

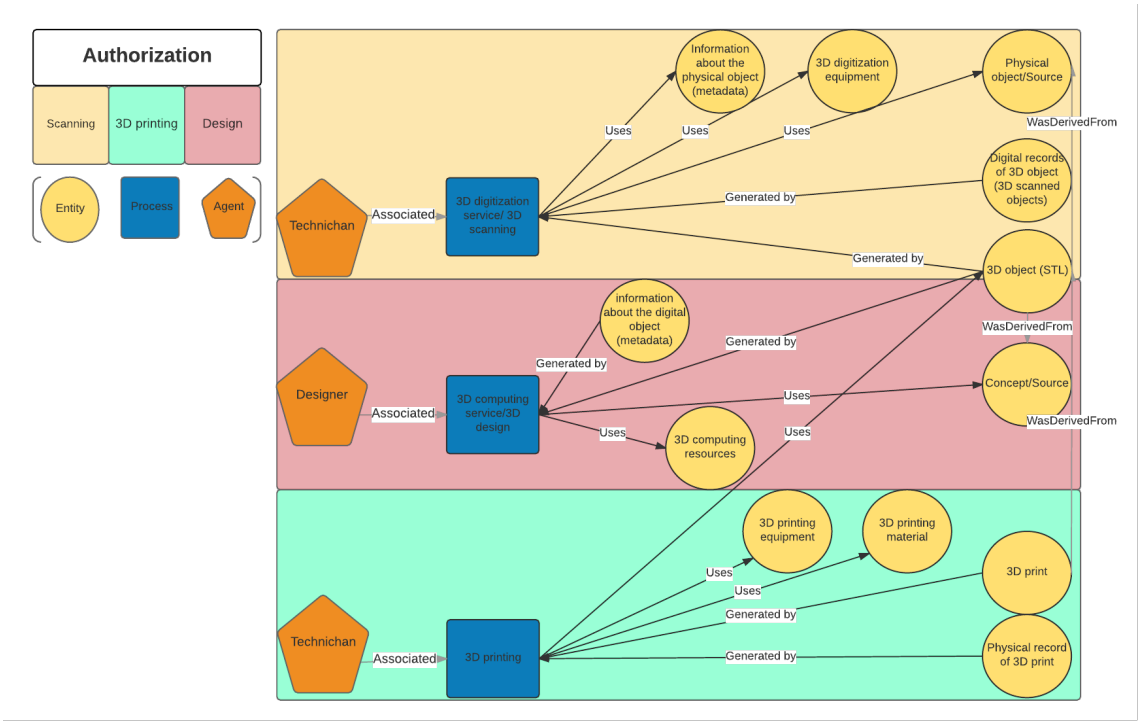



Figure B.4: What to authorize in the additive manufacturing process

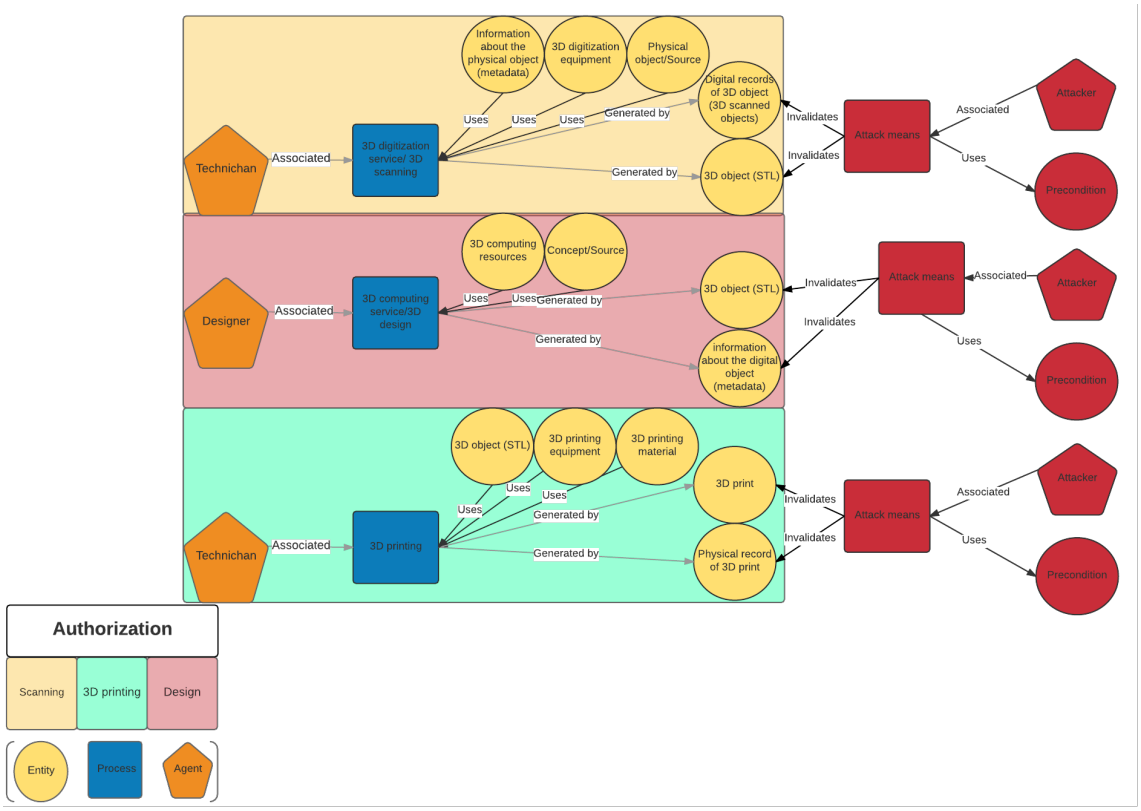



Figure B.5: Attack targets in the additive manufacturing process that will be exploited via authorization weakness

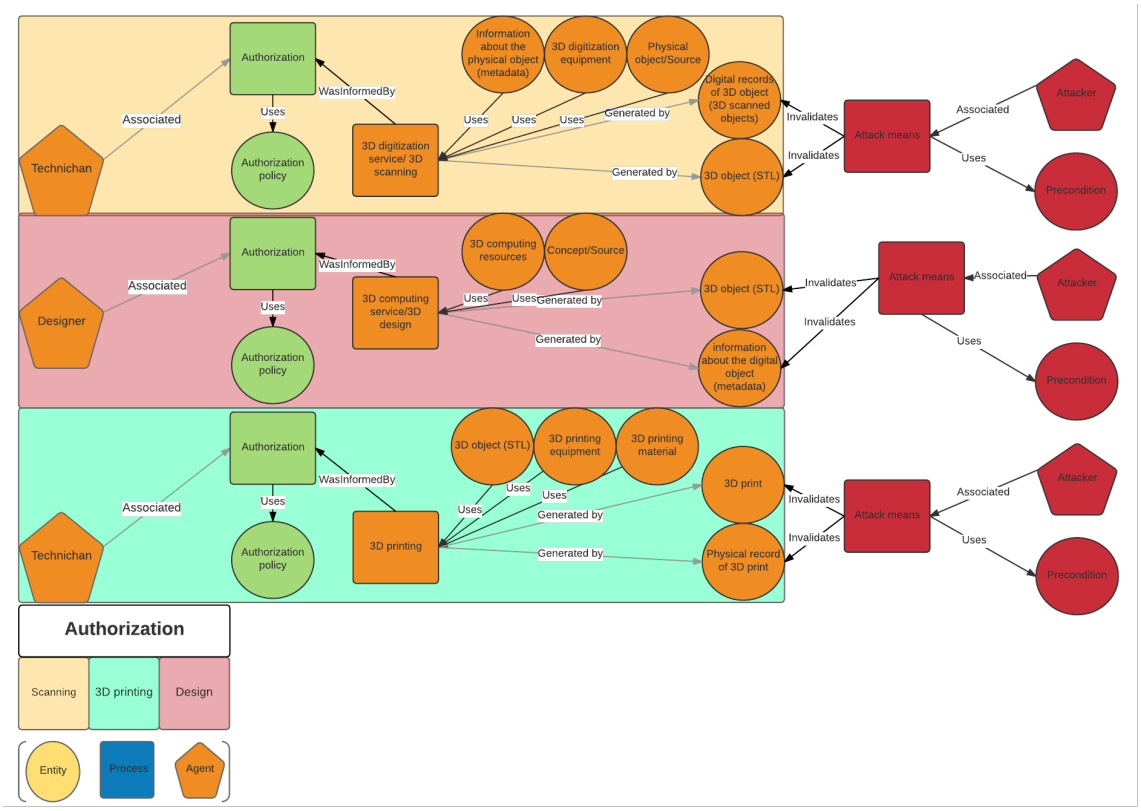



Figure B.6: Authorization hardening recommendations to patch threats to the additive manufacturing process

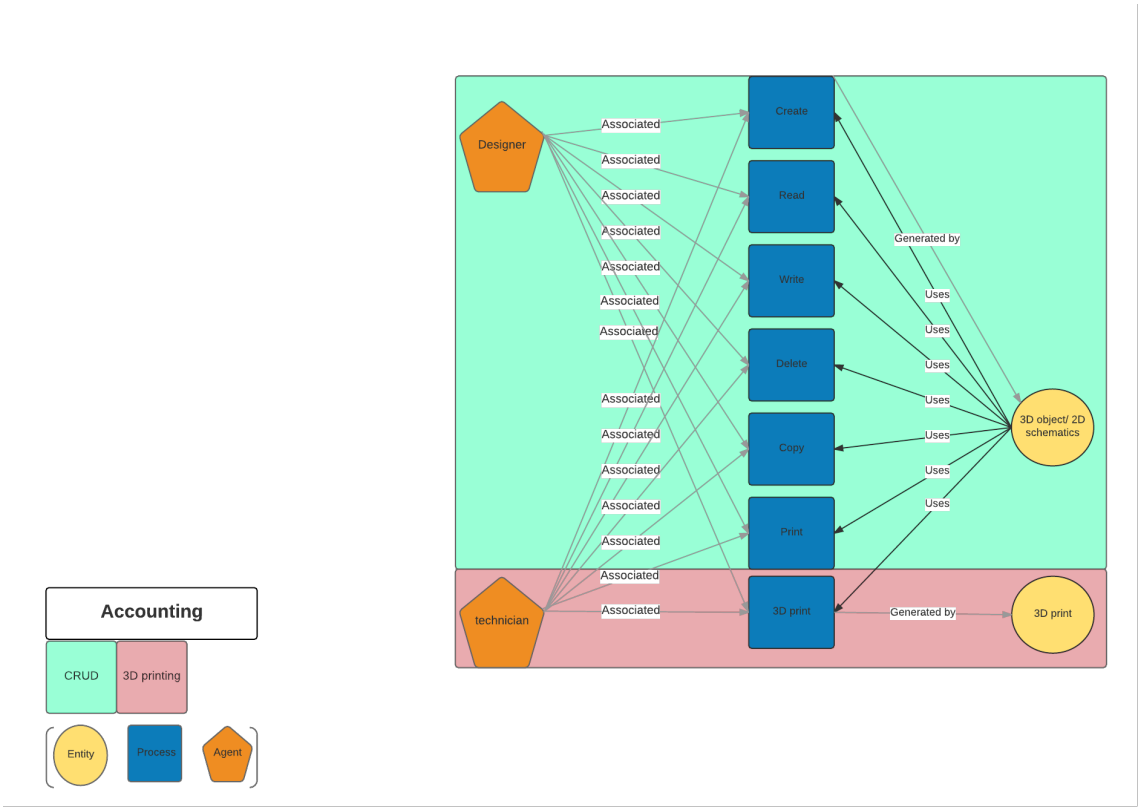



Figure B.7: What to account for in the additive manufacturing process

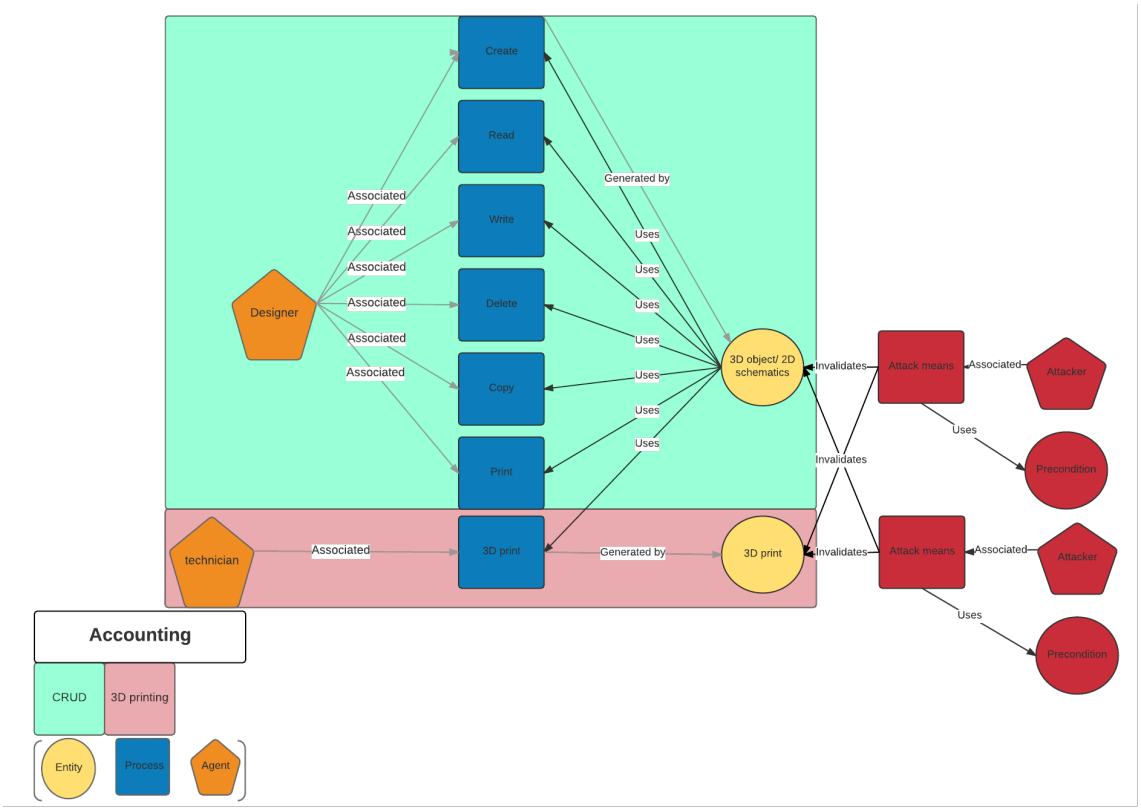



Figure B.8: Attack targets in the additive manufacturing process that will be exploited via accounting weakness

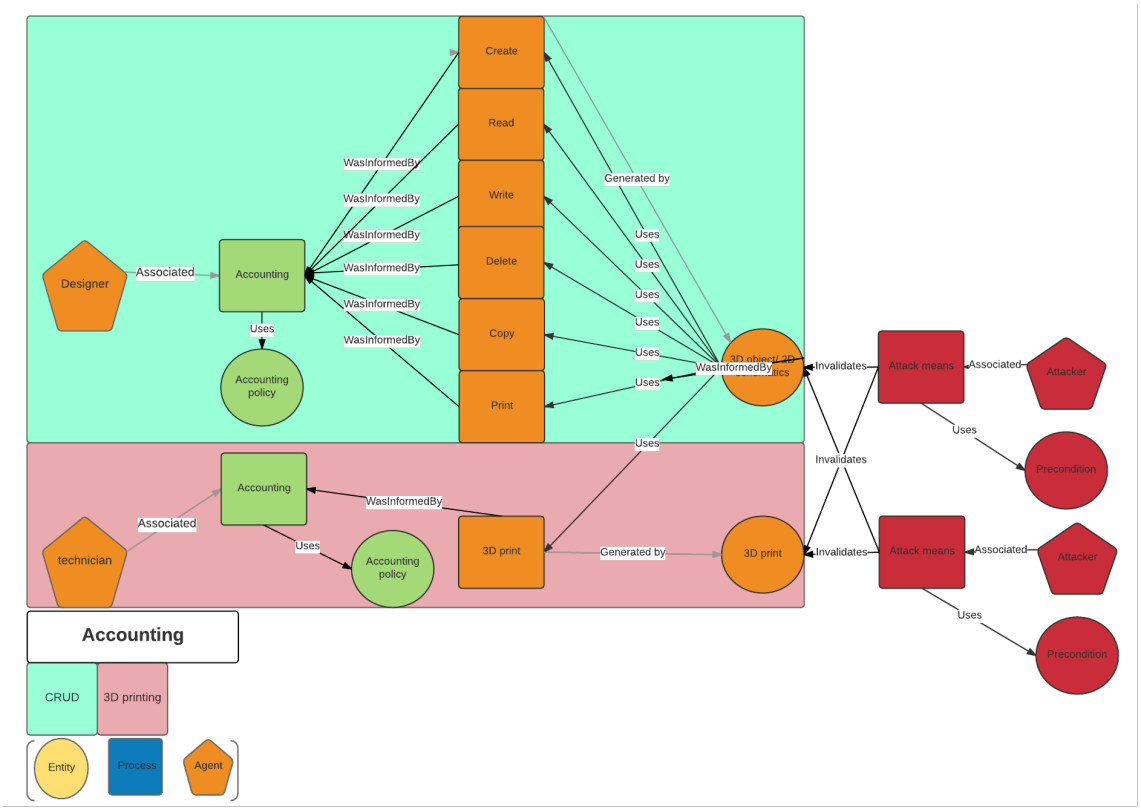



Figure B.9: Accounting hardening recommendations to patch threats to the additive manufacturing process

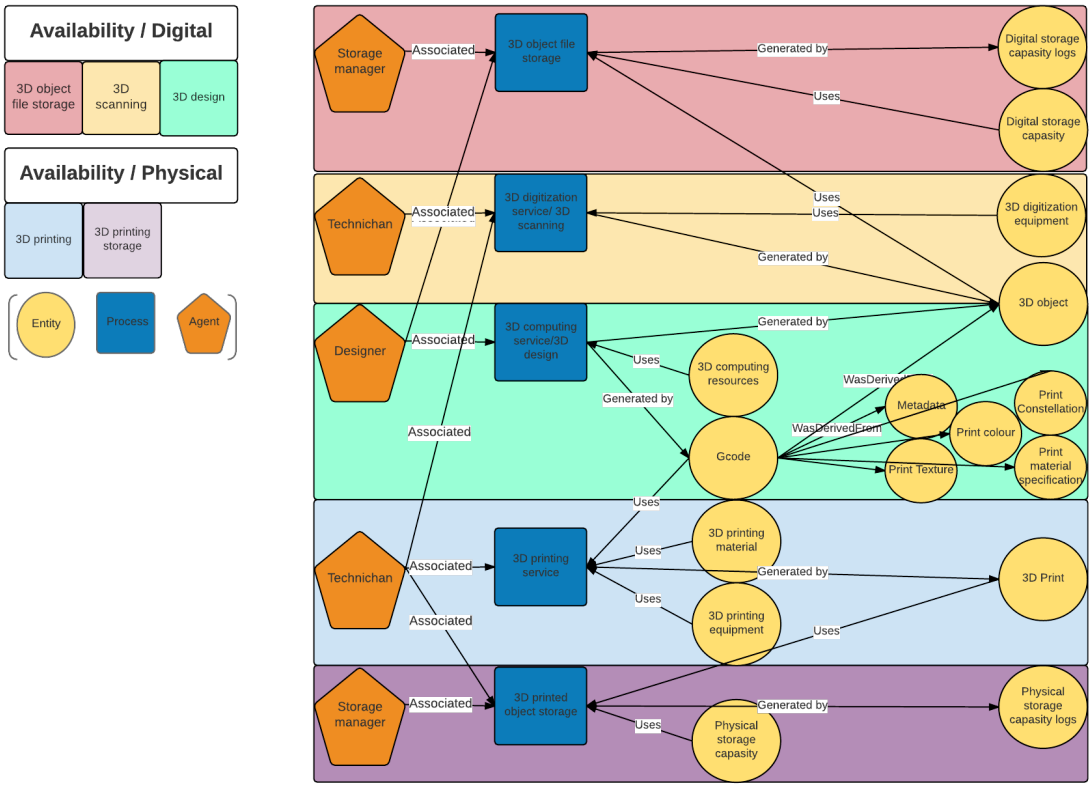



Figure B.10: What to make sure it's highly available in the additive manufacturing process

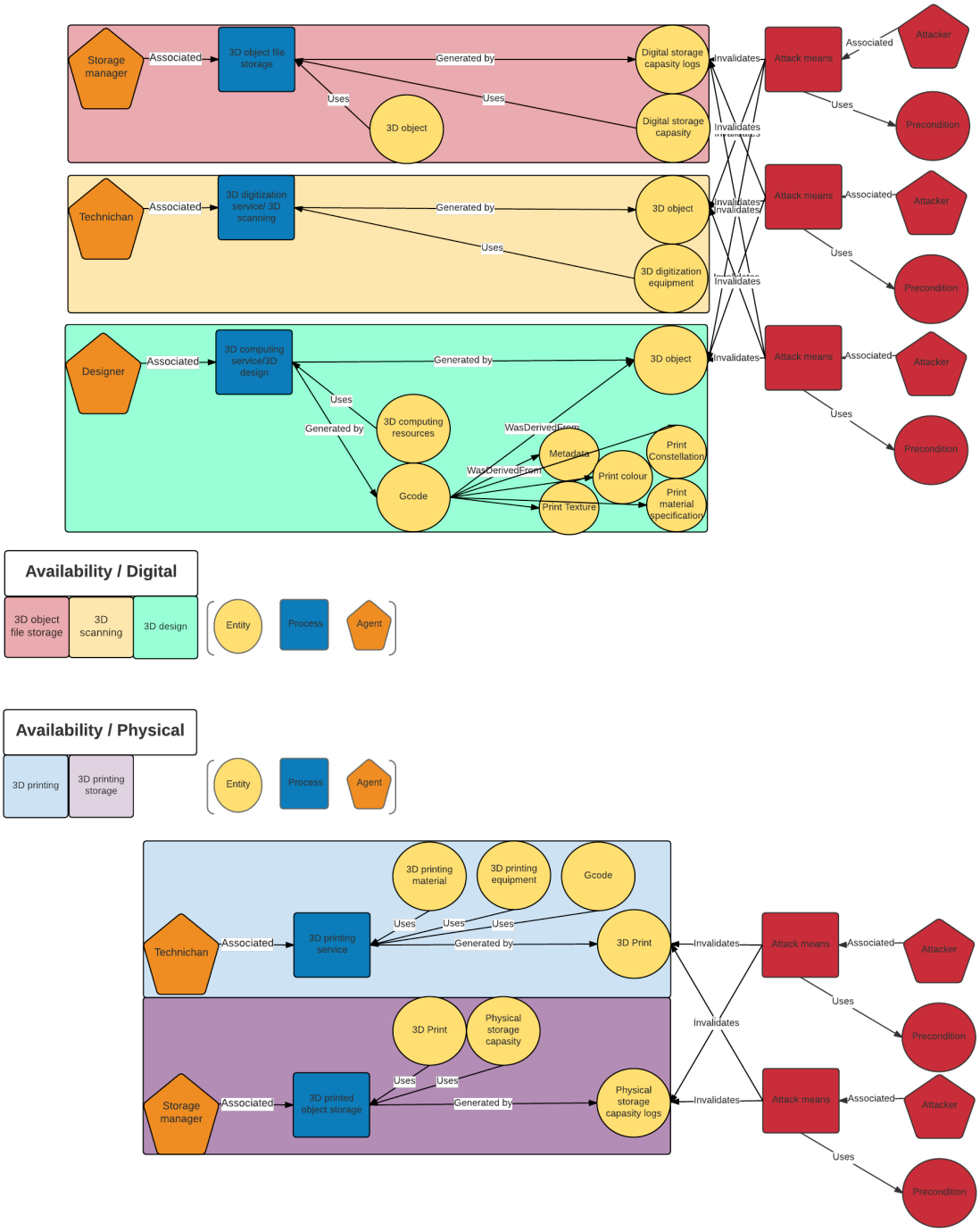



Figure B.11: Attack targets in the additive manufacturing process that will be exploited via an availability weakness

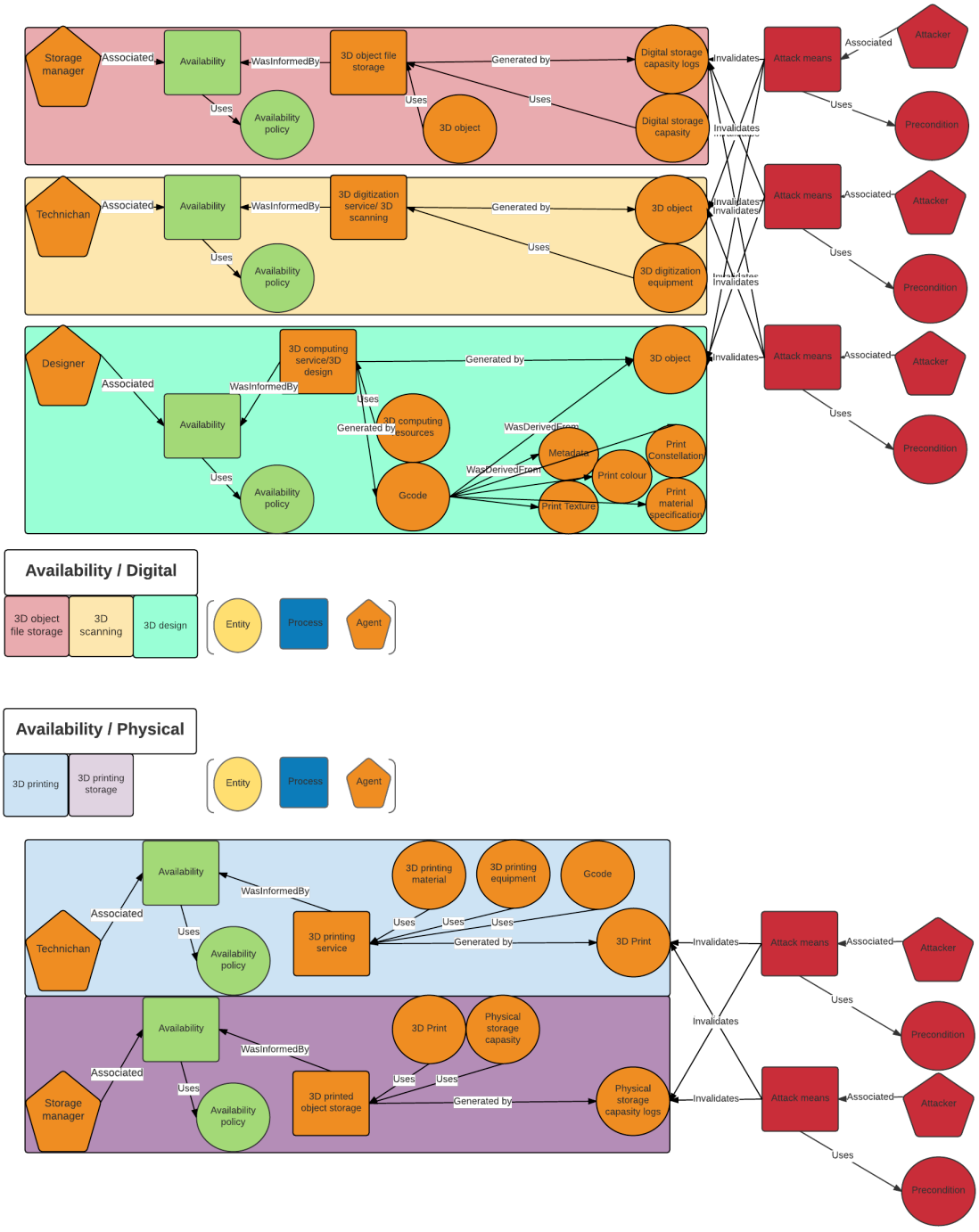



Figure B.12: Availability hardening recommendations to patch threats to the additive manufacturing process

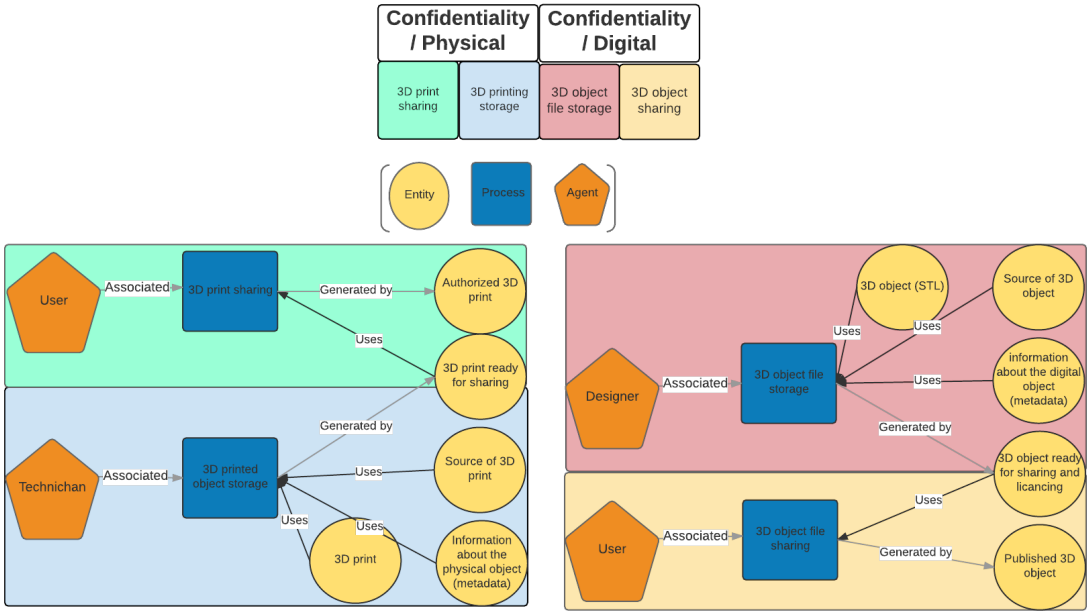



Figure B.13: What to make sure remains confidential in the additive manufacturing process

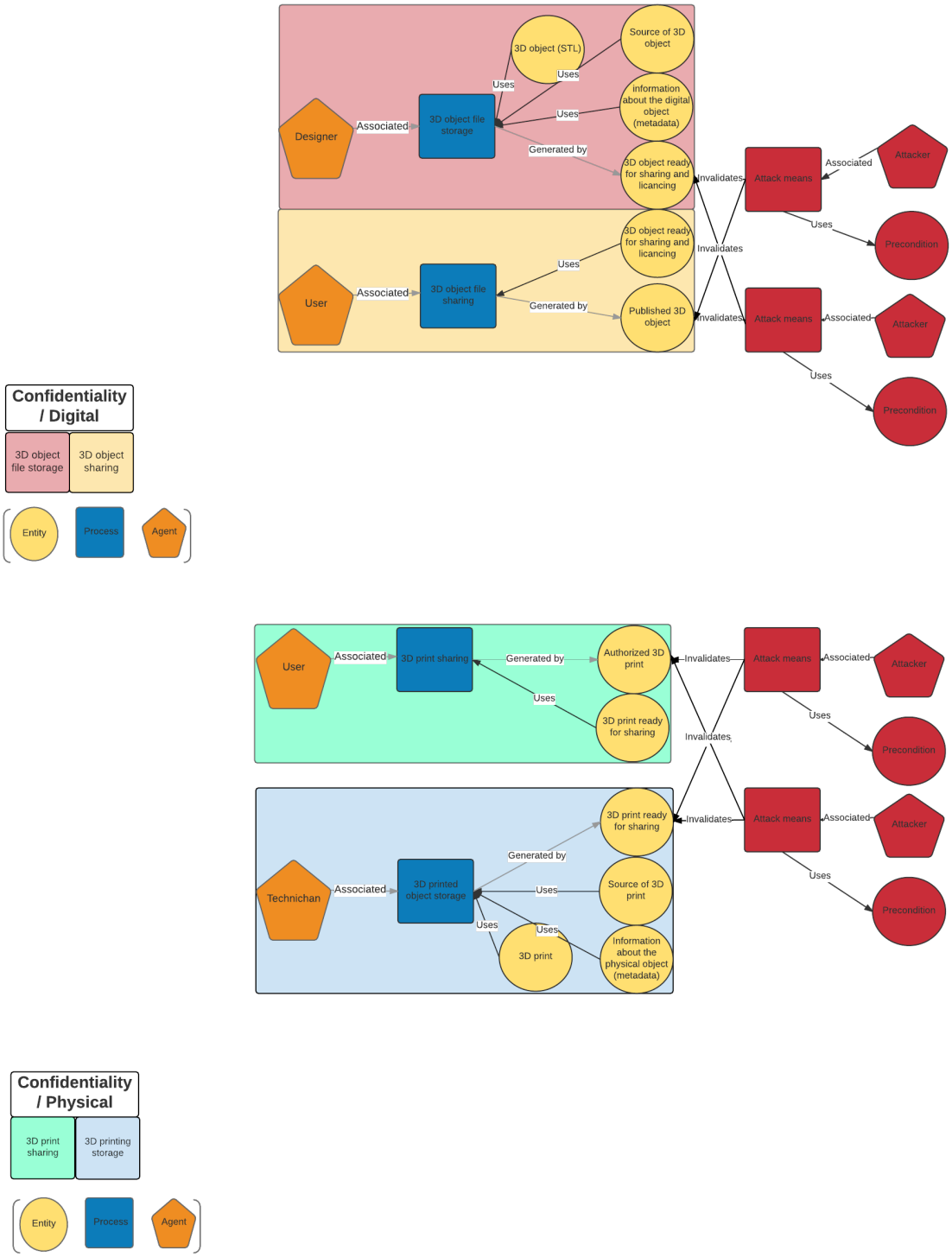



Figure B.14: Attack targets in the additive manufacturing process that will be exploited via confidentiality weakness

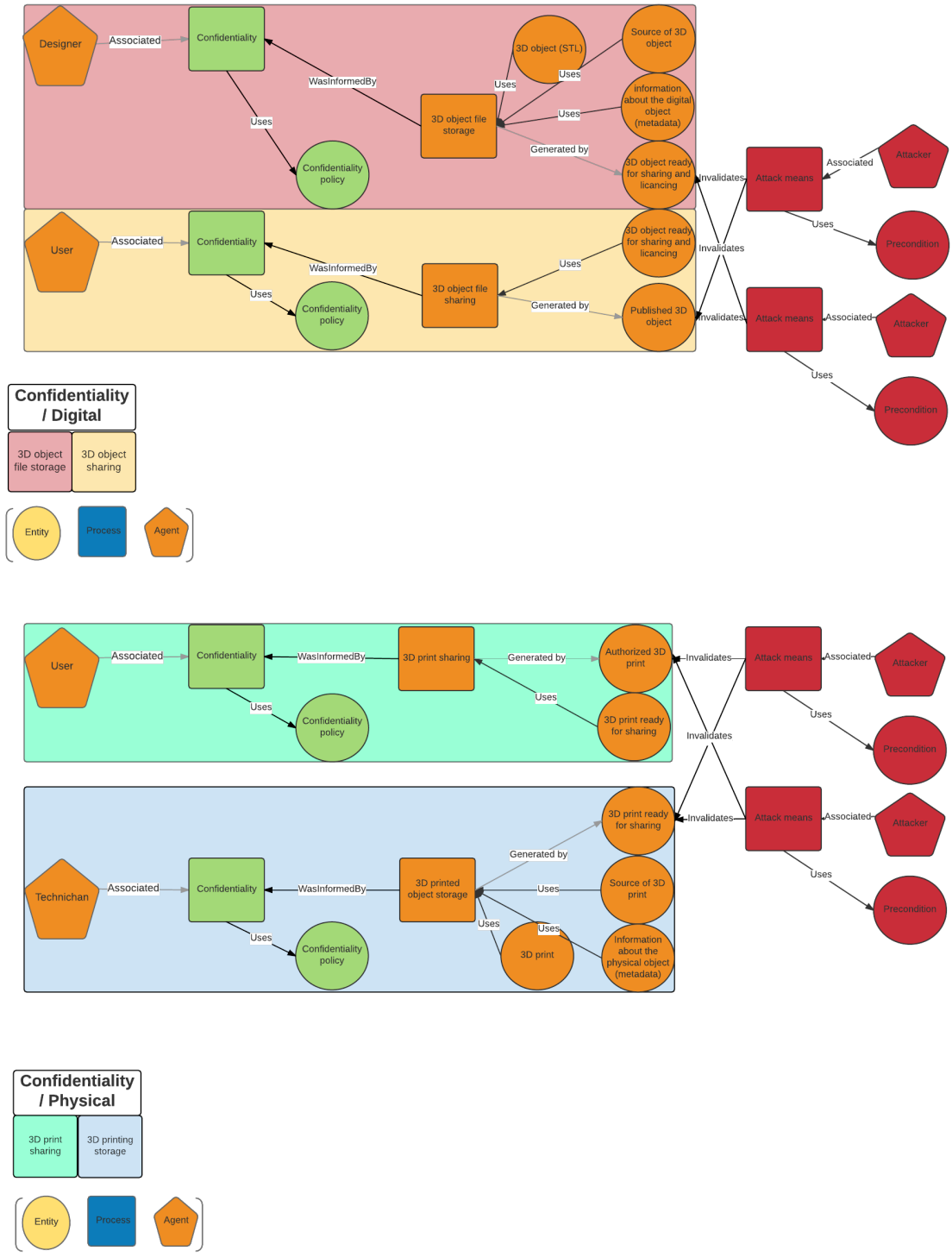



Figure B.15: Confidentiality hardening recommendations to patch threats to the additive manufacturing process

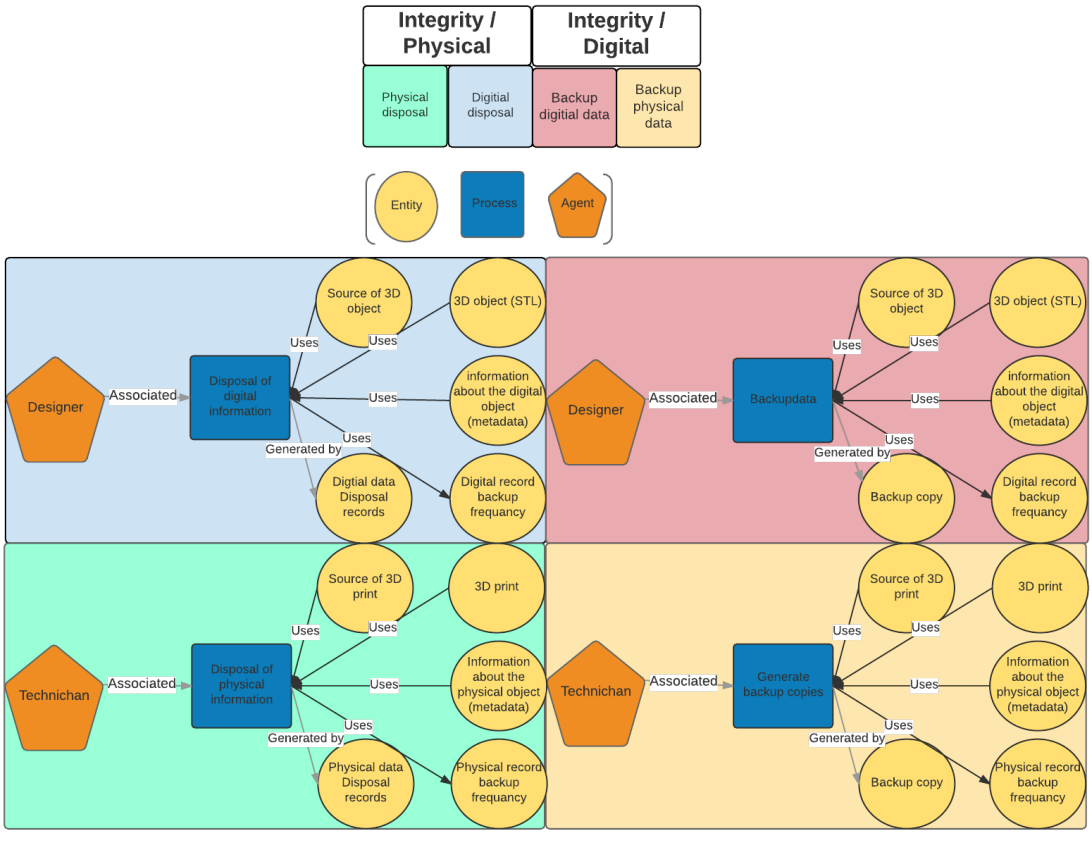



Figure B.16: What to make sure it holds integrity in the additive manufacturing process

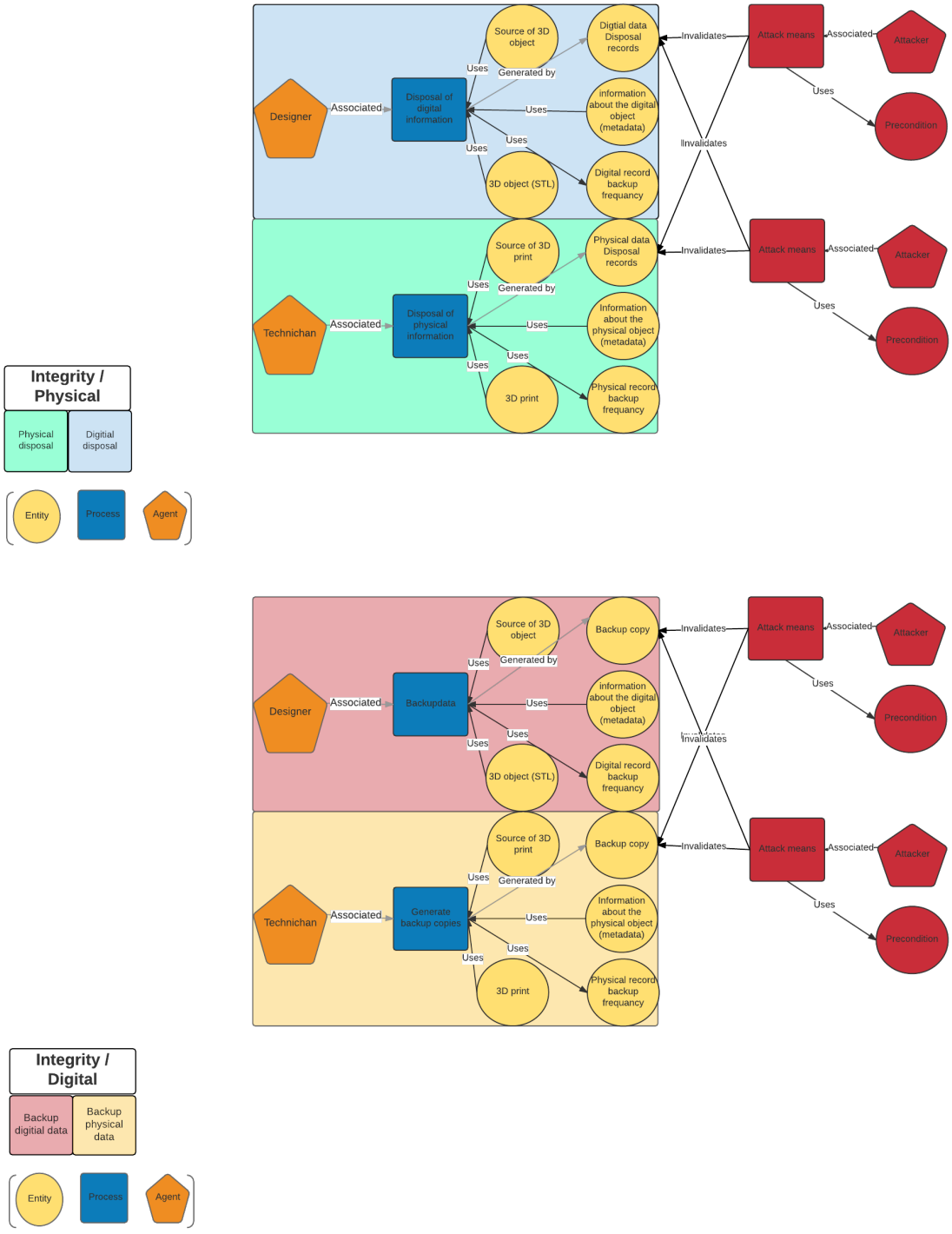



Figure B.17: Attack targets in the additive manufacturing process that will be exploited via an integrity weakness

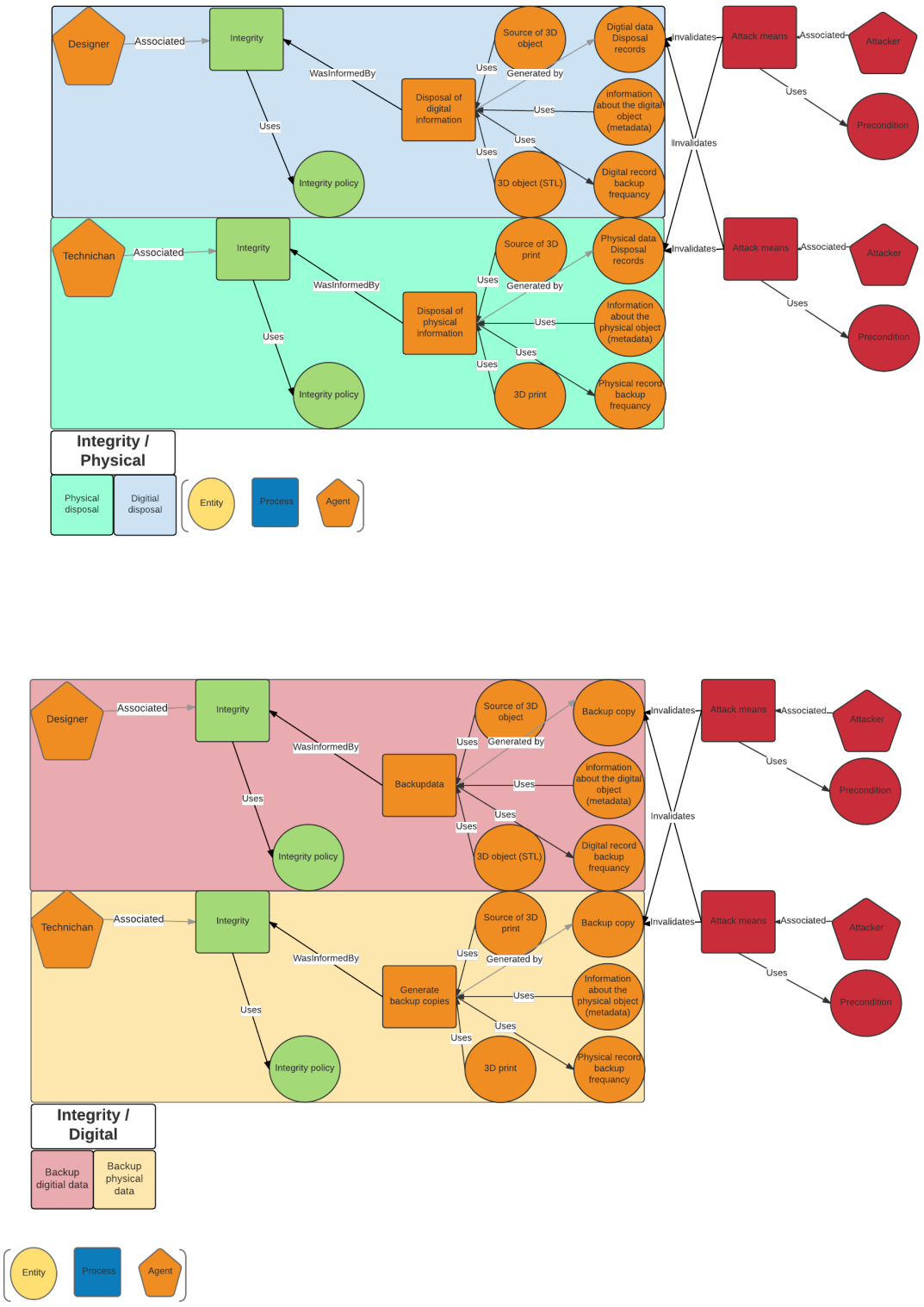



Figure B.18: Integrity hardening recommendations to patch threats to the additive manufacturing process

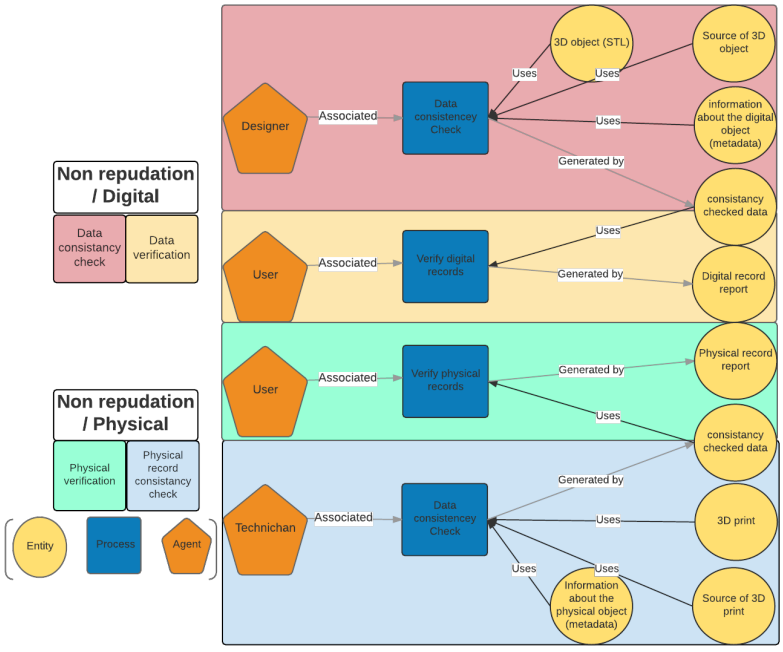



Figure B.19: What to make sure it's "Non-repudiated" in the additive manufacturing process

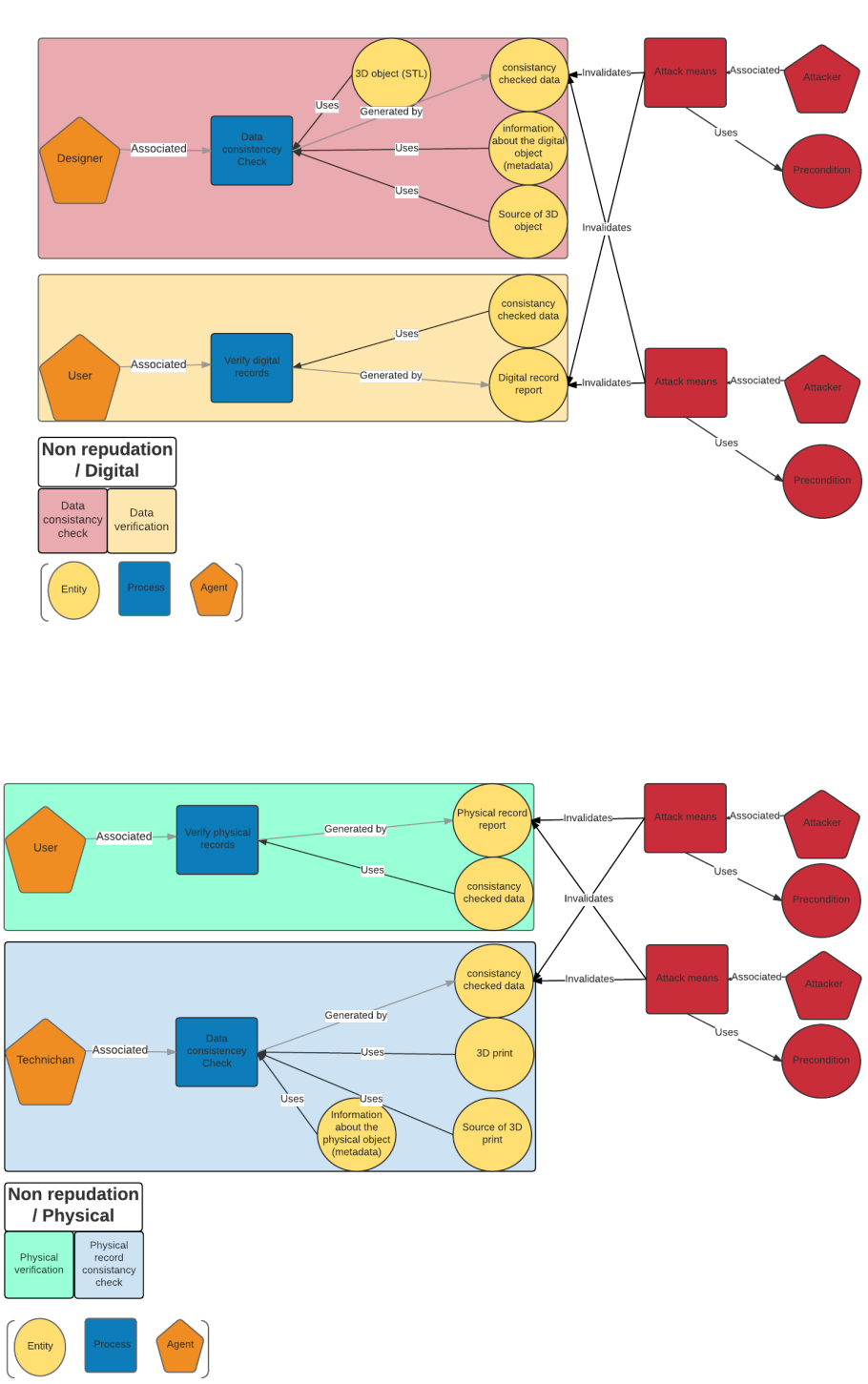



Figure B.20: Attack targets in the additive manufacturing process that will be exploited via Non-repudiation weakness

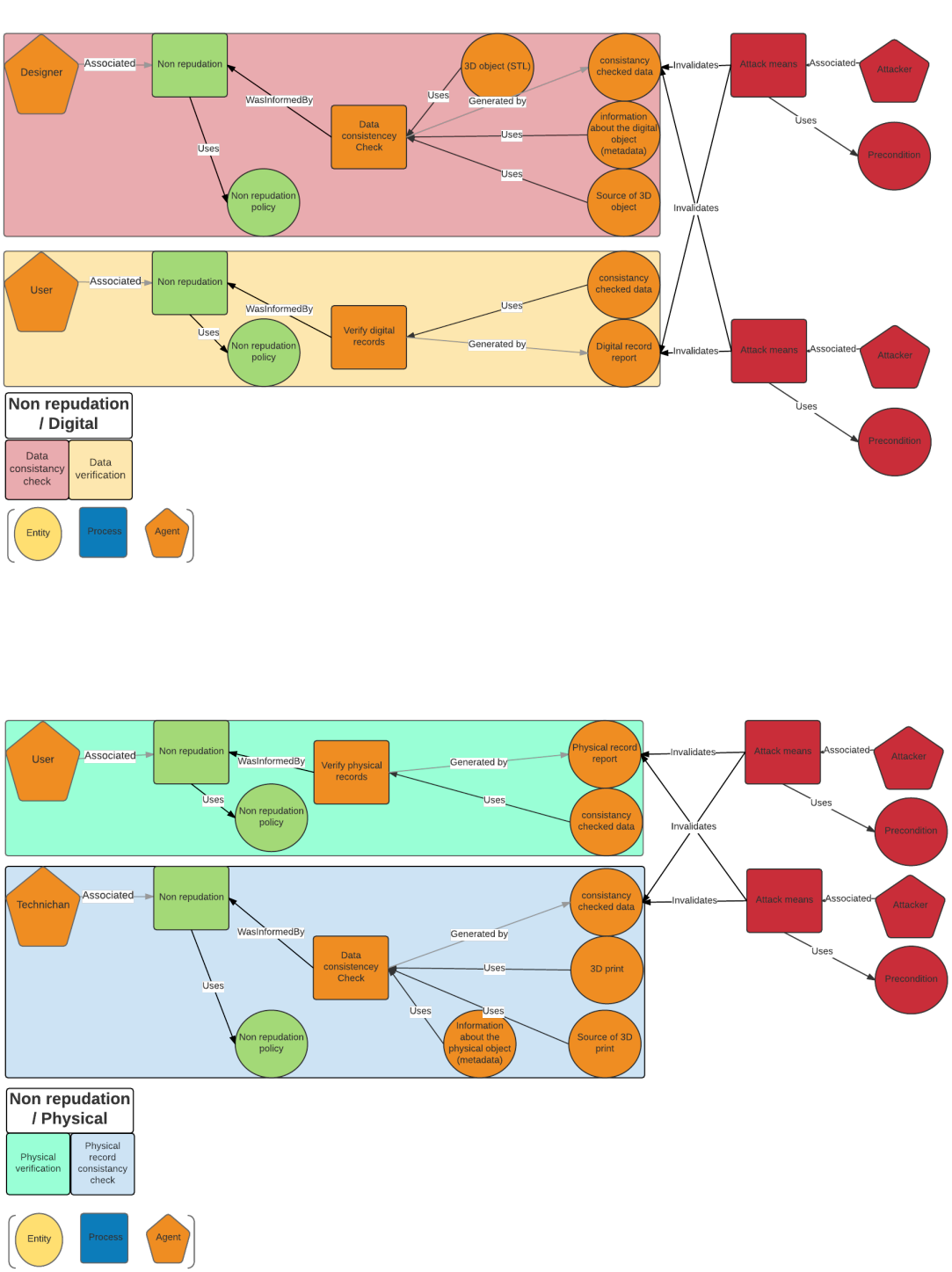



Figure B.21: Non-repudiation hardening recommendations to patch threats to the additive manufacturing process

# Appendix C

# User Interface Design

The following figures are the 3D provenance mockups for user interface design for the prototype validation.

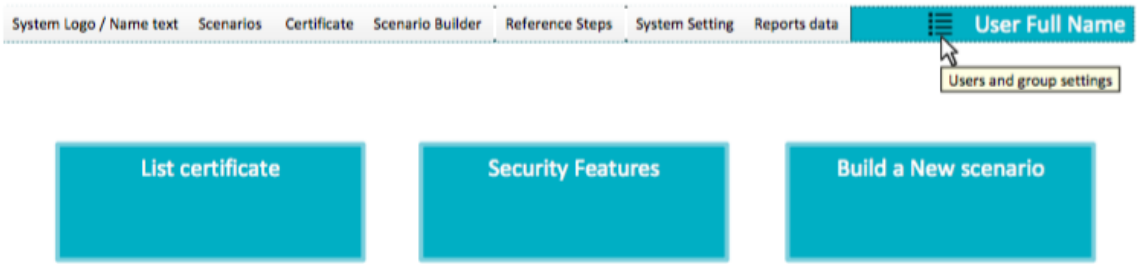



Figure C.1: Admin interface to the system / index

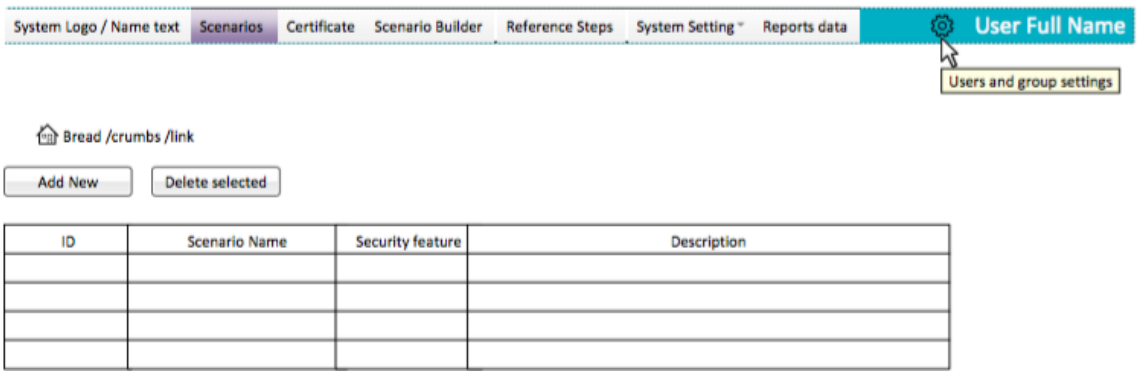



Figure C.2: Admin interface to the system / Scenario List

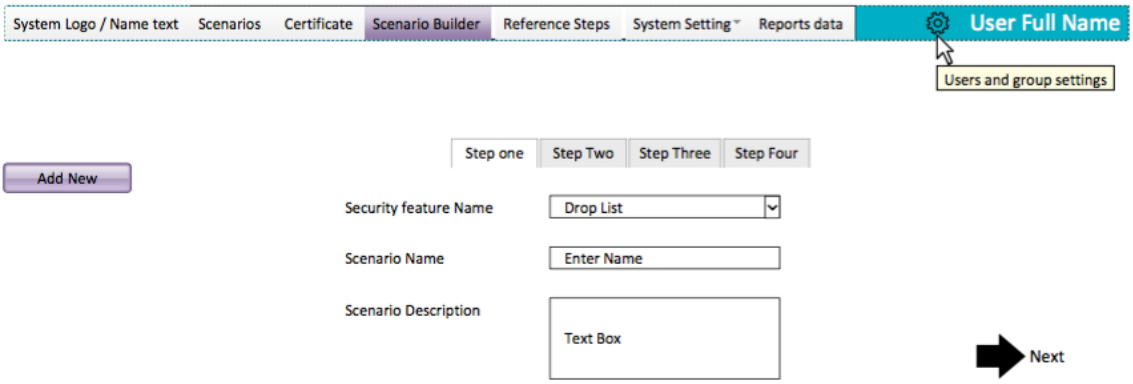



Figure C.3: Admin interface to the system / Scenario Add New Step 1 scenario basic information (take us to scenario builder)

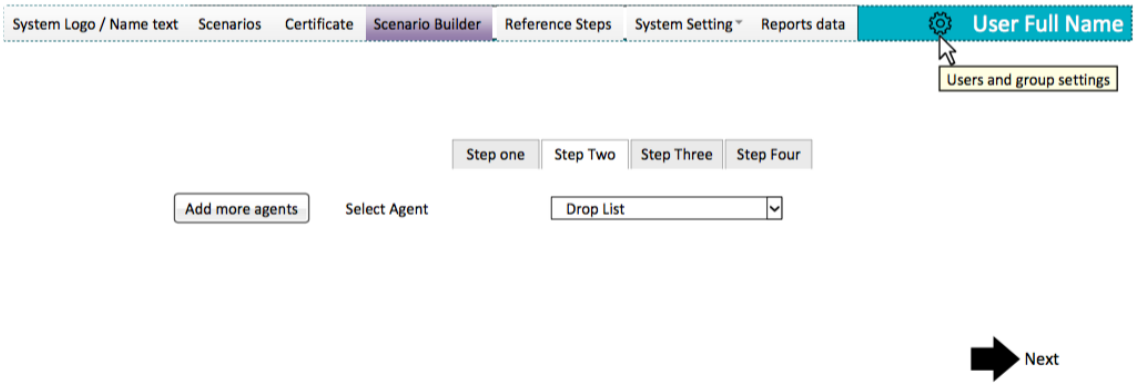



Figure C.4: Admin interface to the system / Scenario Add New Step 2 selecting agents (take us to scenario builder)

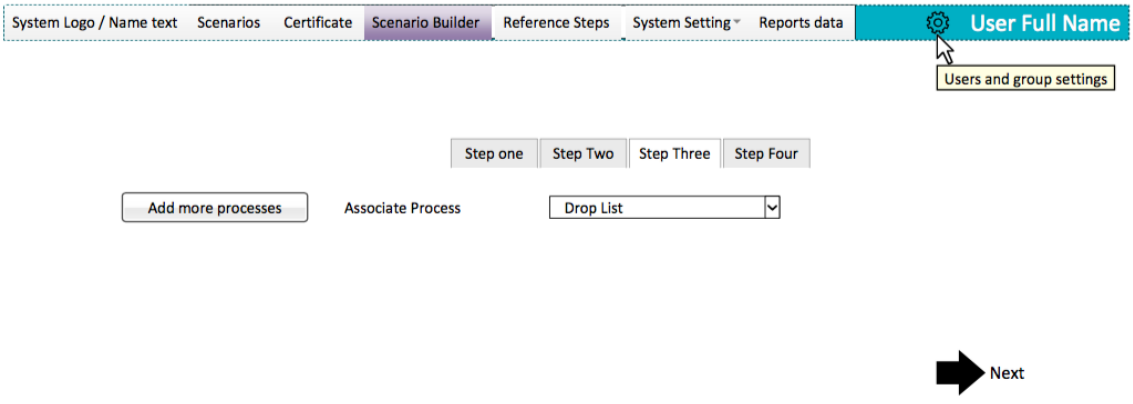



Figure C.5: Admin interface to the system / Scenario Add New Step 3 Associating processes (take us to scenario builder)

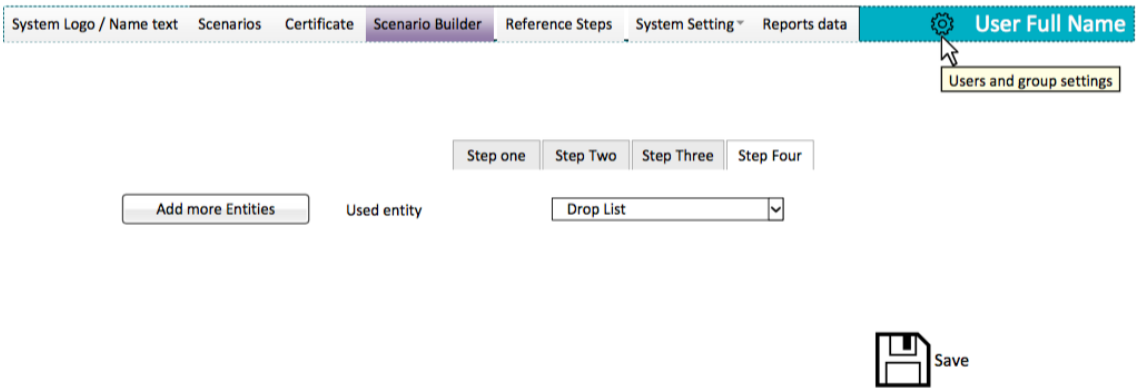



Figure C.6: Admin interface to the system / Scenario Add New Step 4 Used Entities (take us to scenario builder)

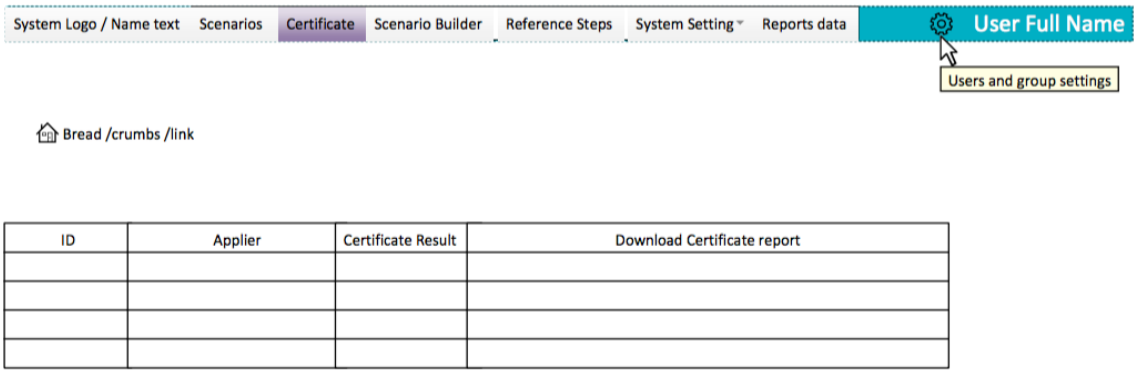



Figure C.7: Admin interface to the system / Certificate List

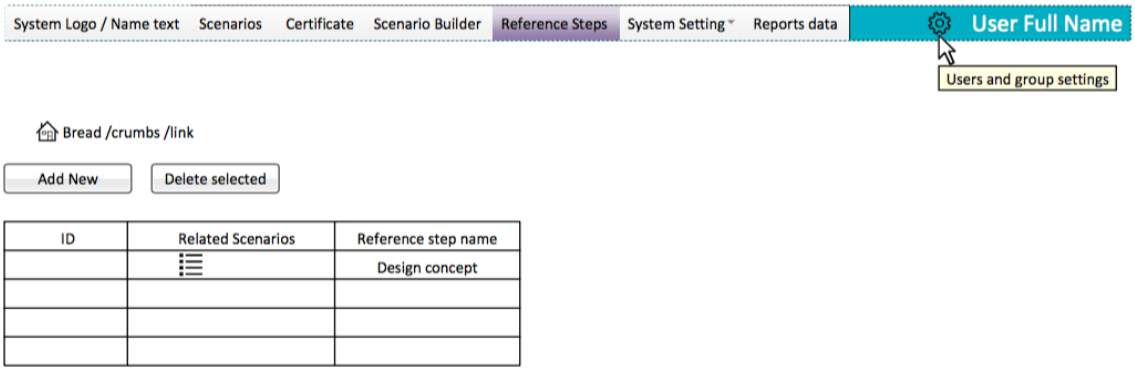



Figure C.8: Admin interface to the system / Reference Steps List

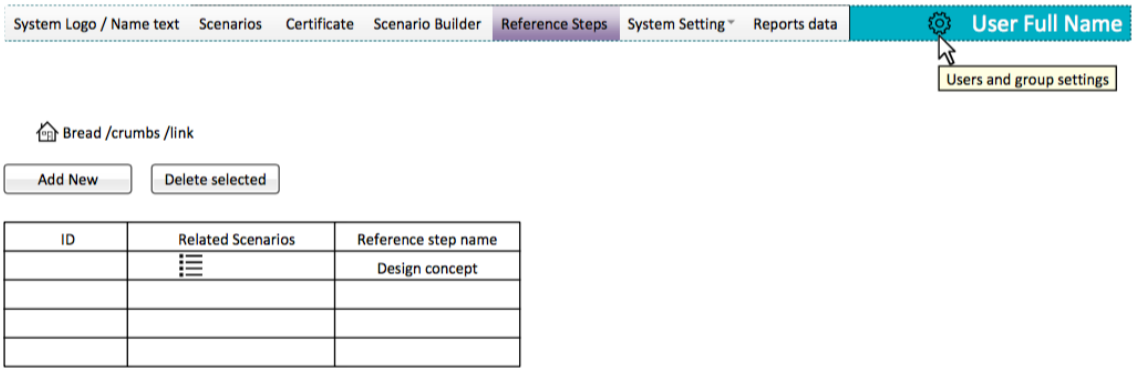



Figure C.9: Admin interface to the system / Reference Steps Add

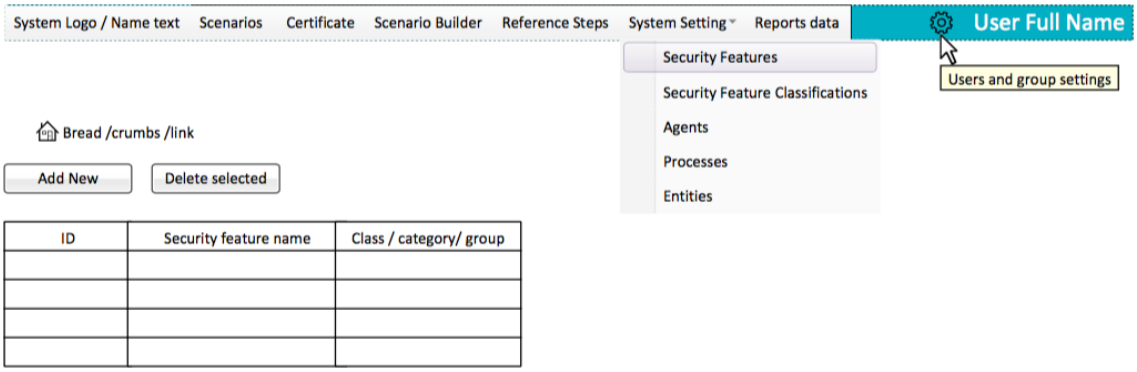



Figure C.10: Admin interface to the system / Security Features List

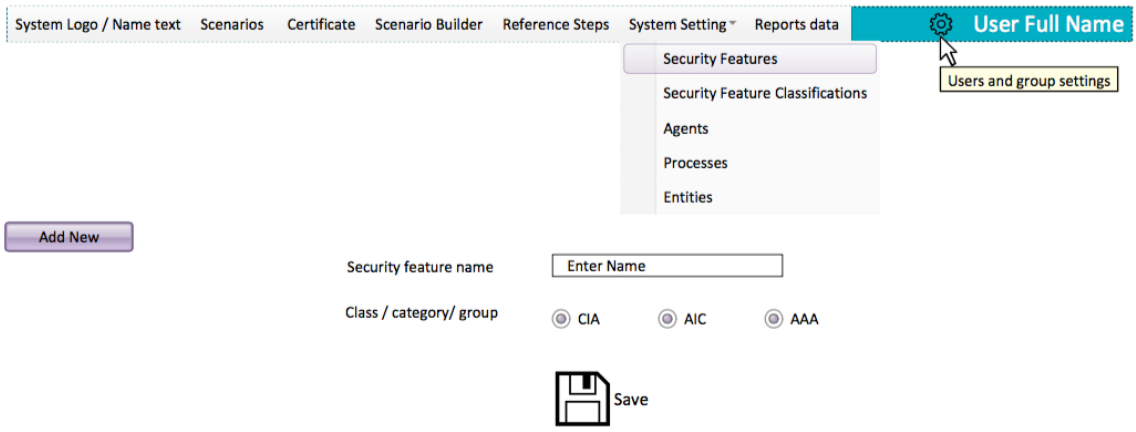



Figure C.11: Admin interface to the system / Security Features Add

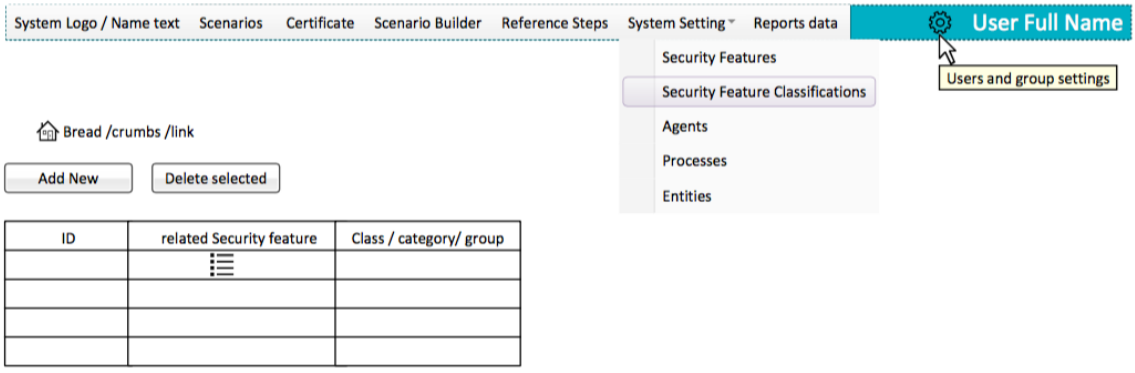



Figure C.12: Admin interface to the system / Security Features classification List

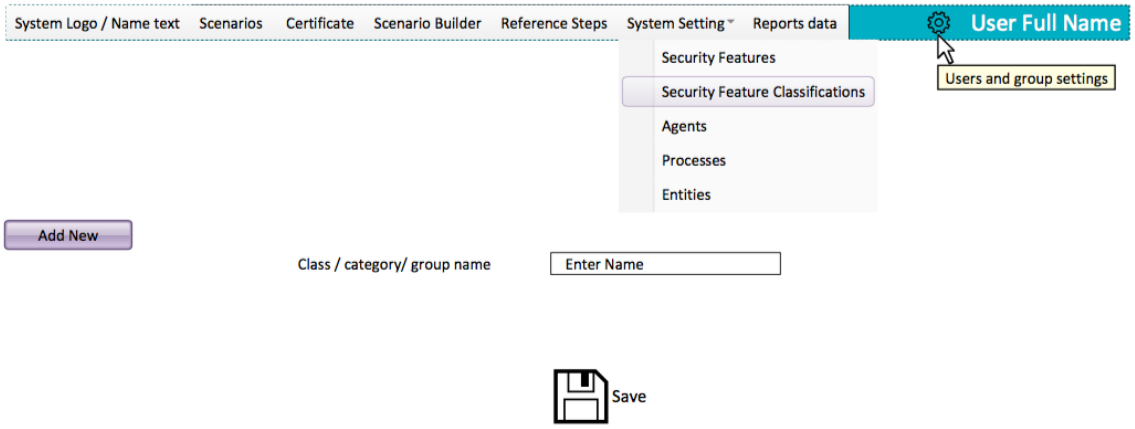



Figure C.13: Admin interface to the system / Security Features classification Add

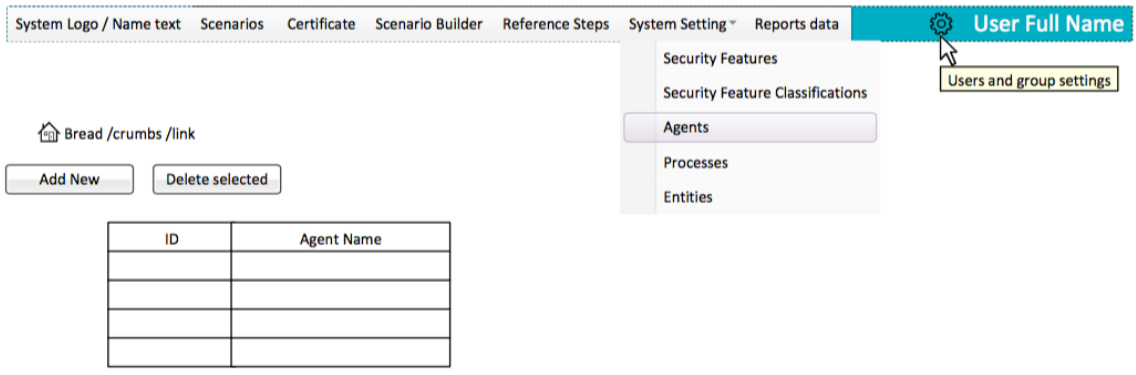



Figure C.14: Admin interface to the system /Agent List

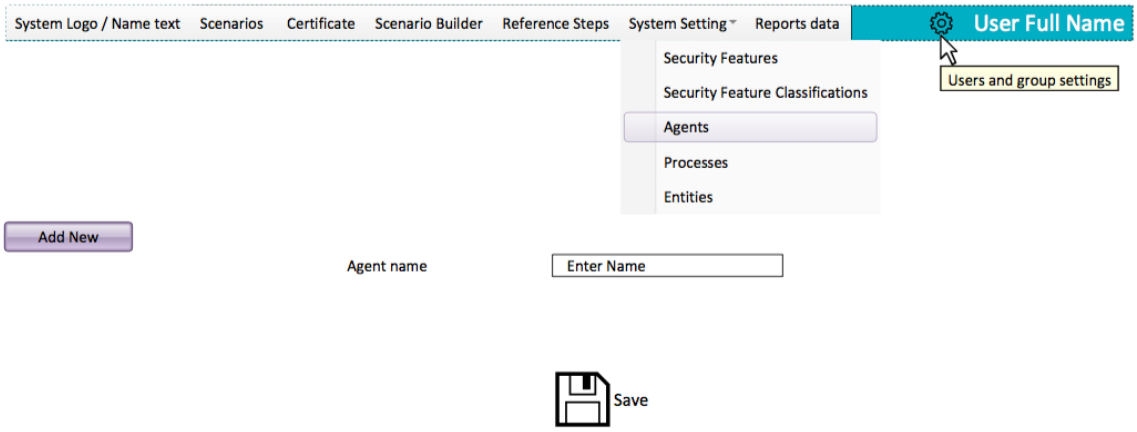



Figure C.15: Admin interface to the system / Agent Add

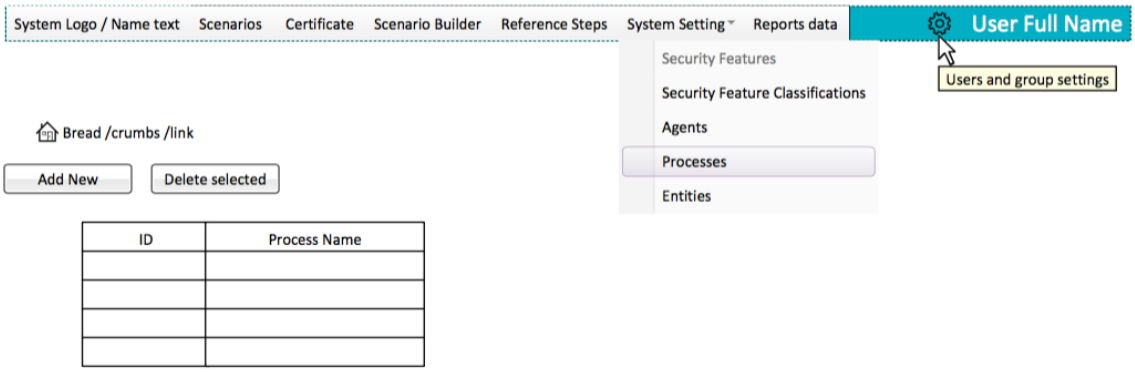



Figure C.16: Admin interface to the system / Process List

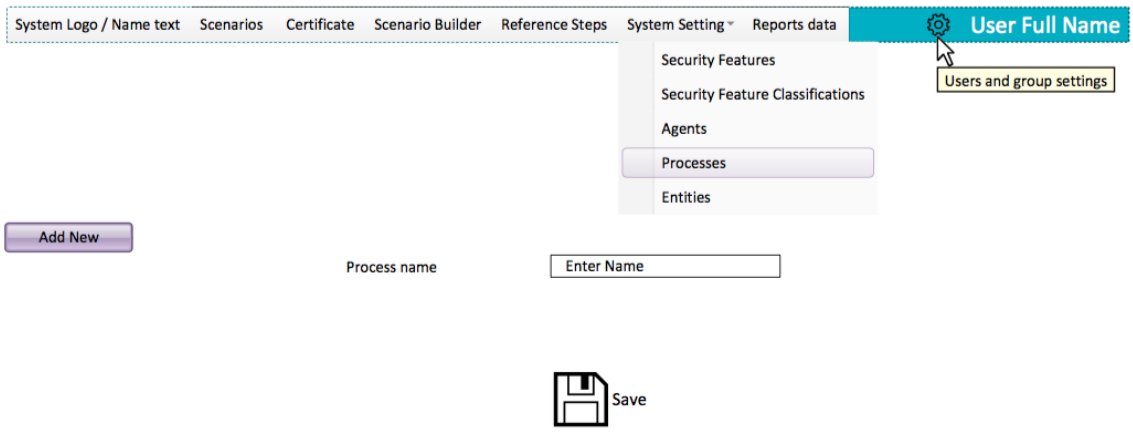



Figure C.17: Admin interface to the system / Process Add

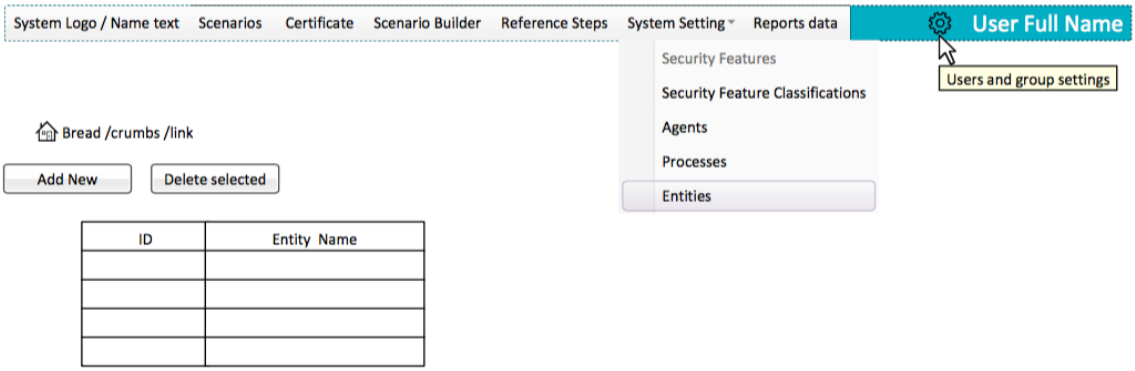



Figure C.18: Admin interface to the system / Entity List

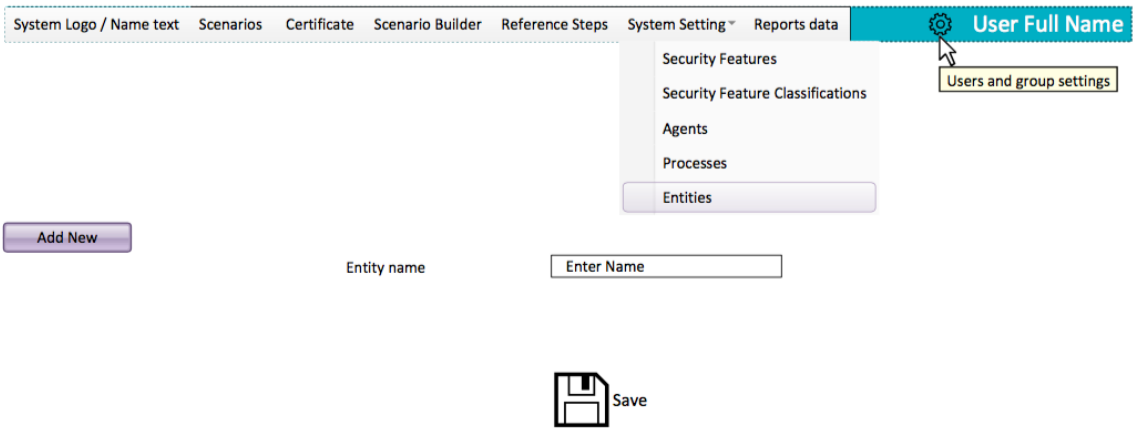



Figure C.19: Admin interface to the system / Entity Add

# Appendix D

# Software Requirement

The following sections are the functional and non functional requirements for 3D Prov cloud based system that provides security as a service

## D.1 Functional Requirement

Later in appendix E document we will describe the granular functions that support the high level functions. But in this section we will describe a higher level functions that the system must have and the following data processing support functions are:

- **Create Server Node:** Create new server nodes that is able to spawn clients. Typically, a server node will have hundreds of client nodes.
- **Create Client Node:** Create a client node that represent a supplier in the supply chain. The client node acts as an independent system for the client to measure their security.
- **Create Compliance:** Create new compliance template with categories and questions that provides an adequate description of the state of compliance.
- **Create Questions:** Create new questions to measure the compliance to government and organisation standards.
- **Create Canned Responses:** Create new canned response to questions. The canned responses are built in the system and will be reused in future deployments.
- **Create Reports:** Create new reports based on the compliance template that is generated from answers to questions and build the automated feedback based on the canned responses.
- **Read Reports:** Ability to access and read compliance reports.

- **Update Responses:** client can update the report based on the action list that the client was given
- **Update Knowledge Base:** Compliance, standards, scenarios, questions and canned responses are pushed to a central knowledge base server that will collect this data from all server nodes.
- **Delete Reports:** The client and consultant can delete a report if needed.

**User Characteristics** Basic user type are client and consultant, once we start testing the MVP well expect to add more specific user types such as administration, operations and maintenance.

- **Client:** Basic computer literacy, non security specialist
- **Consultant:** 5+ experience in cyber security and knowledge in ISO27001, Cyber security essentials, etc.

**Constraints** There are several constrains that limit the developers building the SECaaS system. Limitations such as:

- **Safety and security considerations:** The SECaaS must be built on high security standard.
- **Criticality of the application:** The SECaaS houses the evidence for security requirement which makes the system a target.
- **Regulatory policies:** The system it self must be complainant with the regulating compliance of the host country.
- **Interface to other applications:** The SECaaS needs to include API to upload documents, log files or any type of evidence.
- **Audit functions:** all actions on the system must be audit because it is built as a security tool.

**Assumptions and Dependencies** Based on the type of the 3D Prov SECaaS system the following dependencies can be assumed to provide by design. Such as the following:

- The 3D Prov SECaaS will be dependent on the server platform that is installed on it.
- The template of a compliance will need updating once new changes to the standard are introduced.

- Evidence collection in large supply chain will require a large amount of storage.

**Apportioning of Requirements** The order of importance for the requirements prioritisation is the following:

- **Scenario builder functions:** These function build scenarios of how a process of making something.
- **Security compliance templates:** This template will describe a security template.
- **Visualisation and graphing of the threat analysis:** This function will create visual presentation of the scenario, scenario with threat and scenario with threat and recommendations.
- **Evidence repository:** This function will collect evidence for compliance.
- **API for cloud storage:** This function will provide an application interface to communicate with cloud storage.

## D.2 Non-Functional Requirement

The SECaaS service is built as a self contained cloud based service that is designed to help an organisation and the companies in its supply chain to identify faults and vulnerabilities. The core is built to house compliance requirement questions; the compliance requirements are issued by the government in form of standards. The end users are not expected to be cyber security experts therefore the questions need to be simple and easy to understand. The feedback to the questions will be assessed and a score and set of recommendation is presented back to the client in form of an action list. The end user then acts on the action list and redo the application just for the sections that he was given feedback on.

**Interfaces** The SECaaS is totally self contained and dose not depend on other application other than the cloud service and its comparable to other SECaaS cloud services. Therefore the following is list of interface that are generally used typically with this kind of build.

- **System Interfaces:** The current SECaaS cloud system design does not have any API or interfaces with other pieces of software other than Database connections as this is self contained system. However, we recommend Google API to future proofing the system.

**Database interface:** This interface between the cloud service and the secure data storage. This interface is strictly for administrator use to maintain the data integrity. There is no GUI for this API as it is command prompt only.

**Google services API:** This interface between the user google storage and the cloud based SECaaS. This would be in a form of a GUI to import and export data between the client and the system.

- **Hardware Interfaces:** The cloud based service is web based and should run on current generation operating systems and mobile devices. The recommendation is to build this cloud based service using a suitable web framework such as Laraval PHP framework.
- **Communications Interfaces:** The communication protocol for the SECaaS should run on secure HTTPs and encrypted VPN to transfer sensitive company information. The security of the system operation is very important as it could reveal vulnerabilities in the manufactures using the system.

**Operations** The SECaaS should be customisable to operates according to the organisation security policy, the size of companies and the size of the supply chain. These factors will restrict the frequency of operation and frequency of updates, compliances and certification.

The modes of user operation are:

- **Client mode:** Where a client fills a compliance report and then receives an action list.
- **Consultant mode:** Where a consultant builds the compliance template based on the organisation requirement.

Periods of interactive operations and periods of unattended operations:

- Data inputs operation where client access the system to fill in questioners.
- Data analysis of vulnerabilities and threats in which this process operates unattended.
- Generate figures that reflect the manufacturing process and security operation.

Backup and recovery operations should run automatically and unattended and should have:

- Cloud based redundancy.

- Automated backup.

**Site Adaptation Requirements** The software requirement document describes a minimum viable product and we expect the initialisation requirement will increase after the first trial. However, currently the system need the following initialisation requirement:

- **System initiation:** The system needs a compliance template.
- **Software requirement:** Apache and SQLite DB server

# Appendix E

# System Functions

Based on the data described in F.0.1 the functions of the system are created to handle the inputs and output of the system functions and they are organised into six groups.

**User Management Functions:** Users and groups are management are responsible for creating, reading, updating, deleting groups and users as well as assigning users to groups, as show in Table E.1 and Table E.2.

Table E.1: User Management

| **Functions** | **Inputs** | **Returned Values** |
|---|---|---|
| Create (add) a user | Fields (Name, Email, Contact Number, User Type, Position, Company) | Confirmation message |
| Read user information | Fields (Name ID, Name) | Fields (Name, Email, Contact Number, User Type, Position, Company) |
| Update (edit) user information | Fields (Name, Email, Contact Number, User Type, Position, Company) | Confirmation message |
| Delete (Deactivate) a user | Fields (ID, Name) | Confirmation message |

This management interface will be responsible for assigning permissions to users and groups to have access to the system. Table E.3 is a list of the functions, inputs and outputs.

This interface is what the client sees when he accesses the system. This will give him access to the system functions as shown in Table E.4. Table E.5 is client user management.

**Scenario builder Administrator Functions:** The admin interface holds the building blocks for a production chain. This admin interface will allow the user to create custom building blocks, link them to scenarios and use them to generate the analysis.

Table E.2: Group Management

| **Functions** | **Inputs** | **Returned Values** |
|---|---|---|
| Adding user group | Fields (Name ID, Name,Group ID, Group Name) | Confirmation message |
| Read (list) user groups | Fields (Group ID, Group Name) | Fields (Name ID, Name) |
| Update (edit) user group | Fields (Name ID, Name,Group ID, Group Name) | Confirmation message |
| Assign and reassign user to group | Fields (Name ID, Name, Group ID, Group Name) | Confirmation message |

Table E.3: User and group permission management

| **Functions** | **Inputs** | **Returned Values** |
|---|---|---|
| Setting group permission | Permission to CRUD to the system and functions. | Confirmation message |
| Setting user permission | Permission to CRUD to the system and functions. | Confirmation message |

Table E.4: Client interface

| **Functions** | **Inputs** | **Returned Values** |
|---|---|---|
| Create (Apply) for self-assessment certificate | Fields (assessment ID, Assessment Name, Description) | Confirmation message |
| Read (View) list of reference steps that are certifiable | Fields (assessment ID, Assessment Name) | Fields (assessment ID, Assessment Name, Description, Refrence ID, Refrence name) |
| Read (View) list of scenarios for each reference step | Fields (assessment ID, Assessment Name) | List of associated Scenarios. |

Table E.5: Client profile management

| **Functions** | **Inputs** | **Returned Values** |
|---|---|---|
| Full name. | CRUD- Name | Confirmation message |
| Email address | CRUD- Email | Confirmation message |
| Contact number | CRUD- Number | Confirmation message |
| Company information | CRUD- Text | Confirmation message |

This interface will control the creation, control and association of the production chain building blocks. Table E.6, Table E.7 and Table E.8 describe the functions and (inputs/ outputs) for agents, processes and entities.

- **Agents management:** Agents are people, groups of people or an organisation. Agents are responsible for process(s). Agent management is responsible for creating, reading, updating, deleting agents, making agent associations with scenarios.

Table E.6: Agent management

| **Functions** | **Inputs** | **Returned Values** |
|---|---|---|
| Create (Add) new agent | Fields (Agent ID, Name, Description, Type [Drop Down]) | Confirmation message |
| Read (List) all the available agents. | Fields (Agent ID, Name, Description, Type [Drop Down]) | Information about agent(s). List of associated Scenarios. |
| Update (Edit) an agent. | Fields (Agent ID, Name, Description, Type [Drop Down]) | Confirmation message |
| Deleting an agent | Fields (Agent ID, Name, Scenario ID, Scenario Name) | Confirmation message, Unlink Scenario(s) |
| Edit (Link/Unlink) to the related scenario this agent involved in | Fields (Agent ID, Name, Scenario ID, Scenario Name) | Agent Scenario Associate message |

- **Process management:** Process are associated with agents and need input(s) to produce output(s). Process management is responsible for creating, reading, updating, deleting processes and making process associations with scenarios.
- **Entity management:** Entitles are either generated or used by process(s) or in other terms they can be inputs or output. Entity management is responsible for creating, reading, updating, deleting entities and making process associations with scenarios as well as related security questions.

**Scenarios setting:** A scenario is description of relationships between agents, process and entities. The scenario will also able to illustrate the threats and system hardening processes the functions described in Table E.9. The scenario management is a three step process agents Table E.10, process Table E.11 and entity Table E.12.

- **Scenario management:** The scenario management creates a canvas for pining process, entities and agents. The management will create an interface to link a scenario to the process, entities and agents therefore establishing relationships between them.

Table E.7: Process management

| **Functions** | **Inputs** | **Returned Values** |
|---|---|---|
| Create (Add) new process | Fields (Process ID, Name, Description, Network [Drop Down], Host [Drop Down], Asset) | Confirmation message |
| Read (List) all the available process | Fields (Process ID, Name, Description, Network [Drop Down], Host [Drop Down], Asset) | Information about Process (s). List of associated Scenarios. |
| Update (Edit) a process. | Fields (Process ID, Name, Description, Network [Drop Down], Host [Drop Down], Asset) | Confirmation message |
| Deleting a process | Fields (Process ID, Name, Scenario ID, Scenario Name) | Confirmation message, Unlink Scenario(s) |
| Edit (Link/Unlink) to the related scenario this process involved in | Fields (Process ID, Name, Scenario ID, Scenario Name) | Process Scenario Associate message |

Table E.8: Entity management

| **Functions** | **Inputs** | **Returned Values** |
|---|---|---|
| Create (Add) new entity | Fields (entity ID, Name, Description) | Confirmation message |
| Read (List) all the available entities | Fields (entity ID, Name, Description) | Information about entity (s), List of associated Scenarios. |
| Update (Edit) an entity . | Fields (entity ID, Name, Description) | Confirmation message |
| Deleting an entity | Fields (entity ID, Name, Scenario ID, Scenario Name) | Confirmation message, Unlink Scenario(s) |
| Edit (Link/Unlink) to the related scenario this entity involved in | Fields (entity ID, Name, Scenario ID, Scenario Name) | Entity Scenario Associate message, link Scenario(s), Unlink Scenario(s) |
| Edit (Link/Unlink) to the related security question(s) this entity involved in | Fields (entity ID, Name, Scenario ID, Scenario Name) | Entity Scenario Associate message, link Scenario(s), Unlink Scenario(s) |

Table E.9: Scenario management

| **Functions** | **Inputs** | **Returned Values** |
|---|---|---|
| Create (add) a scenario | Fields (Scenario ID, Name, Description) | Confirmation message |
| Read (list) a scenario | Fields (Scenario ID, Name, Description) | Information about scenarios and agents in the system |
| Update (edit) a scenario | Fields (Scenario ID, Name, Description) | Confirmation message |
| Deleting a scenario | Fields (Scenario ID, Name, Description) | Confirmation message, Unlink scenario to an agent |
| Link/ Unlink a scenario to certificates | Fields (Scenario ID, Name, Description, certificate id, certificate name) | Link scenario to certificates message, link scenario to related certificates., Unlink scenario to related certificates. |
| Link/ Unlink a scenario to agent | Fields (Scenario ID, Name, Description, agent id, agent name) | Link scenario to agent message, link scenario to related agent., Unlink scenario to related agent. |
| Link/ Unlink a scenario to process | Fields (Scenario ID, Name, Description, process id, process name) | Link scenario to process message, link scenario to related process., Unlink scenario to related process. |
| Link/ Unlink a scenario to entity | Fields (Scenario ID, Name, Description, entity id, entitiy name) | Link scenario to entity message, link scenario to related entity., Unlink scenario to related entity. |
| Link/ Unlink a scenario to security features | Fields (Scenario ID, Name, Description, security feature id, security name) | Link scenario to security features message, link scenario to related security features., Unlink scenario to related security features. |

- **Scenario agent linker:** Create scenario  agent, process and entities links, os a three step process where the agents will act as stakeholders or operators, the process are creation tools that need entities as inputs and produce other entities as output. This will be more apparent when linked to process and entities. The functions for linking the scenarios are in Table E.10, Table E.11 and Table E.12.

Table E.10: Scenario agent linker

| **Functions** | **Inputs** | **Returned Values** |
|---|---|---|
| Create (add) a relationship between a scenario and an agent | Fields (Scenario ID, Name, Description, agent ID, Name, Description) | Confirmation message |
| Read (list) all the linkage between scenarios and agents in the system. | Fields (Scenario ID, Name, Description, agent ID, Name, Description) | Information about scenarios and agents in the system |
| Update (edit) a relationship between a scenario and an agent | Fields (Scenario ID, Name, Description, agent ID, Name, Description) | Confirmation message |
| Deleting a relationship between a scenario and an agent | Fields (Scenario ID, Name, Description, agent ID, Name, Description) | Confirmation message, Unlink scenario to an agent |

Table E.11: Scenario process linker

| **Functions** | **Inputs** | **Returned Values** |
|---|---|---|
| Create (add) a relationship between a scenario and a process | Fields (Scenario ID, Name, Description, process ID, Name, Description) | Confirmation message |
| Read (list) all the linkage between scenarios and process in the system. | Fields (Scenario ID, Name, Description, process ID, Name, Description) | Information about scenarios and process in the system |
| Update (edit) a relationship between a scenario and a process | Fields (Scenario ID, Name, Description, process ID, Name, Description) | Confirmation message |
| Deleting a relationship between a scenario and a process | Fields (Scenario ID, Name, Description, process ID, Name, Description) | Confirmation message, Unlink scenario to an process |

- **Scenario security feature linker:** After the the agents, processes and entities are linked together to form a relationship set. The set is placed inside a security feature. Table E.13 is a list of the functions, inputs and outputs.

- **Production chain reference steps management:** The creation of a product goes through multiple steps from start to finish. This management interface will

Table E.12: Scenario entity linker

| **Functions** | **Inputs** | **Returned Values** |
|---|---|---|
| Create (add) a relationship between a scenario and an entity | Fields (Scenario ID, Name, Description, entity ID, Name, Description) | Confirmation message |
| Read (list) all the linkage between scenarios and entity in the system. | Fields (Scenario ID, Name, Description, entity ID, Name, Description) | Information about scenarios and entity in the system |
| Update (edit) a relationship between a scenario and an entity | Fields (Scenario ID, Name, Description, entity ID, Name, Description) | Confirmation message |
| Deleting a relationship between a scenario and an entity | Fields (Scenario ID, Name, Description, entity ID, Name, Description) | Confirmation message, Unlink scenario to an entity |

Table E.13: Scenario security feature linker

| **Functions** | **Inputs** | **Returned Values** |
|---|---|---|
| Create (add) a relationship between a scenario and a security feature | Fields (Scenario ID, Name, Description, security feature ID, Name, Description) | Confirmation message |
| Read (list) all the linkage between scenarios and a security features in the system. | Fields (Scenario ID, Name, Description, security feature ID, Name, Description) | Information about scenarios and security features in the system |
| Update (edit) a relationship between a scenario and a security feature | Fields (Scenario ID, Name, Description, security feature ID, Name, Description) | Confirmation message |
| Deleting a relationship between a scenario and a security feature | Fields (Scenario ID, Name, Description, security feature ID, Name, Description) | Confirmation message, Unlink scenario to an security feature |

link steps with each other to form a production chain. Table E.14 is the functions associated with production chain management.

**Certificate Management**

- **Certificates supervision:** Certification supervision managements creates certification sets that is comprised of set of categories of questions, answers and canned responses. Table E.15 is a list of the functions, inputs and outputs.

Table E.14: Production chain management

| **Functions** | **Inputs** | **Returned Values** |
|---|---|---|
| Create (add) step and link to scenario. | Fields (link ID, Name, Description, scenario(s) id, process(s) name) | Confirmation message |
| Read (List) all the available steps with links to Scenarios | Fields (link ID, Name, Description, scenario(s) id, process(s) name) | Information about link (s), List of associated Scenarios. |
| Update/Edit (Link/Unlink) to the related step | Fields (link ID, Name, Description, scenario(s) id, process(s) name) | Link Scenario Associate message, link Scenario(s), Unlink Scenario(s) |
| Delete Links between steps | Fields (link ID, Name, Description) | Confirmation message, Unlink Scenario(s) |

Table E.15: Certificate supervision

| **Functions** | **Inputs** | **Returned Values** |
|---|---|---|
| Create (add) new certificate to the system | Fields (cert ID, Name, Description, associated standard[drop down]) | Confirmation message |
| Read (list) all available certificates | Fields (cert ID, Name, Description, associated standard) | Information about all available certificates |
| Update (edit) a certificate | Fields (cert ID, Name, Description, associated standard) | Confirmation message |
| Delete a certificate | Fields (cert ID, Name, Description, associated standard) | Confirmation message, unlink category |
| Link/Unlink to a category | Fields (cert ID, Name, Description, associated standard, category ID, category name) | Confirmation message |

**Knowledge Management** Benchmark setting: The benchmark management will build questions, scales and responses to help build a customised benchmark. The benchmarking process needs a set of categories to group the questions to make sense of the information. The scales are built to satisfy the customer subjective security requirements. The responses interpret the answers to the questions and provide automated reports.

- **Category management:** The category management is responsible for grouping questions to answer overall objectives. Table E.16 is a list of functions, input and output of the category management.
- **Questions management:** The question management is a major piece of the system that is responsible for making the queries. The questions are not open

Table E.16: Category management

| **Functions** | **Inputs** | **Returned Values** |
|---|---|---|
| Create (add) new category for questions to the system | Fields (category ID, Name, Description) | Confirmation message |
| Read (list) all available categories | Fields (category ID, Name, Description) | Information about category (s) |
| Update (edit) a category | Fields (category ID, Name, Description) | Confirmation message |
| Delete a category | Fields (category ID, Name, Description) | Confirmation message, Unlink question to category(s), Unlink question answer to category(s) |
| Link/Unlink to the related questions for each category. | Fields (category ID, Name, Description, Question ID, Question Name) | Link Category to Question message, link question to category(s), Unlink question to category(s) |
| Link to the choices that answer the questions in any particular category. | Fields (category ID, Name, Description, Answer ID, Answer Name) | Link Category to Question Answer message, link question answer to category(s), Unlink question answer to category(s) |

ended and intended to collect quantitative data. Table E.17 is a list of functions, inputs and outputs for question management.

Table E.17: Questions management

| **Functions** | **Inputs** | **Returned Values** |
|---|---|---|
| Create (add) new questions to the system | Fields (question ID, Name, Description) | Confirmation message |
| Read (list) all available questions | Fields (question ID, Name, Description) | Information about question (s) |
| Update (edit) a question | Fields (question ID, Name, Description) | Confirmation message |
| Delete a question | Fields (question ID, Name, Description) | Confirmation message, Unlink question to related canned responses. |
| Link/Unlink to the related canned response for any particular question. | Fields (question ID, Name, Description, Question ID, Question Name) | Link Category to Question message, link question to related canned responses., Unlink question to related canned responses. |

- **Response choices management:** The data collected from the responses are

quantitative and not open ended, the responses are meaningless by their own therefore they need to be tied down to specific questions. Table E.18 is a list of the functions, inputs and outputs.

Table E.18: Response choices management

| **Functions** | **Inputs** | **Returned Values** |
|---|---|---|
| Create (add) new responses to the system | Fields (responses ID, Name, Description) | Confirmation message |
| Read (list) all available responses | Fields (responses ID, Name, Description) | Information about responses (s) |
| Update (edit) a responses | Fields (responses ID, Name, Description) | Confirmation message |
| Delete a responses | Fields (responses ID, Name, Description) | Confirmation message, Unlink responses to related canned responses. |
| Link/Unlink to the related canned response for specific question. | Fields (responses ID, Name, Description, Question ID, Question Name) | Link question to responses message, link question to related canned responses., Unlink question to related canned responses. |

- **Canned answers management:** A canned answer will depend on the algorithm that scores the answers to the questions. Its important that the canned answers be descriptive so it can generate meaningful reports. Table E.19 is a list of the functions, inputs and outputs.

Table E.19: Canned answers management

| **Functions** | **Inputs** | **Returned Values** |
|---|---|---|
| Create (add) new answer to the system | Fields (answer ID, Name, Description) | Confirmation message |
| Read (list) all available canned answers in the system. | Fields (answer ID, Name, Description) | Information about answer (s) |
| Update (edit) an answer | Fields (answer ID, Name, Description) | Confirmation message |
| Delete an answer | Fields (answer ID, Name, Description) | Confirmation message, Unlink answer to question |

# Appendix F

# Software Requirement

The following sections are a combination of MVC structure for cloud computing architecture and and the 3D Prov concept prototype in 9.2. The data structure requirements are described in F.0.1 and the data relationships requirements are described in F.0.2.

### F.0.1 Specific Database Requirement

The specific requirement will describe the data types, data structure and relationships. The Inputs and Outputs are centred around the function of the systems described earlier. The Inputs are compliance forms that are constructed inside the SECaaS cloud based system using scenario builder, each field is constructed inside the system. The Data structure for the database should have seven containers

**User Management Container** The user management container houses tables to support user managements functions such as creating users, assigning users to groups and give users and groups permissions to operate functions inside the SECaaS.

- **Users Details Table:** This Table will be dedicated to handling user information within the system. Table field should include.
  - User ID, Type: Integer
  - User Prefix Name, Type: Varchar
  - User First Name, Type: Varchar
  - User Last Name, Type: Varchar
  - User Position Name, Type: Varchar
  - User Company ID, Type: Integer
  - User Group ID, Type: Integer
  - User Email, Type: Varchar

  - Password, Type: Varchar

- **Groups Details Table:** This table is dedicated to handling group management where the administrator will have the ability to assign users into groups. Table fields should include.
  - Group ID, Type: Integer
  - Group Label, Type: Varchar
- **Members Table:** This table is a linking table describe user and group relationship that will serve the user assignment to groups functions.
  - User ID, Type: Integer
  - Group ID, Type: Integer
- **Associated Companies Table:** This table is dedicated to creating company account and associating it with groups and users.
  - Company ID, Type: Integer
  - Company Name, Type: Varchar
  - User ID, Type: Integer
  - Group ID, Type: Integer
- **Permissions Table:** This table describe user and group permission to use the systems function. The permissions function can make a new type of users by defining the functions permission that is given.
  - Permission Table name
  - Group ID, Type: Integer
  - Access Mask, Type: Varchar

**Scenario Builder Container** The scenario builder is responsible for building a manufacturing scenario to produce a product. This is the most important container as it holds the essence for the 3D Prov SECaaS cloud service. Scenario, Scenario Feature and Feature Tables are linked together in order to associate a security property with a scenario:

- **Scenario Table:** this table is main table that is associated scenario and security features as well as the reference step.
  - Scenario ID, Type: Integer
  - Scenario Name, Type: Varchar
  - Scenario Description, Type: Varchar

  - Reference ID, Type: Integer

- **Scenario Feature Table:** this table is a linking table to assign scenarios to security features.
  - Scenario Feature ID, Type: Integer
  - Scenario ID, Type: Integer
  - Feature ID, Type: Integer
- **Feature Table:** this table is responsible for assigning security features.
  - Feature ID, Type: Integer
  - Feature Name, Type: Varchar

**Reference Manufacturing steps Container** Reference, Manufacturing, and Manufacturing Step Table are linked together to create a process that is composed of multiple steps that are linked to manufacturing process.

- **Reference Table:** this table is a linking table responsible for assigning a scenario to manufacturing Step.
  - Reference ID, Type: Integer
  - Reference Name, Type: Varchar
  - Manufacturing ID
- **Manufacturing Table:** this table is a manufacturing table that describes a manufacturing process with multiple steps
  - Manufacturing ID, Type: Integer
  - Manufacturing Name, Type: Varchar
  - Manufacturing Description, Type: Varchar
  - Step ID, Type: Integer
- **Manufacturing Step Table:** this table is contains the steps for manufacturing an object.
  - Step ID, Type: Integer
  - Step Name, Type: Varchar
  - Step Description, Type: Varchar

**Entites, Process and Agents Container** The scenario builder will first create the building blocks and the scenario builder has three sub blocks, the entities, processes and agents.

- **Entity Table:** Is a table containing the entities associated with scenario. An entity can be an input or an output of a process.
  - Entity ID, Type: Integer
  - Entity Name, Type: Varchar
- **Entity Scenario Builder Table:** Is a linking table between scenario and entities, assigining entities to scenarios will help build
  - Entity scenario ID, Type: Integer
  - Scenario ID, Type: Integer
  - Entity ID, Type: Integer
- **Process Table:** Is a table containing the process associated with scenario.
  - Process ID, Type: Integer
  - Process Name, Type: Varchar
- **Process Scenario Builder Table:** Is a linking table between scenario and entities
  - Process scenario ID, Type: Integer
  - Scenario ID, Type: Integer
  - Process ID, Type: Integer
- **Agent Table:** Is a table containing the agent associated with scenario
  - Agent ID, Type: Integer
  - Agent Name, Type: Varchar
- **Agent scenario builder Table:** Is a linking table between scenario and entities
  - Agent scenario ID, Type: Integer
  - Scenario ID, Type: Integer
  - Agent ID, Type: Integer

**Security Standards Container** Security standards table will house the standard and associated scenarios that make up the standard compliance.

- **Standard scenario Table:** Is a linking table between scenario and Standards
  - Standard ID, Type: Integer
  - Scenario ID, Type: Integer

- **Standard Table:** Is a table containing the compliance standard requirement for a company
  - Standard ID, Type: Integer
  - Standard Name, Type: Varchar
  - Standard Decription, Type: Varchar
  - User ID, Type: Integer

**Certificate Management Container** The certificate management create certificates by combining several scenarios, scales and canned responses to produce a certificate score and feedback.

- **Certificate Table:** Is a table containing the custom made certificate that is made for a specific company security requirements
  - Certificate ID, Type: Integer
  - Company ID, Type: Integer
  - Scenario ID, Type: Integer
  - Date Taken, Type: datetime
  - Score, Type: Integer
  - Max Score, Type: Integer
  - Last Edit, Type: datetime
  - User ID, Type: Integer
- **Response Table:** Is a table containing the responses to a certificate and this table enables the system to generate a report of security compliance level with feedback
  - Responce ID, Type: Integer
  - Certificate ID, Type: Integer
  - Question ID, Type: Integer
  - Choice ID, Type: Integer
  - Canned ID, Type: Integer
  - Responce Score, Type: Integer
  - Last Edit, Type: datetime
  - User ID, Type: Integer

**Knowledge Management Container** Knowledge management contains questions and question categories with scales and canned responses as feedback to questions.

- **Questions Table:** Is a table that is responsible for creating the questions to measure the security of an input or an output (entity).
  - Question ID, Type: Integer
  - Entity ID, Type: Integer
  - Question Category ID, Type: Integer
  - Question, Type: Varchar
- **Questions Category Table:** Is a table that is reponcible for grouping questions into categories.
  - Question Category ID, Type: Integer
  - Question Category Name, Type: Varchar
- **Canned Answers Table:** Is a table contains the canned responses to a question and this table enables the system to generate a feedback
  - Canned ID, Type: Integer
  - Question ID, Type: Integer
  - Choice ID, Type: Integer
  - Canned Answer, Type: Varchar
  - Choice Score, Type: Integer
  - Is Max, Type: Tiny Integer
- **Choices Table:** Is a table that is responsible for creating the customised scale to measure security.
  - Choice ID, Type: Integer
  - Question Category ID, Type: Integer

### F.0.2 Logical Database Requirements

The logical requirements are grouped into six containers

- **User Management Container:** A user must be assigned to a company or more to be able to manage one company or more.
  - User ID that is primary key in Users and forging key in Companies and the type of relationship is zero or one to zero or many.

  A user purpose in the system is establish a security compliance therefore a user is expected to fulfil a security standard or many standards.

  - User ID that is primary key in Users and forging key in Standard and the type of relationship is zero or one to many. A user can be assigned to one or more groups
  - Group ID that is primary key in Users and forging key in Groups and the type of relationship is zero or many to zero or many.

  Permissions are given to users to manage the system.

  - Permission ID that is primary key in Rights Table and forging key in Members and the type of relationship is zero or one to zero or many.

  A user can apply to get a certificate and a certificate is only given when its above a certain score.

  - User ID that is primary key in Users and forging key in Certificates and the type of relationship is one or zero to zero or many.

- **Scenario Builder Relationship:** We can consider the Scenarios Table as the major component of the system and it has the following relationships.

  A single scenario can have a significant number of many security features

  - Scenario ID that is primary key in Scenarios and forging key in Scenario Feature and the type of relationship is zero or one to zero or many.

  Each security feature can be assigned to many scenario features.

  - Security Feature ID that is primary key in Security Feature and forging key in Scenario Feature and the type of relationship is zero or one to zero or many.

  A scenario has many entities as input or outputs

  - Scenario ID that is primary key in Scenarios and forging key in Entity Scenario Builder and the type of relationship is zero or one to zero or many.
  - Entity ID that is primary key in Entities and forging key in Entity Scenario using and the type of relationship is zero or one to zero or many.

  An entity is associated with many questions to test the entity.

  - Entity ID that is primary key in Entities and forging key in Questions using and the type of relationship is zero or one to zero or many.

  A scenario has many processes as that make input or outputs

  - Scenario ID that is primary key in Scenarios and forging key in Process Scenario Builder and the type of relationship is zero or one to zero or many.

  - Process ID that is primary key in Processes and forging key in Process Scenario Builder and the type of relationship is zero or one to zero or many.

  A scenario has many stakeholders as agents for the processes

  - Scenario ID that is primary key in Scenarios and forging key in Agents Scenario Builder and the type of relationship is zero or one to zero or many.
  - Agent ID that is primary key in Agents and forging key in Agents Scenario Builder and the type of relationship is zero or one to zero or many.

  A scenario is only one part of bigger process so it needs me assigned a reference step.

  - Reference ID that is primary key in Reference Step and forging key in Scenarios and the type of relationship is zero or one to zero or many.
  - Manufacturing ID that is primary key in Manufacturing and forging key in Reference Step and the type of relationship is zero or one to zero or one.
  - Step ID that is primary key in Manufacturing Step and forging key in Manufacturing Step and the type of relationship is zero or one to zero or many.

  A scenario can be reused to be used as part of another standard scenario

  - Scenario ID that is primary key in Scenarios and forging key in Standard Scenario and the type of relationship is one and only one to zero or many.

  A certificate is issued based on combining several scenarios

  - Scenario ID that is primary key in Scenarios and forging key in Certificates and the type of relationship is one and only one to zero or many.

- **Security Standards:** A standard is constructed using several standard scenarios

  - Standard ID that is primary key in Standard and forging key in Standard Scenario and the type of relationship is one and only one to zero or many.

- **Certificate Management:** A certificate is issues based on a score that is a result of many responses.

  - Certificate ID that is primary key in Certificates and forging key in Responses and the type of relationship is zero or one to zero or many.

- **Knowledge Management:** A question can have many canned answers based on the score.

  - Question ID that is primary key in Questions and forging key in Canned Answers and the type of relationship is zero or one to zero or many. Each Canned answer has many choices

- Choice ID that is primary key in Choices and forging key in Canned Answers and the type of relationship is zero or one to zero or many. One question category has many questions.
- Question Cat ID that is primary key in Question Cat and forging key in Choices and the type of relationship is zero or one to zero or many.

# References

(2009). *STL 2.0: A Proposal for a Universal Multi-Material Additive Manufacturing File Format*, number 1.

17296-4:2014, I. (2013). Draft BS ISO 17296-4 Additive manufacturing - Rapid technologies (rapid prototyping).

21827:2008, I. (2008). Information technology – Security techniques – Systems Security Engineering – Capability Maturity Model ( SSE-CMM ).

52915, B. I. D. (2013). Draft BS ISO DIS 52915 Additive manufacturing file format (AMF) Version 1.1.

7498:1984, I. (1984). Information Processing Systems, Open Systems Interconnection, Basic Reference Model. *International Standards Organization, Geneva, Switzerland*.

Abel, R. L., Parfitt, S., Ashton, N., and Lewis, S. G. (2011). Digital preservation and dissemination of ancient lithic technology with modern micro-CT. *Computers & Graphics*, 35(4):878–884.

Abolghasemi, M., Aghainia, H., Faez, K., and Mehrabi, M. A. (2008). LSB data hiding detection based on gray level co-occurrence matrix (GLCM). In *Proc. Int. Symp. Telecommunications IST 2008*, pages 656–659.

Alface, P. and Macq, B. (2007). From 3D mesh data hiding to 3D shape blind and robust watermarking: a survey. *Transactions on data hiding and multimedia security II*, pages 91–115.

Allard, T. (2005). Use of hand-held laser scanning and 3d printing for creation of a museum exhibit. *6th International Symposium on Virtual Reality, Archaelogy and Cultural Heritage*.

Andrew Moir, Anthony Dempster, Rachel Montagnon, D. B. and Woods, R. (2016). 3D printing: the legal implications of an emerging new technology. *PLC Magazine*.

Archibald, M. M. (2016). Investigator triangulation: A collaborative strategy with potential for mixed methods research. *Journal of Mixed Methods Research*, 10(3):228–250.

AutoCAD (2014). Autodesk, AutoCAD, 2014 Documentation.

Bak, D. (2003). Rapid prototyping or rapid production? 3D printing processes move industry towards the latter. *Assembly Automation*, 23(4):340–345.

Belanger, M. (2011). Amazon. com's Orwellian Gaffe: The Legal Implications of Sending E-Books Down the Memory Holy. *Seton Hall L. Rev.*, 41:361.

Berman, B. (2011). 3-D printing: The new industrial revolution. *Business Horizons*, 55(2):155–162.

Beuvray, M. (2008). *Archaeology iSpace*.

Birnholtz, J. (2006). What does it mean to be an author? The intersection of credit, contribution, and collaboration in science. *Journal of the American Society for Information Science and Technology*, 57(13):1758–1770.

Boritz, J. E. (2005). IS practitioners' views on core concepts of information integrity. *International Journal of Accounting Information Systems*, 6(4):260–279.

Bourke, P. (2012). PLY - Polygon File Format. Stanford University.

Bradshaw, S., Bowyer, A., and Haufe, P. (2010). The intellectual property implications of low-cost 3D printing. *ScriptEd*, 7(1):5–31.

Burkardt, J. (2004). OBJ Files - A 3D Object Format. Stanford University.

Burrows, M., Abadi, M., and Needham., M. (1989). A logic of authentication. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 426(1871):233–271.

Caldiera, V. and Rombach, H. (1994). The goal question metric approach. *Encyclopedia of software engineering*, 2:1–10.

Celani, G., Cancherini, L., and Jardini, A. (2009). 3D digitation of museum sculptures for model-making purposes: difficulties and possible solutions. *Anais do VRAP*, pages 1–4.

Chaudhry, P. E. and Walsh, M. G. (1996). An assessment of the impact of counterfeiting in international markets: The piracy paradox persists. *The Columbia Journal of World Business*, 31(3):34–48.

Congress, U. (1998). Digital millennium copyright act. *Public Law*, 105(304):112.

Consortium, M. (2015). 3D Manufacturing Format 3MF. Technical report, 3MF Consortium.

Copeland, B. J. (2010). *Colossus: The secrets of Bletchley Park's code-breaking computers*. Oxford University Press, Inc., New York, NY, USA.

Cullen, C. T., Hirtle, P. B., Levy, D., Lynch, C. A., and Rothenberg, J. (2000). *Authenticity in a Digital Environment.* ERIC.

Curless, M. and Levoy., B. M. (1996a). 3D Fax.

Curless, M. and Levoy., B. M. (1996b). A Volumetric Method for Building Complex Models from Range Images Volumetric integration. In *SIGGRAPH 96 Proceedings of the 23rd annual conference on Computer graphics and interactive techniques*, pages 303–312, New York, USA. ACM, ACM.

Davies, D. (1983). Applying the RSA digital signature to electronic mail. *Computer*, 16(2):55–62.

Delgado, I. N., Fonseca, D., and Salle, A. L. (2012). Architecture Degree Project: Use Of 3d Technology, Models And Augmented Reality Experience With Visually Impaired Users. *iiisci.org*, 10(2):57–62.

Dictionary, O. E. (2007). Oxford english dictionary online.

Engel, K. and Sommer, O. (1999). Remote 3d visualization using image-streaming techniques. *ISIMADE-11 TH Internationl Conference on Systems Research, Informatics and Cybernetics.*

Fadhel, N., Crowder, R. M., and Wills, G. (2015). Provenance in the Additive Manufacturing Process. *IFAC-PapersOnLine*, 48(3):2345–2350.

Fadhel, N. F., Crowder, R. M., Akeel, F., and Wills, G. B. (2014). Component for 3D printing provenance framework: Security properties components for provenance framework. *Internet Security (WorldCIS), 2014 World Congress on*, pages 91–96.

Fadhel, N. F., Crowder, R. M., and Wills, G. B. (2013a). Approaches to Maintaining Provenance throughout the Additive Manufacturing Process. *World Congress on Internet Security (WorldCIS), 2013*, pages 82–87.

Fadhel, N. F., Crowder, R. M., and Wills, G. B. (2013b). Maintaining provenance throughout the additive manufacturing process. *IJISR*, 3(3):466–475.

Forte, M. and Kurillou, G. (2012). Teleimmersive Archaeology. *Archeomatica*, pages 40–45.

Garg, H., Agrawal, S., and Varshney, G. (2012). Double Security Watermarking Algorithm for 3D Model using IEEE-754 Floating Point Arithmetic. *International Journal of Computer Applications*, 46(9):18–22.

Gill, R. and Syan, C. S. (2006). Demystification of concurrent engineering. In *CAD/CAM Robotics and Factories of the Future: 22nd International Conference 19th-22nd July*, pages 981–987. Narosa Publishing House.

Gilman, C. R. and Rock, S. J. (1995). The use of step to integrate design and solid freeform fabrication. In *Proc., Solid Freeform Fabrication Symposium*.

Grosman, L., Smikt, O., and Smilansky, U. (2008). On the application of 3-D scanning technology for the documentation and typology of lithic artifacts. *Journal of Archaeological Science*, 35(12):3101–3110.

Groth, P. and Moreau, L. (2013). Prov-n: The provenance notation. Technical report, W3C.

Guion, L. A., Diehl, D. C., and Mcdonald, D. (2010). *Triangulation: Establishing the Validity of Qualitative Studies.* University of Florida.

Hartley, R. I. and Sturm, P. (1997). Triangulation. *Computer vision and image understanding*, 68(2):146–157.

Hawi, T. A., Qutayri, M. A., and Barada, H. (2004). Steganalysis attacks on stego-images using stego-signatures and statistical image properties. In *Proc. TENCON 2004. 2004 IEEE Region 10 Conf*, pages 104–107.

Hull, C. W. (1986). Apparatus for production of three-dimensional objects by stereolithography. US Patent 4,575,330.

Islam, S. and Falcarin, P. (2011). Measuring security requirements for software security. *2011 IEEE 10th International Conference on Cybernetic Intelligent Systems (CIS)*, pages 70–75.

Jick, T. D. (1979). Mixing Qualitative and Quantitative Methods: Triangulation. *Action. Qualitative Methodology*, (24):602–611.

Johnson, N. F. and Jajodia, S. (1998). Exploring steganography: Seeing the unseen. *IEEE computer*, 31(2):26 – 34.

Johnson, R. B. and Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *Educational researcher*, 33:14–26.

Johnson, R. B., Onwuegbuzie, A. J., and Turner, L. A. (2007). Toward a definition of mixed methods research. *Journal of mixed methods research*, 1(2):112–133.

Jones, D. E. (1974). Ariadne Column. *New Scientist*, 64(917):80.

Kaplowitz, M. D. and Hoehn, J. P. (2001). Do focus groups and individual interviews reveal the same information for natural resource valuation. *Ecological Economics*, 2(36):237–247.

Karasik, A. and Smilansky, U. (2008). 3D scanning technology as a standard archaeological tool for pottery analysis: practice and theory. *Journal of Archaeological Science*, 35(5):1148–1168.

Kharif, O. and Decker, S. (2013). 3-D Printing Stirs Copyright Clash on Homemade IPhone Gear: Tech. *www.bloomberg.com*.

Koller, D. and Levoy, M. (2005). Protecting 3d graphics content. *Communications of the ACM*, 48(6):74–80.

Levy, G., Schindel, R., and Kruth, J. (2003). Rapid manufacturing and rapid tooling with layer manufacturing (LM) technologies, state of the art and future perspectives. *CIRP Annals-Manufacturing Technology*, 2(Lm).

Lie, W.-N. and Chang, L. C. (1999). Data hiding in images with adaptive numbers of least significant bits based on the human visual system. In *Image Processing, 1999. ICIP 99. Proceedings. 1999 International Conference on*, volume 1, pages 286 –290 vol.1.

Likert, R. (1932). A technique for the measurement of attitudes. *Archives of psychology*, 22(140):55.

Lin, C.-H., Liu, J.-C., Shih, C.-H., and Lee, Y.-W. (2008). A Robust Watermark Scheme for Copyright Protection. In *Proc. Int. Conf. Multimedia and Ubiquitous Engineering MUE 2008*, pages 132–137.

Manacorda, S. and Chappell, D., editors (2011). *Crime in the Art and Antiquities World*. Springer New York, New York, NY.

Maryon, H. (1956). The Colossus of Rhodes. *The Journal of Hellenic Studies*, 76:68–86.

McConnell, J. (1994). National Training Standard for Information Systems Security (INFOSEC) professionals.

Mellis, D. A. (2011). *Case Studies in the Digital Fabrication of Open-Source Consumer Electronic Products*. PhD thesis, Massachusetts Institute of Technology.

Moreau, L., Clifford, B., Freire, J., and Futrelle, J. (2011). The open provenance model core specification (v1. 1). *Future Generation computer systems*, 27(6):743–756.

Moreau, Luc and Missier, P. (2013). Prov-dm: The prov data model.

Niven, L., Steele, T. E., and Finke, H. (2009). Virtual skeletons: using a structured light scanner to create a 3D faunal comparative collection. *Journal of Archaeological Science*, 36(9):2018–2023.

Noorani, R. (2006). *Rapid Prototyping: Principles and Applications*. Wiley.

Ohbuchi, R., Takahashi, S., Miyazawa, T., and Mukaiyama, A. (2001). Watermarking 3D polygonal meshes in the mesh spectral domain. *Graphics Interface*.

Okubo, M., Yamamoto, Y., and Kamei, S. (1972). Polymer Science. *Polymer*, 1(9):861–865.

Perona, F., Lv, D. L. P., Wudqvihu, W. R., Iurp, G., Wud, D. Q. H., Wr, V., and Ylylg, W. K. H. (2012). SKINNING FUTURE TEXTILES through living material technologies and electronic multi- - sensory experiences. Creative Technologies and Practices.

Rabiee, F. (2004). Focus-group interview and data analysis. In *Proceedings of the Nutrition Society*, pages 655–660.

Reid, E. M. and Merkley, A. R. (2015). Manufacturing control system. US Patent 9,037,282.

Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126.

Robson, S. and Foster, A. (1989). *Qualitative research in action*. Edward Arnold, 1989, illustrated edition.

Røkke, J. M., Muller, G., and Pennotti, M. (2011). Requirement elicitation and validation by prototyping and demonstrators: user interface development in the oil and gas industry. In *Systems Research Forum*, volume 5, pages 89–108. World Scientific.

Ru, X.-M., Zhang, H.-J., and Huang, X. (2005). Steganalysis of audio: attacking the Steghide. In *Proc. Int Machine Learning and Cybernetics Conf*, volume 7, pages 3937–3942.

Sangoi, R. and Smith, C. G. (2005). Printing radio frequency identification (RFID) tag antennas using inks containing silver dispersions. *Journal of dispersion science and technology*, 25(4):513–521.

Schäfer, A., Mara, H., Freudenreich, J., Breuckmann, B., Düffort, C., and Bock, G. (2011). Large scale angkor style reliefs: high definition 3d acquisition and improved visualization using local feature estimation. In *Proceedings of the 39th Conference in Computer Applications and Quantitative Methods in Archaeology*, pages 70–80.

Scopigno, R., Callieri, M., Cignoni, P., Corsini, M., Dellepiane, M., Ponchio, F., and Ranzuglia, G. (2011). 3D Models for Cultural Heritage: Beyond Plain Visualization. *Computer*, 44(7):48–55.

Shaw, M. (2002). What Makes Good Research in Software Engineering ? *International Journal on Software Tools for Technology Transfer (STTT)*, 4(1):1–7.

Simske, S. (2011). Smart Packaging for Security and Logistics. *NIP & Digital Fabrication Conference*, Vol.2011(No 2. Society for Imaging Science and Technology).

Sirringhaus, H., Kawase, T., and Friend, R. H. (2000). High-resolution inkjet printing of all-polymer transistor circuits. *Science*, 290(5499):2123–2126.

Smallwood, R. (2012). *Safeguarding Critical E-Documents: Implementing a Program for Securing Confidential Information Assets*. John Wiley & Sons, Inc., Hoboken, New Jersey.

Smith, L. (2011). Stop online piracy act. *US Government*.

Snyder, R. M. (2014). An overview of the past, present, and future of 3D printing technology with an emphasis on the present. *Association Supporting Computer Users in Education "Our Second Quarter Century of Resource Sharing"*, pages 93–99.

Sterling, B. (2005). *Shaping Things*. MIT Press.

Stevenson, A. (2010). *Security: definition of security in Oxford dictionary (British & World English)*. Oxford University Press.

Stewart, D. and Shamdasani, P. (1990). *Focus Groups: Theory and Practice*. Sage Publications Ltd, London.

Swainson, W. K. (1977). Method, medium and apparatus for producing three-dimensional figure product. US Patent 4,041,476.

Swix, S., Stefanik, J., and Batten, J. (2003). Method and system for providing interactive media VCR control. Patent and Trademark Office.

Thompson, C. (2012). 3d printing's forthcoming legal morass. *www.wired.com*.

Velsen,M. (1997). The Labs: 3DS Specifics. Autodesk Inc.

Walters, P., Huson, D., Parraman, C., and Stanić, M. (2009). 3D printing in colour: technical evaluation and creative applications. In *Proc. Impact Multidisciplinary Printmaking Conference*, number September, pages 16–19, Bristol.

Weinberg, M. (2010). It Will Be Awesome If They Don't Screw It Up. *Public Knowledge*, (November).

Willis, K. and Wilson, A. (2013). InfraStructs: fabricating information inside physical objects for imaging in the terahertz region. *ACM Transactions on Graphics (TOG)*.

Wu, H.-t. and Cheung, Y.-m. (2012). Secure watermarking on 3d geometry via ICA and orthogonal transformation. *Transactions on Data Hiding and Multimedia Security VII*, pages 52–62.

Wynholds, L. (2011). Linking to scientific data: Identity problems of unruly and poorly bounded digital objects. *International Journal of Digital Curation*, 6(1):214–225.

Yampolskiy, M., Yampolskiy, M., Horvath, P., Koutsoukos, X. D., Xue, Y., and Sztipanovits, J. (2013). Taxonomy for description of cross-domain attacks on CPS Taxonomy for Description of Cross-Domain Attacks on CPS. In *Proceedings of the 2nd ACM international conference on High confidence networked systems*, pages 135–142. ACM.

Zhi-ping, Z., Zi-wen, S., Hui, K., and Zhi-Cheng, J. (2007). Steganalysis for Quantization Index Module Hiding Scheme Based on Guassian Distribution. In *Proc. IEEE Int. Conf. Control and Automation ICCA 2007*, pages 1591–1593.