Provisioning Security in A Next Generation Mobility as a Service System

Tope Omitola[1], Ben Waterson[2], Niko Tsakalakis[3], Richard Gomer[1], Sophie Stalla-Bourdillon[4], Tom Cherrett[5] and Gary Wills[1]

[1]*Electronics & Computer Science, University of Southampton, Southampton, UK*

[2]*Maritime & Environmental Engineering, University of Southampton, Southampton, UK*

[3]*School of Law, University of Southampton, Southampton, UK*

[4]*Immuta Inc., USA*

[5]*Transportation Research Group, University of Southampton, Southampton, UK*

t.omitola@ecs.soton.ac.uk, bjw3@soton.ac.uk, nt1n16@soton.ac.uk, r.c.gomer@soton.ac.uk, sstalla-bourdillon@immuta.com, tjc3@soton.ac.uk, gbw@ecs.soton.ac.uk

Keywords: Security, Security Analysis, STRIDE, Next Generation Transportation Systems, Privacy, Mobility as a Service

Abstract: The urban mobility landscape is evolving at an amazing rate, with the number of mobility services growing rapidly around the world. This evolution has brought about the concept of Mobility-as-a-Service (MaaS) in providing transportation services. MaaS capitalises on the Internet of Things to provide access to seamless multi- and inter-modal mobility to the end-user. A well implemented MaaS scheme involves many stakeholders, including passengers, producing, sharing, and consuming (personal) data. In order to encourage MaaS uptake in the general population, participating stakeholders must be confident of the ensuing data privacy and security, as part of their interactions with the system. In this paper, we use STRIDE Threat Modeling framework to analyse the threats that may arise in a MaaS ecosystem. From these threats, we develop mitigations that can be used to eliminate and/or reduce such threats. This threat elicitation and their accompanying mitigations can be used as springboards to establish the necessary security to engender trust in MaaS usage.

1 INTRODUCTION

Mobility affords a range of societal and economic benefits, from access to services and employment to economic development and cultural exchange. But current transport systems suffer from a number of intractable problems, including congestion, emissions of greenhouse gases (GHGs) and local air pollutants, accidents, social isolation and inaccessibility of amenities and services (Rahman and van Grol, 2005). At the same time, urbanisation, a growing population, delayed car ownership, electrification, increasing connectivity, and automation are ushering in a new future in transportation, with disruptive ramifications for many stakeholders, especially operators and regulators, plus new service expectations by citizens. This transformation has enabled the evolution of Mobility-as-a-Service (MaaS) into a concept that promotes the integration of transport services to provide one-stop access through a common interface (Mukhtar-Landgren et al., 2016). MaaS capitalises on Internet of Things technologies (IoT) to provide access to seamless multimodal and intermodal mobility to the end-user. It has the potential to provide an alternative to private car ownership and could contribute to reducing traffic congestion, the impact of climate change and improve access to mobility for aging populations. For these reasons, interest in MaaS is increasing across the world [e.g., (Citymapper,), (Dubai-RTA,)].

In theory, a well implemented MaaS scheme could lead to a reduction in private car usage and improved access to mobility for certain groups of people. Achieving these aims is desirable because they could help solve many of the pressing challenges of modern living, including traffic congestion, poor air quality and public health, concerns about climate change and social isolation, and could help bring together the different MaaS stakeholders.

2 MaaS and Its Stakeholders

Mobility as a Service (MaaS) is the integration of, and access to, different transport services (such as pub-

lic transport, ride-sharing, car-sharing, bike-sharing, scooter-sharing, taxi, car rental, ride-hailing and so on) in one single digital interface suggesting the most suitable solutions based on the user's travel needs (Fidler,). A MaaS system or application will be available anytime offering integrated planning, booking and payment, providing easy mobility and enable life without having to own a car. Figure 1 shows a MaaS exemplar.

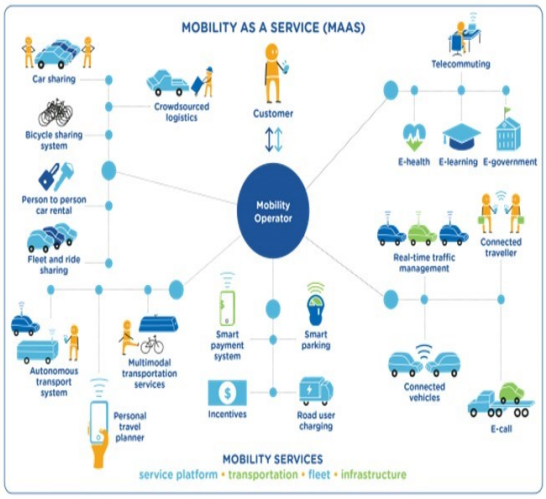

Figure 1: A Mobility as a Service Exemplar (from (Fidler,)).

As Figure 1 intimated, different stakeholders are involved in the operation of a MaaS. A stakeholder is any entity (individual or organisation) to which a piece of data relates or that processes or gets access (legally or not) to a piece of data at any stage of its lifecycle (Le Métayer and Joyee De, 2016). These stakeholders include (Kamargianni and Matyas, 2017):

1. The Customer (or Passenger) who consumes the MaaS offer from the MaaS Provider(s) (and/or Operators)
2. The MaaS Provider, which could either be a public transport authority or a private company
3. Transport Operators, selling their capacity to MaaS providers while enabling access to their data via secure APIs (Application Programming Interfaces)
4. Data Providers. As MaaS relies heavily on data and their interoperability, data providers offer data and analytics capabilities to MaaS providers, processing data of transport operators and collecting data from a range of other sources (i.e. customers' mobile phones, social media etc.)
5. Multiservice Journey Planner Providers. These providers offer multimodal and intermodal journey planning capabilities, enabling passengers to plan their journeys
6. Ticketing and payment solutions providers, offering (advanced) payment and ticketing capabilities for MaaS passengers

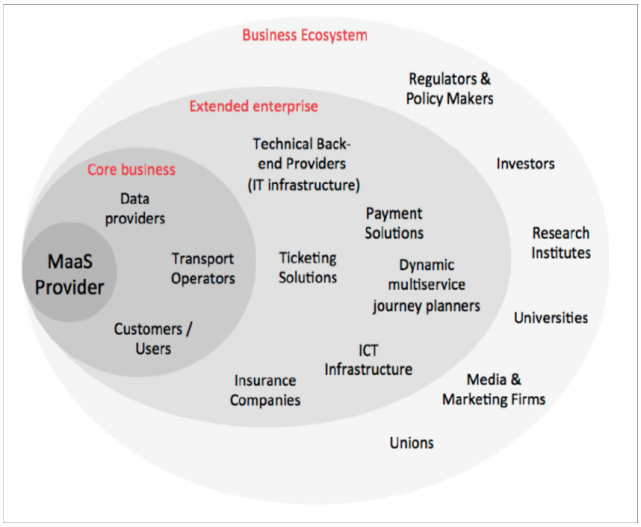

Figure 2: Stakeholders in a Mobility as a Service System (from (Kamargianni and Matyas, 2017)).

Other stakeholders include: Universities and Research Institutes; Unions and Lobby Groups ; Regulators and Policy Makers; Investors; and Insurance companies. Figure 2 shows many of the stakeholders of a MaaS system.

In a MaaS ecosystem, where in order to provide a fully integrated set of transportation services, stakeholder interactions must occur over trust boundaries. A **trust boundary** is an electronic communication or network boundary over which two or more different business entities conduct transactions, and where mutual trust is needed to achieve a friction-free or friction-less execution of these transactions.

But, there is dependence on the security of these business entities (or stakeholders) and over their respective trust boundaries. This dependence, or interdependence, on the security of other actors in the provisioning of transportation services brings with it the notion of risk. The root source of risk is dependence, especially dependence on the expectation of a stable system and a secure state. Dependence is not only individual but mutual, and therefore in order to engender trust amongst the participants of a MaaS ecosystem, we need to assure and ensure the existence of a stable system and secure state in their interactions.

The concerns of stakeholders with regards to se-

curity of interactions with one another, and the trust held of the MaaS system need to be addressed.

3 MaaS, Security, And Trust

As MaaS systems, as exemplars of IoT, have evolved and become refined and effective, end-users continue to delegate important tasks to these technologies. The data and datasets generated and consumed in a typical Maas system can be classified into three broad categories: (1) data pertaining to passengers, e.g. passengers' personal data, (2) data pertaining to the other stakeholders in the system, e.g. transport service providers, and (3) open data. Examples of such data include (Treharne et al., 2017): journey plans, passenger names, passenger location, etc. Data pertaining to the transportation system itself include route and schedule data, vehicles' location data, maintenance, staff and operations data, and companies' financial data.

In a MaaS system, the prementioned data and datasets are being generated, shared and consumed by participating stakeholders. But, when it comes to security and privacy of these datasets, the current forms of IoT technologies, such as an IoT-enabled MaaS system, have changed the nature of the problem. A MaaS system may take information collected and generated for one purpose and re-purpose the same data for a different use, i.e. the data moves from primary to secondary uses. For example, passenger's location data used by the MaaS system for location-aware services, such as available facilities at stations, may be re-purposed for user profiling and targeted marketing purposes. With the re-purposing of datasets from their primary usage to secondary uses, the value of information in these datasets has moved from the primary purpose of why the data was collected to secondary usages. This re-purposing of datasets could undermine the roles assigned to individuals and other stakeholders, in the MaaS ecosystem, thereby affecting, adversely, the security of the entire system.

Therefore, these opaque data cycles in a MaaS environment result in a lack of traceability and security of data flows that may impinge on the data subjects' ability, especially passengers, to make informed decisions about their collected information. This inability to make informed decisions leads to erosion of trust in data subjects while interacting with the MaaS system. A data subject is an identified or identifiable natural person whom the personal data relates to (GDPR,).

Successful deployments and operation of next generation transport systems will require mechanisms for establishing and maintaining trust in the systems' ability to provide adequate privacy and well functioning security of the interactions of the devices, applications and entities running between all the participants of the ecosystem.

With the emergence of IoT, our physical world now melds with the digital, with everyday objects continuing to get connected to the online world through a rapid increase in the deployment of embedded sensors. This brings into view the juxtaposition of security with privacy. There are many examples of (personal) data leaks leading to vulnerabilities and threats in cyber- and physical security. Names and addresses, and other identifying details of the general public are increasingly being stored in various government and commercial databases, where stalkers and rogue employees have been able to find ways to abuse such databases, e.g. (Angwin, 2015) and (Ramer,). Phone companies have started selling mobile phone location data to private enterprise as well as government law enforcement (News,). Our smart phone applications location data are being used by dozens of companies for various purposes (Times,), with no assurance of how securely these datasets are being handled and how vulnerable they are to hacking. "State-sponsored actors" hacking into and stealing consumer data (Perez,). The issue with these data leaks and their juxtaposition to security is three-fold: (a) unauthorised intruders accessing these datasets, (b) the possibly nefarious things that may be done to the people these data refer to, and (c) the unforeseen uses and all the intimate inferences that this volume of data can generate going forward (Burt,), because when data is out there, it is harder to control. Examples like these have made privacy and security to converge (Burt,). The Organisation for Economic Co-operation and Development (OECD) has put their imprimatur on this sensitive topic, by outlining a set of principles to ensure privacy of data subjects. One of such principles is the "Security Safeguards Principle", which said, "Personal data should be protected by **reasonable security safeguards** against such risks as loss or unauthorised access, destruction, use, modification, or disclosure of data." (OECD,).

This points to the salience of security as part of the solution to assuring data protection and privacy of all the stakeholders in a MaaS ecosystem, and to the importance of analysing the security of MaaS systems and applications.

4 Related Work in Security Analysis of MaaS Systems and Applications

There is a vast literature in the security of Intelligent Transportation Systems (ITS) and also of Internet of Things (IoT) of which MaaS is an instantiation of these, and are applicable to it. Callegati et. al. (Callegati et al., 2017) mentioned ITS security threats exploiting vulnerabilities in: (i) network security (threats such as spoofing, sniffing, Denial of Service), (ii) data security (locality, integrity, segregation, authenticity, confidentiality, privacy, access control), (iii) authentication, identity management, sign-on process, and authorisation, (iv) virtualisation vulnerability, and (v) availability. A threat is any circumstance or event with the potential to adversely impact organisational operations and assets, individuals, and/or other organisations, through an information system via unauthorised access, destruction, disclosure, or modification of information, and/or denial of service. Threat events are caused by threat sources. A threat source is characterised as: (i) the intent and method targeted at the exploitation of a vulnerability; or (ii) a situation and method that may accidentally exploit a vulnerability. In general, types of threat sources include: (i) hostile cyber or physical attacks; (ii) human errors of omission or commission; (iii) structural failures of organisation-controlled resources (e.g., hardware, software, environmental controls); and (iv) natural and man-made disasters, accidents, and failures beyond the control of the organisation (Geer and Archer, 2012). A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

In addition to the issues mentioned in (Callegati et al., 2017), there are other security issues pertinent to MaaS. Data exchange and sharing are inherent in the smooth functioning of MaaS, Viggiano et. al. (Viggiano et al., 2020) observed that security risks can be present if data provides special insight into infrastructure and the locations of the people who use transport services which could be used in a physical attack. They also noticed that throughout the data management and sharing processes, there are risks of cyber-attacks that can expose private and personal data. Callegati et. al. (Callegati et al., 2017) observed other types of security vulnerabilities pertaining to MaaS operations. They observed the possibility of the presence of data leakage (which they described as "the accidental distribution of private or sensitive data to unauthorized entities"), the manipulation of service behaviour, manipulation of service workflows, the theft of business intelligence data, and device misbehaviour, through actors exploiting weaknesses in interaction protocols of devices, applications, and services of stakeholders. Many of these vulnerabilities and threats are exploitable by insiders, i.e. by employees of the companies concerned. There are other threats, such as manipulation of service behaviour, manipulation of service workflows, and device misbehaviour that are exploitable by outsiders, possibly through the trust boundaries of the stakeholders. There are various methods of MaaS security analysis.

Traditional security analysis methods, such as **THROP** (Dürrwang et al., 2017), work with threat models that are based on the fault-error-failure chain model. While these models are valid to describe threats to isolated components, they are insufficient to describe system threats in complex interconnected systems, as we have in modern MaaS systems. **OCTAVE** (Alberts et al., 1999) is a risk based strategic assessment and planning technique for security, and mainly used to assess an organisation's information security needs. OCTAVE is best suited for enterprise information security risk assessments, which makes it unsuitable for MaaS security which extends beyond a single enterprise.

Therefore, in this work, we use the **STRIDE** (Shostack, 2014) Threat Modelling framework to analyse the threats that may arise in a MaaS ecosystem. **STRIDE** takes a threat-centric approach to security analysis associating each threat with a particular asset from attackers' perspective. An advantage of STRIDE is that it helps change a designer's focus from the identification of specific attacks to focusing on the end results of possible attacks. A second advantage is it helps to analyse the vulnerabilities that may arise at the interface of trust boundaries of subsystems of an overarching system of systems, such as a MaaS.

5 Security Analysis of a MaaS System

The success of MaaS requires accumulation of significant amounts of data and information, some of which will include information about identifiable individuals, i.e. personal data. And, delivering a seamless travel planning experience to users will also require significant sharing of these data, in real-time, between transport operators and other stakeholders. This section describes how we have used the STRIDE Modelling framework to analyse the threats and vulnerabilities in a MaaS system.

5.1 STRIDE

STRIDE (acronym for **S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of Service, and **E**levation of Privilege) can be divided into the following stages:

- Define usage scenarios
- Create one or more Data Flow Diagrams (DFDs) of the system being analysed
- Determine and Identify Threat and Threat types to the system. These threats are majorly the negation of the main security properties of confidentiality, integrity, availability, authentication, authorization and non-repudiation.
- Plan Mitigation. In this final step, proper countermeasures and defences are introduced for threats and/or threat types

5.2 Motivating Example and Usage Scenario

Figure 2 showed the business ecosystem and the stakeholders that can participate in the fulfilment of transportation services in a MaaS. In our motivating example, we focus on a scenario of a passenger wanting to travel in a city offering both tram and bus transportation services. The passenger uses a MaaS application (MaaS App) as provided by the MaaS provider to book tickets, via a third party(3^{rd}-party) ticketing service, for their journeys that will utilise both tram and buses.

5.3 System Data Flow Diagrams

Figure 3 shows the Data Flow Diagram (DFD) of the system.

The stakeholders in this scenario include:

- Passenger(s)
- The MaaS App (possibly provided and run by the MaaS provider)
- Tram operator(s)
- Bus operator(s)
- The 3^{rd}-party Ticketing and payment service provider

In this work, we have chosen the aforementioned stakeholders, focussing on their relationships in order to highlight the salient security issues involved in a next generation MaaS system.

5.3.1 Service workflow at Trust Boundaries

Some interactions take place at the interfaces between the entities of the ecosystem, and they are:

1. Passenger, using the MaaS App plans to make a journey, and uses the 3^{rd}-party Ticketing and payment service provider to plan either single journeys or multiple journeys, using the 3^{rd}-party ticketing service provider's Journey Planner process
2. The details of these queries are sent to the 3^{rd}-party ticketing service provider's Customer Relationship Management (CRM) process
3. The CRM, after running the queries, returns the journey plans details back to the Passenger
4. If the Passenger is happy with the journey plans, payment is made via the Payment process of the 3^{rd}-party ticketing service provider (4a), and payment acknowledgement is sent to the passenger (4b)
5. Passenger, travelling on the Tram or the Bus, will present their tickets, via the MaaS App, for verification (5a) and verification result(s) sent back (5b)
6. Should the Passenger present multiple or shared journey tickets, these are checked and verified via the Shared Ticketing processes of the transport operators and the 3^{rd}-party ticketing service provider. Also included will be timetable and live service data that will allow the Journey Planner process to function
7. If the Passenger is in possession of Vouchers, these can be redeemed at either the Tram operator or the Bus operator (7a) and result(s) of redemption sent back to passenger (7b)

5.3.2 Service workflow - Internal

The following interactions and data flows occur within each entity:

8. The CRM process stores data into the CRM database (CRM DB)
9. At set intervals, these data are pulled by the Data Aggregator
10. ... into the Aggregated database (Aggregated DB) [the data in this database may be used to perform activites such as quality of service assessments, service level agreements audits, etc.]

Although there are security vulnerabilities and threats in both the internal and external service workflows, it is very beneficial to distinguish between

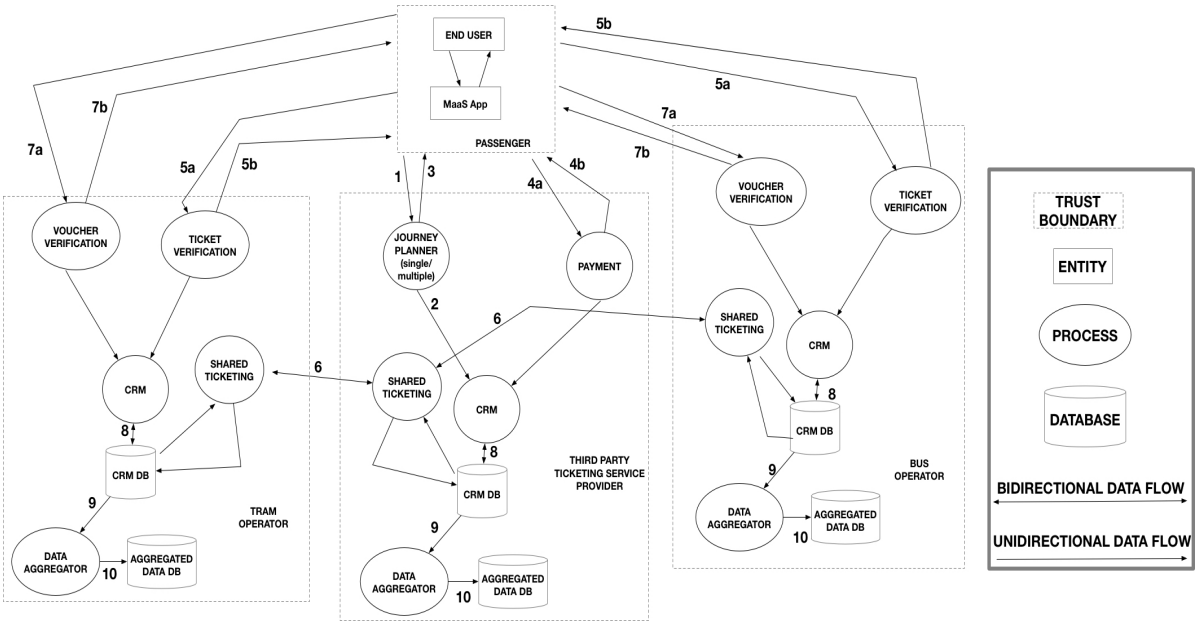

Figure 3: System Data Flow Diagram (labels on data flows are further expanded on in Sections 5.3.1 & 5.3.2)

these two types during security analysis in order to provide the appropriate mitigation mechanisms.

By taking a threat-centric approach to security analysis, STRIDE provides us with the right framework for threats' determination and identification.

5.4 Determination and Identification of Threat (types) to the system

In the determination and identification stage, we use each of the terms in the STRIDE acronym, applying each to the elements of the system's data flow diagram. Each term denotes a security threat which an adversary or attacker can use to gain illegal or unauthorized access to the MaaS system. In order to ensure its security, a MaaS system needs to assure the following properties: authenticity of the principal (or entity) engaged in the interaction, integrity of the data and messages being exchanged, non-repudiation of actions of principals (and entities), confidentiality of messages being exchanged between principals (and entities), availability of services (and processes), and authorization of legitimate principals (or entities) performing valid (or legitimate) actions. The STRIDE threats are the opposite of these aforementioned properties. Tables 1 and 2 show our application of STRIDE to determine and identify threats to the MaaS system.

Once the threats have been identified, the next step is the creative effort of planning mitigations that can be deployed to inhibit or reduce threat occurrence.

5.5 Plan Mitigation

The hardest part of the operations manager's and the system designer's job is usually figuring out what to protect and how, and since people often end up protecting the wrong things, or protecting the right things in the wrong way (Anderson, 2008), determining and identifying threats to the system (as done in Section 5.4) are the corner-stones of developing secure systems (Anderson, 2008).

Table 3 shows some of the mitigation strategies and techniques that can be deployed to mitigate or inhibit the threats enumerated in Tables 1 and 2.

The mitigation plan is divided into the six STRIDE threat categories/types, with each threat type linked to the security property of which it can affect. Then comes the derivation of possible mitigation strategies and techniques that can be deployed to counter the threats.

The identified threats to the MaaS system together with the mitigation strategies and techniques (Table 3) can be used to: (a) understand MaaS system's security requirements, (b) design the system architecture, and (c) by considering security requirements and design early in the engineering process, it dramatically lowers the odds of re-designing, re-factoring, and/or facing a constant stream of security design faults, helping to deliver a more stable and secure secure system.

Table 1: MaaS Threats

Threat -per- (DFD)Element	**Property Violated**	**Threat Examples**
Spoofing The Passenger	Authentication	Pretending to be something or someone other than the passenger, to the MaaS App
Spoofing the Journey Planner process	Authentication; Authorization	Pretending to be something or someone other than the passenger, ∴ can scehdule inappropriate or illegal journeys
Spoofing the Payment process	Authentication; Authorization; Non-repudiation	Pretending to be something or someone other than the passenger; can use the legitimate passenger's payment method to pay for illegal/invalid and valid journeys
Spoofing the Voucher Verification Process	Authentication; Integrity	Attacker pretending to be something or someone other than the passenger, presenting legitimate vouchers of passenger
Spoofing the Ticket Verification process	Authentication; Integrity	Attacker pretending to be something or someone other than the passenger, presenting valid tickets that are not theirs and/or amending ticket information
Spoofing the CRM process	Authentication; Integrity; Confidentiality; Authorization; Non-Repudiation	By spoofing the CRM process, the attacker can change details of vouchers & tickets; they can read information of other processes communicating via the CRM process. By being able to read & edit information, actions can easily be repudiated
Spoofing the Shared Ticketing process	Authentication; Integrity	Attacker can use this opportunity to amend the nature, type, value, and times of shared tickets
Spoofing the Data Aggregator process	Authentication; Integrity; Confidentiality	As the Data Aggregator is responsible for aggregating data of certain profile, Attacker is able to read & amend these information while in transit
Tampering with the CRM process	Integrity	Attacker is able to emend data coming from and/or written to the CRM DB
Tampering with the Data Aggregator process	Integrity	Attacker or legitimate passenger may claim that theor tickets were not released to them after they have made payment
Tampering with the CRM DB	Integrity; Confidentiality	Attacker is able to modify CRM DB
Tampering with the Aggregator Data DB	Confidentiality; Integrity	Attacker is able to modify Aggregator Data DB

Table 2: MaaS Threats (contd)

Threat -per- (DFD)Element	**Property Violated**	**Threat Examples**
Repudiating Payment action	Non-repudiation	Attacker or legitimate passenger may claim that their tickets were not released to them after making payment
Repudiating voucher redemption action	Non-repudiation	Attacker or legitimate passenger may claim they did not redeem voucher(s)
Information Disclosure against payment action	Confidentiality	Attacker is able to read payment message transferred across the network. Attacker may also be able to re-direct traffic as well as execute traffic analysis
Information Disclosure against the Journey Planner process	Confidentiality	Attacker, by being able to read journey planner data flows, is able to discern passenger's itineraries
Information Disclosure against Ticket & Voucher Verification actions	Confidentiality	Attacker may be able to discern passenger's itineraries, and probably other personal data, from ticket & voucher details

6 Conclusion

This paper applied the STRIDE Threat Modelling framework for security analysis of a MaaS. We showed how, by taking a threat-centric approach to security analysis, STRIDE helped us to associate threats and threat types to stakeholder assets from an adversary's perspective. Through this analysis, we were able to identify the threats and vulnerabilities to MaaS security, and to help plan mitigations towards eliminating and/or reducing such threats. Establishing and maintaining privacy and security are salient to engendering trust in a system. By eliciting threats in MaaS and designing mitigations to counter such threats, we showed how MaaS security can be established, helping to increase stakeholder trust in MaaS and next generation transportation systems.

For future work, we will broaden the inclusion of more stakeholders in our security analysis, and as STRIDE is independent of risk assessment techniques, we will explore the application of risk assessment techniques, such as OWASP's (Open Web Application Security Project) Risk Rating Methodology (OWASP,), to prioritise the threats described in this paper.

Table 3: Threats Mitigation Plan

Threat Types	**Linked to Security Losses**	**Possible Mitigation Strategy**	**Possible Mitigation Techniques**
Spoofing	Authentication	Cryptographic / Encryption	HTTPS/SSL, IPSEC
Tampering	Integrity	Cryptographic	HTTPS/SSL, IPSEC, Message Authentication Codes
Repudiation	Non-repudiation	Cryptographic / Logging of actions	Digital Signatures
Information Disclosure	Confidentiality	Cryptographic / Encryption	HTTPS/SSL, IPSEC
Denial of Service	Availability	Flexible with resources, Provision of access control lists	Watch out for exhaustible resources, such as memory, network & cpu resources
Elevation of Privilege	Authorization	Provision of access control lists Logging of actions Cryptographic	HTTPS/SSL, IPSEC

ACKNOWLEDGEMENT

This work has been supported by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity, which has been funded by the UK EPSRC under grant number EP/S035362/1

REFERENCES

Alberts, C., Behrens, S., Pethia, R., and Wilson, W. (1999). Operationally critical threat, asset, and vulnerability evaluation (octave) framework, version 1.0. Technical Report CMU/SEI-99-TR-017, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA.

Anderson, R. J. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley Publishing, 2 edition.

Angwin, J. (2015). *Dragnet nation: A quest for privacy, security, and freedom in a world of relentless surveillance*. Griffin.

Burt, A. Privacy and cybersecurity are converging. here's why that matters for people and for companies.

Callegati, F., Giallorenzo, S., Melis, A., and Prandini, M. (2017). Cloud-of-things meets mobility-as-a-service: An insider threat perspective. *Computers & Security*, 74.

Citymapper. Citymapper pass. https://citymapper.com/pass?en.

Dürrwang, J., Beckers, K., and Kriesten, R. (2017). A lightweight threat analysis approach intertwining safety and security for the automotive domain. pages 305–319.

Dubai-RTA. Smart apps. https://www.rta.ae/wps/portal/rta/ae/home/smart-apps.

Fidler, E. Mobility-as-a-service at the arc smart city forum. https://www.arcweb.com/blog/mobility-service-arc-smart-city-forum.

GDPR. Gdpr article 4 lit. 1.

Geer, D. E. and Archer, J. (2012). Stand your ground. *IEEE Security Privacy*, 10(4):96–96.

Kamargianni, M. and Matyas, M. (2017). The business ecosystem of mobility-as-a-service.

Le Métayer, D. and Joyee De, S. (2016). *Privacy Risk Analysis*, volume 8 of *Synthesis Lectures on Information Security, Privacy, and Trust*. Morgan & Claypool Publishers.

Mukhtar-Landgren, D., Karlsson, M., Koglin, T., Kronsell, A., Lund, E., Sarasini, S., Smith, G., Sochor, J., and Wendle, B. (2016). Institutional conditions for integrated mobility services (ims): Towards a framework for analysis. k2 working papers 2016:16.

News, V. Precision market insights from verizon to help brands better understand and engage with customers. https://www.verizon.com/about/news/vzw/2012/10/pr2012-10-01.

OECD. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Organisation for Economic Co-operation and Development.

OWASP. Owasp risk rating methodology.

Perez, S. Yahoo confirms state-sponsored attacker stole personal data of "at least" 500 million users. https://techcrunch.com/2016/09/22/yahooConfirmsStateSponsoredAttackerStolePersonalData/.

Rahman, A. and van Grol, R. (2005). Sustainable mobility, policy measures and assessment. Technical report.

Ramer, H. Mother of slain woman settles lawsuit against info-broker. http://usatoday30.usatoday.com/tech/news/internetprivacy/2004-03-10-boyer-suit-settled_x.htm.

Shostack, A. (2014). *Threat Modeling: Designing for Security*. Wiley Publishing, 1st edition.

Times, N. Y. Your apps know where you were last night, and they're not keeping it secret. https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

Treharne, H., Wesemeyer, S., Schneider, S., Ross, T., May, A., Cockbill, S., Akram, R. N., Markantonakis, K., Blainey, S., Pritchard, J., and Casey, M. (2017). Personalised rail passenger experience and privacy.

Viggiano, C., Weisbrod, G., Jiang, S., Homstad, E., Chan, M., and Nural, S. (2020). *Data Sharing Guidance for Public Transit Agencies - Now and in the Future*.