Domain Based Security: Improving Practices

Zia Hayat*
University of Southampton
zia.hayat@baesystems.com

Jeff Reeve
University of Southampton
jsr@ecs.soton.ac.uk

Chris Boutle
BAE SYSTEMS Integrated System Technologies
chris.boutle@baesystems.com

Abstract DBSy (Domain Based Security) is being used more and more for the identification, analysis and documentation of security issues in enterprise CIS (Communication & Information Systems) projects particularly in the military domain. The methodology incorporates numerous security related activities in the early stages of the systems lifecycle to aid in the specification of high-level, technology independent security functionality solutions.

This report focuses on research carried out into improving practices within the DBSy user community with particular emphasis on:

- Applicability and indeed advantages of using DBSy to model: mobile, autonomous and ad-hoc CIS from a business processes perspective
- Ranking risks[1] according to an appropriate value system
- Modeling business connections in an extensible manner

The IFPA (Indirect Fire Precision Attack) and CVF (Future Carrier) projects were used as case studies, in order to identify the extent to which DBSy supports the modelling of the aforementioned concepts. Section 1 introduces the significance of DBSy and the reasons for its use in military enterprise projects such as IFPA & CVF, section 2 then highlights limitations identified in the current specifications of DBSy and how it maybe advantageous to build upon the current specifications. Section 3 discusses solutions proposed in order to overcome the limitations identified in section 2. Section 4 illustrates the usefulness of the proposed solutions in terms of IFPA & CVF with section 5 containing the findings from this research.

Key Words: Autonomous Systems, Business Connections & Ranking Risks

*Sponsored by BAE SYSTEMS Integrated System Technologies, Security Research Group, Frimley, Camberley, Surrey GU16 7EX, UK

[1]The terms risk and compromise path will be used interchangeably throughout this report

1 Introduction

From our experiences of applying DBSy to various infosec projects it has been found to be a highly intuitive and flexible methodology, providing designers and accreditors with the required information to assess security from a cost-benefit point of view. Such cost-benefits assessment may not be directly financial instead relating to user experience and the agility of the processes in place to enable the business and allow it to react effectively to changing circumstances.

Most modern military CIS are procured under increasingly demanding time and cost restrictions. These restrictions combined with requirements to integrate new and existing systems providing NEC (Network Enabled Capability) have exacerbated the need to provision for security from an early stage ideally from the initial feasibility phase. Early consideration of security provides a better understanding of the security issues ultimately providing a more effective solution meeting the requirements with lower associated costs.

Due to its integrated and systematic approach for identifying, analysing and documenting security issues at an early stage DBSy has been used to specify security functionality from a technology independent point-of-view in both IFPA & CVF.

Mobile and autonomous CIS allow flexible and sophisticated modes of operation, which are increasingly necessary for businesses to efficiently, fulfil their requirements. Such systems also introduce ad-hoc communications, which need to be securely managed. Together mobile & autonomous CIS and the ad-hoc communications they utilise present significant security challenges. It is therefore important for DBSy to be able to model such issues if it is to effectively analyse enterprise CIS architectures for military and non-military business.

In order to successfully minimise potential risks it is important to gain an understanding of their severity relevant to one another, DBSy must therefore facilitate such a requirement. Many businesses also require specialised connection types for communications between business processes DBSy must therefore provide an extensible mechanism to model such connections.

2 Perceived Limitations in DBSy Specifications

Due to the relative novelty of DBSy it has not been fully tested through application to real life projects. In our modelling of IFPA we encountered the problem of describing an autonomous system, which is also mobile and requires ad-hoc communications with other physically distributed systems. Current specifications of DBSy do not identify how to model such behaviour.

Although it has been found that DBSy does not explicitly support the modelling of mobile, ad-hoc and autonomous systems, the advantages of providing such techniques have also been investigated. DBSy unlike most other modelling tools illustrates the maximum allowed connectivity between

various business processes. Although the explicit representation of mobile processes and ad-hoc communications would provide a more complete representation of an architecture this cannot be seen to enhance the understanding of security issues. As all processes (static or mobile) and communications (permanent or ad-hoc) must be explicitly defined in a uniform manner, ensuring that the superset of all such processes and their connections are fully specified.

Due to the limited usefulness of explicitly modelling mobile CIS and ad-hoc communications it was decided to concentrate on developing mechanisms for the description of autonomous CIS. However as previously stated no technique within DBSy currently exists to model autonomous systems.

Features from the specifications [4] most closely aligned to modelling autonomous systems are sensors[2], effectors[3] and business domains[4]. A traditional business domain is restricted to representing a logical group of people who may collaborate and share information relatively freely and sensors & effectors do not permit explicit valuation. These limitations mean the current specifications do not satisfy our requirements for modelling autonomous business processes in IFPA, where we have a unique business process of a defined value (protective marking & criticality level) which does not explicitly represent any logical grouping of people, instead autonomously aiming to achieve the dynamic goals of people in business domain(s).

There is currently no specification for the systematic ranking of risks within DBSy. Such an approach would aid in reporting risks in a more meaningful and concise manner thus allowing for resources to be concentrated into those risks perceived to be of greatest threat according to the ranking mechanism. This is particularly significant in larger projects such as CVF, where the security analyst can be swamped by the vast number of potential risks with no sense of their relative significance.

The specific nature of certain projects means the business connections between various processes are not adequately modelled using the standard connection types, which are part of the current DBSy specification. A more generic method for expressing connection types is therefore required this was highlighted in our modelling of IFPA, where we require a messaging connection between an autonomous business process and person(s) with whom it may communicate. This is contrary to the current standard messaging connection type which is defined for communications between people in business domains only.

[2]A sensor is defined as: Connects an environment to a domain, enabling information to be collected from the environment.

[3]Effectors have various definitions depending on its instance for example a printer is described as: Connects a domain to an environment, enabling information to be printed.

[4]A business domain represents the logical places where people work and exchange data by means of software acting on their behalf.

3 Proposed Improvements to DBSy Specifications

The discussions in sections 1 and 2 suggest the concept of autonomy must be addressed, enabling accurate modelling of the envisaged CIS architecture for IFPA, thus providing a valuable insight into the security implications involved. Abstractly an autonomous system can be described as some combination of integrated sensing and effecting capability. Such systems may react to sensed data in a semi-automatic manner, using pre-defined or real-time[5] decision rules upon which to base effecting actions.

The ABD (Autonomous Business Domain) construct has been devised to model autonomous processes in DBSy, its graphical representation is given in figure 1. Its specification can be summarised as: *A logical computing and communication base, which may accumulate, transmit and process data.* An ABD must:

- Be hosted upon an island of infrastructure
- Connect to: environment(s) via sensors and/or effectors and business domain(s) via business connection(s)
- Have a unique identifier within an infosec business model
- Have an appropriate valuation such as protective marking as well as codes and caveats as necessary

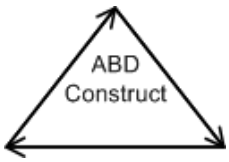

Figure 1: Graphical representation of the ABD business process construct.

Due to the generic nature of its specification the ABD is applicable in a wide range of instances particularly military, due to the increasing number of CIS projects requiring autonomous capability such as guided munitions, unmanned underwater vehicles, smart mines etc. The potentially sensitive nature of the business carried out by ABDs suggests they must be hosted upon island(s) of infrastructure, highlighting the need for well defined and secure points of communication with other processes.

From the specification of an ABD it is proposed to label ABDs with *protective marking* and *codes & caveats*. Therefore ABDs can be analysed as a point of attack (in the compromise step analysis stage) just as any other important business process in DBSy such as conventional business domains. This aids in the identification of risks associated with such processes.

[5]Real-time decisions maybe from a human user operating in business domain(s), e.g. MITL (Man-In-The-Loop)

For example mobile code can give attackers the opportunity to re-configure autonomous processes to react to authorised or un-authorised instructions (e.g. command & control) in malicious or un-intended ways. Potential attacks may vary from the leakage of confidential data to integrity and even denial-of-service.

The compromise path analysis technique currently specified in DBSy to identify potential risks maybe used in conjunction with an appropriate value system to rank risks. An overview of the process proposed to identify and rank risks is given below and summarised in figure 2.

1. Define an infosec architecture model
2. Carry out compromise step analysis on the infosec architecture model
3. Identify compromise paths
4. [6] Carry out HMG IS3 (Her Majesty's Government Infosec Standard 3) connection level calculations for each compromise path identified in step 3
5. List individual compromise paths in order of severity according to HMG IS3 connection levels calculated in step 4

In order to calculate the HMG IS3 connection level for individual compromise paths[7] it is suggested to take into account the difference in protective marking, codes and caveats of both the attacker and victim domains.

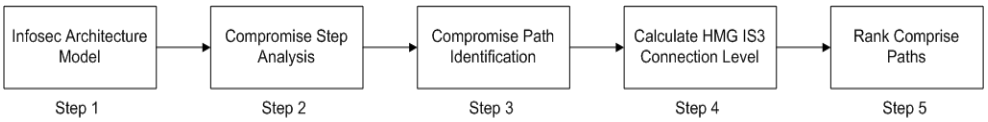

Figure 2: Overview of proposed threat analysis technique.

It is suggested non-standard business connection instances are referenced by a unique identifier, this is illustrated in further detail in section 4. Such an approach would aid in the modelling of non-standard business connections, as well as providing potentially useful security information, due to the sensitivities of specific connection types and the data they transmit.

[6] This step (4) maybe replaced by any valuation scheme of relevance to the project being undertaken, the example given is for UK (United Kingdom) MoD (Ministry of Defence) projects.

[7] Such a path maybe a direct or indirect connection in terms of the infosec business model (developed as part of the infosec architecture model), however this is not relevant in the current context.

4 Application of Improvements

The example infosec architecture model illustrated in figure 3 highlights the use of an ABD with table 1 showing the use of a referencing table to describe non-standard business connections. It can be seen how an ABD may use sensors and effectors as well as other business connections to enable it in carrying out its required business. From table 2 it can be seen how risks can be ranked according to an appropriate value system[8].

The ranking of compromise paths[9] according to their severity is suggested as a suitable risk ranking mechanism. Deriving risks according to a mechanism such as that illustrated in figure 2 would also prove inexpensive, as most of the steps shown are likely to already be carried out in the majority of projects which utilise DBSy.

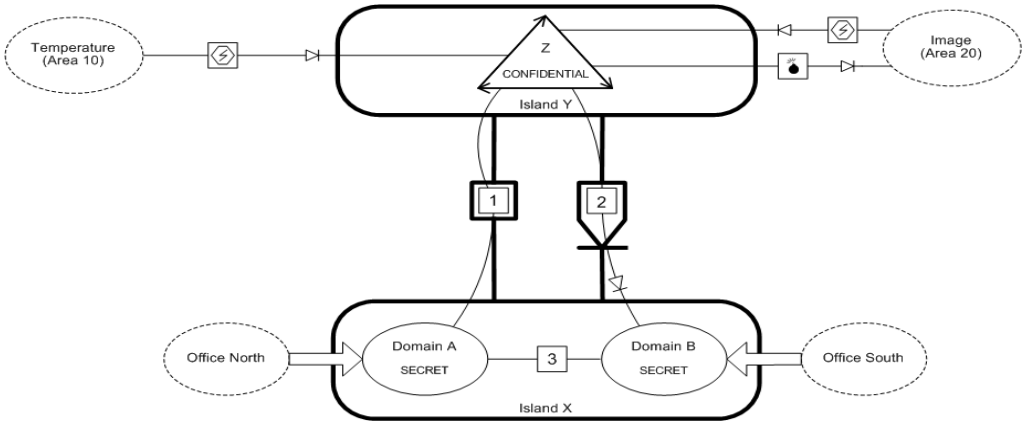

Figure 3: Illustrates the use of the ABD component and referencing of non-standard business connections.

Connection Id	Connection Description
1	Logistics Messaging
2	Imaging & Temperature Information
3	Mission Specific Messaging

Table 1: Defines each non-standard connection for the example infosec architecture in figure 3.

[8]HMG IS3 using only protective markings was used in the example given in table 2.

[9]If a series of compromise steps from a potential attacker to a victim process consist solely of soft security functions this is defined as a compromise path. There are two distinct risk types, which are classified according to the direction of the data flow, these are:

- **Confidentiality** risks whereby data flows from the victim to the attacker process
- **Integrity & Availability** risks whereby data flows from the attacker to the victim process

From a detailed threat analysis carried out using in house software developed previously, three compromise paths have been identified. These paths can also be identified from figure 4. The risks are as follows:

- Attacker:**A** - Victim:**B** (Risk T)
- Attacker:**Z** - Victim:**A** (Risk U)
- Attacker:**B** - Victim:**A** (Risk V)

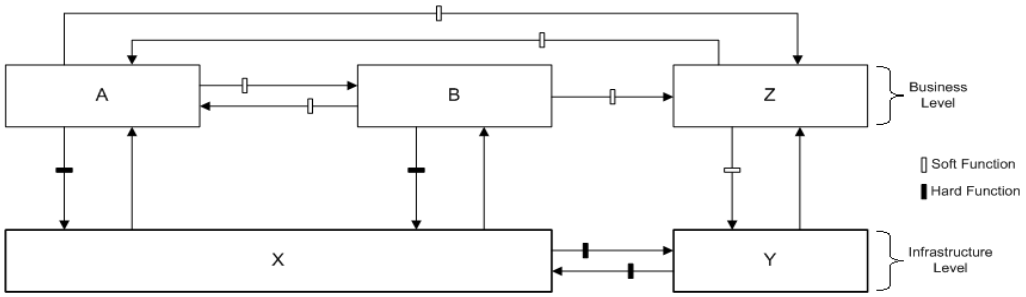

Figure 4: Illustrates the compromise paths of the infosec architecture in figure 3.

It must be noted that an indirect compromise path also exists whereby process **Z** is the attacker and process **B** is the victim via process **A**, however it has not been explicitly identified as the individual risks U and V can be seen to encompass this risk.

Risk	**HMG IS3 Level**	**Ranking**
T	1	2
U	2	1
V	1	=2

Table 2: Ranking of risks for the example infosec architecture in figure 3.

Although the ranking mechanism outlined does not explicitly express the type of risk (i.e. Confidentiality, Integrity or Availability) this can be identified from the compromise step analysis stage.

5 Conclusions

Experience in applying DBSy to the IFPA and CVF projects has shown it to be a flexible and indeed effective methodology for the identification, analysis and documentation of security issues in infosec architectures. However due to its relative novelty as well as its broad appeal it has been shown that individual user communities such as the military will have to adapt the methodology for their needs, building on the fundamental building blocks towards more comprehensive techniques.

The issues of mobile systems and ad-hoc communications have been found to not require specific adaptation as this would add little to the usefulness of the methodology in security terms. However autonomous systems such as those proposed in IFPA have been found to require innovation by the user community in order to leverage the advantages of DBSy.

The ranking of potential risks has been identified as a valuable procedure providing useful information to analysts and developers of systems, for the purposes of concentrating scarce resources according to the potential severity of risks. Such a ranking mechanism would aid in large projects such as CVF particularly where the number of risks are numerous proving difficult to identify the relative severity of risks.

The modelling of specialised business connection types allows for a more intuitive description of the communications between business processes as well as, giving a more comprehensive insight into potential security implications due to the nature of the data in transit. This was highlighted from our work on IFPA where it was necessary to specify business connections currently unavailable in the standard template.

Acknowledgements: Thanks to Richard Elder & Chris Coles for their invaluable contribution, to this piece of work. Martin Field provided useful feedback on the presentation of this paper.

References

[1] M.Z. Hayat, *Domain Based Security Threat-Analysis*, AMS Integrated Systems & University of Southampton, UK, January 2005.

[2] K.J. Hughes, *Domain Based Security: enabling security at the level of applications and business proceses*, QinetiQ, Malvern, UK, 2002.

[3] MoD, *HMG Infosec Standard 3: Connecting Business Domains*, UK, October 2001.

[4] A.P. Page, G.D. Dickin, C.L. Robinson, *Domain Based Security: Abbreviations and Glossary of Terms*, QinetiQ, Malvern, UK, 2003.

[5] C.L. Robinson and K.J. Hughes, *Managing Infosec Risk in Complex Projects*, QinetiQ, Malvern, UK, 2001.

[6] C.L. Robinson, K.J. Hughes, I. Staniforth and S. Wiseman, *Classes of Security Functions for use with an Infosec Architecture Model*, QinetiQ, Malvern, UK, 2003.

[7] S. Wiseman and K.J. Hughes, *Categories of IS3 Functionality to support compromise path analysis*, QinetiQ, Malvern, UK, 2003.