Cybersecurity Requirements for Supporting Enterprise Interoperability of Multi-Sided Platforms

Violeta Damjanovic-Behrendt

1 Salzburg Research, Jakob Haringer Str. 5/II, 5020 Salzburg, Austria
violeta.damjanovic@salzburgresearch.at

Abstract. We report on work in capturing cybersecurity requirements for cloud-based and IoT-enabled Multi-Sided Platforms (MSPs). Our approach is designed to capture security aspects related to business rules and constraints of MSPs, thus shaping the platform’s behaviour and the participants interaction and leading towards safer enterprise interoperability. We design the MSPs Privacy Requirements Framework and the MSPs Security Architecture, in order to cater for specific use case-centric and platform-centric cybersecurity requirements. To ensure compliance with the upcoming GDPR, we discuss the mapping between elicited cybersecurity requirements and GDPR rules. The new GDPR regulation is expected to have significant implications on businesses in the EU, and our approach is designed to achieve full compliance with it.

Keywords: Cybersecurity, Platforms, Multi-sided Platforms, Enterprise Interoperability, Privacy, GDPR.

1 Motivation

Enterprise interoperability of Multi-Sided Platforms (MSPs) enables separately developed enterprise systems, which incorporate different business models and domains to effectively share their data, exchange information through negotiation, interact and perform customized business processes, and maximize their efficiency through interworking. MSPs support interaction and interoperability between two or more sides; e.g., a two-sided platform manages the interaction between two distinct groups (e.g., consumers and software providers), while MSPs facilitate the recurring interaction between more than two distinct groups [1]. Some examples of multi-sided platforms are Uber, XBox, eBay, AirBnB, to name a few.

This paper presents our approach to capturing cybersecurity requirements supporting the design and development of the NIMBLE platform’s infrastructure and its services. The NIMBLE platform is designed as an MSP, enabling multi-sided B2B trade and enterprise collaboration. The platform development is funded through the EU H2020 research and innovation programme (for more: https://www.nimble-project.org/).

NIMBLE’s MSP business model involves contractual relationships between buyers and suppliers, as well as logistics and other services affiliated with the platform. De-
signed for cloud environments, the NIMBLE models support a federation of platform instances, each providing a set of core services and offering additional, specifically tailored services enabling interoperation at regional, sectorial, or topical levels. The flexibility of such an MSP increases the complexity of enterprise interoperability and opens issues related to cybersecurity and possible serious harm that can be caused to the participating companies, e.g., revealing sensitive information (personal data, design and operational information) and losing customers, facing a host of legal and financial penalties, putting businesses at risk through cyber jamming communication, spoofing and data manipulations affecting the decision-making process.

**Paper organization.** Section 2 discusses related work on MSPs and platform evolution models, which are used to analyse the overall growth, effectiveness and performances of MSPs in supporting enterprise interoperability. A related work on cybersecurity frameworks and strategies for MSPs is also presented in this section. Section 3 discusses cybersecurity methods used as a baseline to create the MSP Privacy Requirements Framework in NIMBLE. Section 4 describes our approach to cybersecurity requirements elicitation for MSPs, encompassing several aspects targeting enterprise interoperability. For example, we firstly create our MSP Security Architecture, from which we further derive core platform-centric security controls and specify a set of related cybersecurity requirements. Secondly, we map these security controls into the new General Data Privacy Regulation (GDPR) requirements, which will become enforceable in the EU in May 2018. Section 5 concludes the paper.

## 2 Related Work

### 2.1 Multi-Sided Platforms and Their Evolution Models

Enterprise MSPs contribute to frictionless access to markets through the reduction of both search costs and shared transaction costs among multiple participating sides [2]. The direct interaction over MSPs occurs with high frequency between participants affiliated with the same platform. Such frequent interaction expands network effects and fosters an extensive platform adoption. In turn, this positively affects the value of the platform to all affiliated sides [1], while the complexity of economic and technology factors that drive the strategic design of MSPs increases accordingly.

MSPs prove to be systems that evolve gradually over time, and the phenomenon of the platform’s evolution is examined in several platform evolution models:

- Hagiu [2] observes platform evolution as a gradual transition from being one-sided to two-sided and multi-sided platform;
- Evans [3] recognizes the importance of a critical mass of users, which can be achieved by following a zig-zag strategy for attracting new platform participants;
- Tiwana [4] focuses on concrete evolutionary metrics to estimate the speed and effectiveness of a platform’s evolution.

Tiwana’s model is the only model that recognizes the importance of aligning platform architecture, governance and business strategy in order to progress the MSPs. However, the above models do not provide coherent decisions on either architecture or governance and business strategies for MSPs that would practically drive platform
owners and developers. Thus, the authors in [5] design the Reach and Range Framework for MSPs as an analytical tool providing in-depth understanding of MSP’s key mechanisms (such as reach and range), which are used to address the main strategic challenges during platform evolution. In our work, we follow the Tiwana’s model for the design of our security requirements methodology in order to elicit more complete cybersecurity requirements and better support their management and further evaluation.

2.2 Cybersecurity Frameworks and Strategies Affecting Multi-Sided Platforms

Capturing functional and non-functional cybersecurity requirements for MSPs puts a strong emphasis on an early integration of security and privacy with software development, which is ensured through the key concepts of Information Security, as defined in the ISO/IEC 27000:2009 standard [6]. This standard ensures that the information is neither violated nor compromised through possible critical situations, i.e. device malfunctions, threats (software attacks, ransomware, viruses and the like), identity theft, hazards, natural disasters, etc.

In our work, we select several privacy requirements frameworks which are important either because they are influential with regulations or have been designed to provide practical advice for developers:

- The Fair Information Practices (FIP) framework opens a list of privacy elements which are useful to be discussed in the system design phase. The current EU Directive on the Protection of Personal Data (1995) is based on FIP, which brings the following eight principles on personal data [7][8]: Collection Limitation Principle, Data Quality Principle, Purpose Specification Principle, Use Limitation Principle, Security Safeguards Principle, Openness Principle, Individual Participation Principle, and Accountability Principle.

- The Seven Laws of Identity framework improves usable security topics (user-centric privacy) through the definition of seven principles: User Control and Consent, Minimal Disclosure for a Constrained Use, Justifiable Parties, Directed Identity, Pluralism of Operators and Technologies, Human Integration, Consistent Experience Across Contexts.

- The Data Minimization strategy is designed with the aim to reduce privacy risks and provide users with maximum control over their sensitive information [9]. Specific mechanisms can be applied to validate the integrity of algorithms, demonstrate compliant handling of data, prove that data collectors and processors respect privacy policies, etc. The data minimization principles are: Minimize Collections of data in the system; Minimize Disclosure by constraining the flow of information to parties other than the entity to whom the data relates; Minimize Replication of data; Minimize Centralization by avoiding single point of failure in the system, Minimize Linkability of data, and Minimize Retention of data in the system.

- Microsoft Privacy Guidelines for Software Products and Services. Despite recent privacy issues with Windows 10 [10][11], this document offers practical guide-
lines for creating notice and consent experiences, providing sufficient data security, maintaining data integrity, supplying controls for developing software products, etc. One of the core principles in this document is about user’s consent, related to what personal data will be collected, with whom it will be shared, and how it will be used.

- Finally, the new GDPR (see: http://www.eugdpr.org/) is a complex regulation created to enhance personal privacy rights, increase duty for protecting personal data, provide mandatory personal data breach reporting, etc. [12]. The GDPR will become enforceable in May 2018 and will have significant implications on businesses in the EU.

3 Cybersecurity Considerations for Multi-Sided Platforms

Our approach to security and privacy requirements elicitation for the purpose of engineering and delivering secure platform solutions for a variety of MSP’s users (e.g. suppliers, logistic operators, service providers, cloud providers, retailers and platform providers), combines several views on MSPs:

- A platform-centric view resulting in the design of the MSP security architecture and its alignment to the technical NIMBLE platform architecture;
- A use case-centric view resulting in security and privacy control services for MSP’s users;
- A data-centric view that designs and implements data security and privacy services, governance models, and necessary GDPR compliance models.

In our work, we follow the formulation of security as a property to prevent unauthorized access to and modification of information and data, as well as unauthorized use of resources [13], while privacy is seen as a common application of security technologies, with a significant intersection with data provenance that adds security controls for preserving both data integrity and confidentiality [14][15]. Privacy ensures the development of platform services that satisfy user’s requirements related to privacy protection and disclosure of both personal and corporate information.

For the development of privacy preserving mechanisms for MSPs, we combine the FIP framework, the Seven Laws of Identity, the Data Minimization principles and methods for the GDPR implementation as described in [16].

Table 1 presents an excerpt from our work showing the convergence of the proposed privacy frameworks into privacy requirements for MSPs.

| Fair Information Practices | Laws of Identity | Data Min. Principles | GDPR | Conversion into privacy requirements |
|---------------------------|------------------|----------------------|------|-------------------------------------|
| Collection Limitation Principle | User Control and Consent | Implementing privacy procedures for seeking, recording and managing consent | Does the user give consent for the collection and use of his sensitive data? Do we have established privacy methods and tools for seeking, recording and managing consent? |
### Purpose Specification Principle

Documenting all personal and sensitive personal data that the organization holds

*Is the purpose of collecting sensitive data clearly defined? Are personal data and sensitive personal data adequately documented in the system?*

### Individual Participation Principle

Deletion and modification of personal data by the data subject; Privacy procedures for access requests

*Does the user have rights to his sensitive data (e.g. obtaining data from a data controller, having the data erased, rectified, completed or amended, when required)? Is there a way for the user to request access to his data?*

## 3.1 MSPs Privacy Requirements Framework

Table 2 illustrates the proposed MSPs Privacy Requirements Framework, which addresses the three views: user-centric, platform-centric and data-centric view that incorporates a set of GDPR requirements.

| MSP Privacy Requirements Practices | Conversion into privacy requirements |
|-----------------------------------|---------------------------------------|
| **User-centric approach** | | |
| User consent w.r.t. Data Collection | Does the user give consent for the collection and use of his sensitive data? Do we have established privacy methods and tools for seeking, recording and managing consent? |
| User Rights and Controls w.r.t. Data Collection | Does the user have rights to his sensitive data (e.g. obtaining data from a data controller, having the data erased, rectified, completed or amended, when required)? Does the user have control over his sensitive data? Is there a way for the user to request access to his data? |
| **Data-centric approach** | | |
| Purpose Specification | *Is the purpose of collecting sensitive data clearly defined?* |
| Data Quality | Is sensitive data accurate, complete and up-to-date? Is user’s age verified? |
| Minimize Data Collection | *Is the amount of collected data minimal?* |
| Minimize Disclosure | Does the system disclose the least amount of sensitive data and with its limited use? |
| Minimize Replication | *Is the amount of entities where data is stored or processed, minimal?* |
| Minimize Centralization | *Is the number of single point of failure in the system minimal? Is sensitive data minimally centralized in the system?* |
| Minimize Linkability | *Is the amount of linked sensitive data minimal?* |
| Minimize Data Retention | *Is retention of data in the system minimal?* |
| Security Safeguards | Is sensitive data protected? |
| Openness and Interworking of Providers and Technologies | Does open developments, practices and policies respect sensitive data? Does interworking technologies have privacy mechanisms taking into account respect for sensitive data? |
| GDRP Requirements                                      | Are privacy notices updated? Are privacy notices clearly explained? | Are the mechanisms for detecting personal data breaches established? Are the mechanisms for reporting personal data breaches defined? Do we have defined procedures for investigating a personal data breach? | Is the ICO’s code of practice on Privacy Impact Assessment implemented? Are we using another method to assess privacy impact? | Is the guidance from the Article 29 Working Party (EU-GDPR) which is about processing under the authority of the controller or processor implemented? |
|------------------------------------------------------|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Reviewing and keeping up-to-date privacy notices      |                                                                     |                                                                                                                 |                                                                                                                                  |                                                                                                                                  |
| Detecting, reporting and investigating a personal     |                                                                     |                                                                                                                 |                                                                                                                                  |                                                                                                                                  |
| data breach                                          |                                                                     |                                                                                                                 |                                                                                                                                  |                                                                                                                                  |
| Assessing privacy impact                             |                                                                     |                                                                                                                 |                                                                                                                                  |                                                                                                                                  |
| Implementing the guidance from the Article 29 Working|                                                                     |                                                                                                                 |                                                                                                                                  |                                                                                                                                  |
| Party                                                |                                                                     |                                                                                                                 |                                                                                                                                  |                                                                                                                                  |

4 Cybersecurity Requirements Capturing for MSPs

In our work, the process of cybersecurity requirements elicitation for MSPs includes the following steps:

- **Use case-centric security and privacy requirements elicitation**, which is based on requirements collected from platform’s participants;

- **Platform-centric security and privacy requirements elicitation**, which is based on the problem context of the platform’s system, its architecture and design of components and services;

- **Mapping between use case-centric and platform-centric cybersecurity requirements** with the aim to eliminate possible inconsistencies and repetitions between requirements; and

- **Security and privacy requirements evaluation** that is based on STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) threat analysis [19]. STRIDE analyses assets of the platform and its data flows, and identifies possible threats and vulnerabilities that can affect the platform. The threats point to what the attacker can do to harm the platform, while vulnerabilities are weaknesses of the platform that could be easily exploited by the attacker.

Figure 1 illustrates our approach to requirements capturing for MSPs. Firstly, we apply the ISE/IEC 27000 series of Information Security standard for capturing security requirements related to the platform’s participants and their use cases, and to the MSP’s technical architecture and components. In this way, we identify and specify both use case-centric and platform-centric security requirements related to MSPs. For the privacy requirements, we use the MSPs Privacy Requirements Framework (presented in Section 3.1). Secondly, we map the use case- and platform-centric security and privacy requirements in order to eliminate inconsistencies and repetitions between requirements. Finally, we use STRIDE-based methods for the evaluation of security requirements (for more details, see [18]).
The objective of our approach to cybersecurity elicitation is to identify the most important security controls and measures to be implemented and maintained during the MSP’s security lifecycle. In addition, we design an MSPs Security Architecture (see Fig. 2) for the analysis of platform-centric cybersecurity requirements.

4.1 MSPs Security Architecture

MSPs Security Architecture is derived from the NIMBLE Microservice Architecture [17]. Platform-centric security and privacy requirements for each of the identified security controls are elaborated in detail in [18]. The basic security controls have been addressed by the following core components:

- **The FrontEnd component** is designed to ensure an easy-to-use interaction with the users, and to handle authentication, load balancing and related security controls ensuring that only authenticated users can access the platform’s services and data. Security monitoring methods must be in control of provenance data, revealing information about the platform’s connection parameters.

- **The Open API component** implements access control management, authorization methods, and security monitoring applications for monitoring unauthorized attempts to invoke an API.

- **The Data Store and Data Management components** ensure various security methods for protecting against front-end threats, log threats, tampering, ensuring data integrity and preventing information disclosure.

- **Core Services, Service Registry and Service Discovery components** include security controls for protecting Product Catalogues against unauthorized access and distribution, SQL injection attack against Product Catalogues, etc.

- **Core Security and Privacy controls** implement Identity Management, Access Control Management, Authorization and Authentication, Data Provenance Man-
agement, Trust and Reputation Management, and Data Integrity and Data Quality Management.

Fig. 2. MSPs Security Architecture.

4.2 Security Controls for Data Integrity and Data Quality Management, and their Mapping with the GDPR

A failure to control the distribution of data, data integrity and data quality often leads to data breaches, loss of sensitive information and data manipulation, which need to be prevented using adequate security controls, e.g. only authenticated users can access data in a controlled manner. Data manipulation related to MSPs enables comparison of products and suppliers, filtering and ordering information in a way that forces unfair trade and monopolies.

Provenance information about access to the system needs to be kept in audit logs, while security controls for anomaly detection are performed to capture unusual behaviour. Provenance information matters in cybersecurity as a measure for preventing data manipulation that can cause harmful changes of product specifications (e.g. power outages, data sabotage, etc.). The secure exchange of business information through file sharing, email and messaging system for negotiation, is another big concern for platform participants interacting over MSPs.

To demonstrate mapping compliance of the MSPs Security Architecture and its security controls with the GDPR requirements, in Table 3, we discuss security controls supporting Data Integrity and Data Quality Management (more details are given in [18]).
Table 3. Security controls supporting Data Integrity and Data Quality Management.

| Security control name                | Security control description and its compliance with the GDPR                                                                 |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Data Integrity and Data Quality Policy | Data Integrity and Data Quality Policy must be clearly defined and based on the MSPs Privacy Requirements Framework (in order to incorporate different approaches: use-case-centric view, data-centric view and the GDPR requirements). |
| Data input validation                 | Controls over various factors: predictable behaviour, manual override, timing, etc. must be integrated, which corresponds to the Data Quality Principle and the GDPR requirement for verifying sensitive data for its accuracy, completeness and for being up-to-date. |
| Data and metadata protection          | Protection against unauthorized access and manipulation; Automated restricted access; Cryptographic protection; GDPR requirement for deletion of personal data and/or personal data modification by the data subject; GDPR requirement for supporting subject’s requests to access personal data; |
| Data protection at rest               | Cryptographic protection, off-line storage; GDPR requirement for deletion and/or modification of personal data by the data subject; |
| Data protection in shared resources   | Cryptographic protection; GDPR requirement for deletion of personal data and/or personal data modification by the data subject; |
| Notification of data integrity violations | Monitoring services must be provided; GDPR requirement for detecting, reporting and investigating personal data breaches; GDPR requirement for reviewing existing privacy notices and keeping them up-to-date |
| Informed consent by Design            | User must have an informed consent on the data usage, which prevents the use of data in a way that is not according to the user wish; GDPR requirement for implementing privacy procedures for seeking, recording, and managing user’s consent |

5 Conclusion

The ultimate role of MSPs in digital automation is to increase speed to market, minimize costs and optimize manufacturing and logistic processes through enterprise interoperability. The overall growth, effectiveness and performances of MSPs can be analyzed using the platform’s evolution models. We consider the Tiwana’s platform evolution model, which aligns the architecture of MSPs, governance and business strategies to further progress evolution of MSPs, as an approach that can be extended towards cybersecurity. Therefore, in this paper we the MSPs Privacy Requirements Framework and its specific MSPs Security Architecture featuring security controls that are specifically designed to ensure compliance with the GDPR. In that way, the role of the MSPs can be seen as a “regulatory role”, which shapes enterprise interaction and online behaviour, and which is expected to lead towards safer enterprise interoperability.
References

1. Hagiu, A., Wright, J.: Multi-sided platforms. Harvard Business School, Boston, MA Working Paper 12-024 (2011).
2. Hagiu, A., Wright, J.: Multi-sided platforms: from microfoundations to design and expansion strategies. Harvard Business School, Boston, MA Working Paper 09-115 (2008).
3. Evans, D.S.: How catalysts ignite: the economics of platform-based start-ups. In A Platform, Markets and Innovation (A. Gawer, Ed.). Cheltenham and Northampton, US: Edward Elgar, pp. 99-130 (2009).
4. Tiwana, A.: Platform ecosystems, aligning architecture, governance, and strategy. Amsterdam: Morgan Kaufmann, 2014.
5. Staykova, K., Damsgaard, J.: Adoption of mobile payment platforms: managing reach and range. J. of theoretical and applied electronic commerce research. ISSN 0718-1876 (2016).
6. ISO/IEC 27000:2009 (E). Information technology - Security techniques - Information security management systems - Overview and vocabulary. ISO/IEC. (2009).
7. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980). Online: http://bit.ly/2xfYFv3 Last access: September 2017
8. World Privacy Forum. A Brief Introduction to Fair Information Practices. (2008) Online: http://bit.ly/2xmslsb Last access: September 2017
9. Gürses, S., Tronsoco, C., Diaz, C.: Engineering Privacy by Design. COSIC 2011. (2011). Online: https://www.esat.kuleuven.be/cosic/publications/article-2589.pdf
10. Warren, T.: Microsoft finally reveals what data Windows 10 really collects. (2017). Online available from: http://bit.ly/2EJRrC2 Last access: October 2017.
11. Boomi, D.: How Windows 10 data collection trades privacy for security. (2017) Online: http://bit.ly/2gQyhAK Last access: October 2017
12. Microsoft whitepaper. Beginning your General Data Protection Regulations (GDPR) Journey for Windows 10. (2017). Online available: http://bit.ly/2iRu1p2
13. Amin, M.: Formal Methods for Information Security (1993) Online:http://bit.ly/2mxvb6Y
14. Martin, A., Lyle, J., Namilkuo, C.: Provenance as a Security Control. In Proceedings of the 4th USENIX Conference on Theory and Practice of Provenance, USA. (2012)
15. Sultana, S., Bertino, E., Shehab, M.: A provenance based mechanism to identify malicious packet dropping adversaries in sensor networks. In CDCSW 2011, pp. 332–338 (2011).
16. Overview of the GDPR. (2017). Online: http://bit.ly/29lxF0U
17. Innerbichler, J., Gonul, S., Damjanovic-Behrendt, V., Mandler, B., Strohmaier, F.: NIMBLE Collaboration Platform: Microservice Architectural Approach to Federated IoT, In Proceedings of the 1st Global IoT Summit 2017 (GloTS17), Switzerland (2017).
18. NIMBLE D6.1: Security and Privacy Requirements. Project Deliverable. (2017) (to appear: https://www.nimble-project.org/deliverables/)
19. A. Shostack (2014). Threat Modelling. Designing for Security. John Wiley & Sons, Inc.