Towards a Framework for Designing Secure Mobile Enterprise Applications

Basel Hasan
Department of Computing Science
Oldenburg University
Oldenburg, Germany
basel.hasan@uni-oldenburg.de

Jorge Marx Gómez
Department of Computing Science
Oldenburg University
Oldenburg, Germany
jorge.marx.gomez@uni-oldenburg.de

Joachim Kurzhöfer
AS Inpro GmbH
Lufthansa Systems
Oldenburg, Germany
joachim.kurzhoefer@lhsystems.com

Abstract— **Mobile devices like smartphones and tablets are not only designed for private use, but also for business use as well. Mobile solutions, such as mobile enterprise resource planning and mobile business intelligence, are nowadays becoming more common. However, without strong consideration of security, especially in mobile devices, these solutions would be very risky. Enterprise data are classified in security levels, in which security threats and countermeasures are grouped. These levels indicate the fulfillment degree of the security objectives in each group. From the enterprise point of view, the boundaries between these levels concerning the mobile devices are not clear. In this research, risk analysis with focus on mobile devices is conducted and a framework to design secure Mobile Enterprise Applications (MEAs) is developed. This framework supports developers in the decision making process when designing secure MEAs side by side with promoting the trustworthy usage of mobile devices in business sectors.**

Keywords: Enterprise Mobility; MEAs; Security; Risk Analysis; User Acceptance.

I. INTRODUCTION

Mobile technologies and applications have been greatly improved in the recent few years making the ubiquitous communications a growing reality [1, 2]. It comes to the enterprise mobility concept when the enterprise integrates mobile technologies into its existing IT infrastructure besides giving its employees better possibilities to work on the move effectively [3]. Nowadays, the talk is about MEAs (e.g., Mobility for SAP, which enables mobile access to SAP® CRM, SAP® ERP and various SAP® Workflows via smartphones and tablets [4]).

MEAs are characterized according to A. Giessmann et al. [5] as: "[…] applications that are designed for and are operated on mobile devices and which facilitate business users within core and/or support processes of their enterprises". They are classified into five categories: mobile broadcast, mobile information, mobile transaction, mobile operation, and mobile collaboration applications [6]. Mobile broadcast category facilitates large-scale information broadcast, such as advertisement and promotions. Mobile information category provides information requested by the mobile user, such as job vacancies and timetables. Mobile transaction category eases and executes transactions, such as e-transactions and the transactions of Customer Relationship Management (CRM). Mobile operation category covers internal operational aspects of the business, such as inventory management and Supply Chain Management (SCM). Finally, mobile collaboration category supports collaboration among employees and various functional units. The proposed framework takes these five aforementioned categories into consideration.

Mobility gives enterprises many advantages. It enables the ubiquitous real-time access to critical business information which supports the managers to meet strategic decisions in shorter time to satisfy their customers' need [3, 7]. Consequently, mobility increases worker productivity and reduces business operation costs [7]. Due to these advantages, enterprises demand mobility and flexibility of their workers as inevitable success factors [8]. However, the involvement of mobile technologies and applications has also brought new security challenges and risks, particularly on mobile devices.

In this paper, the most relevant definition of information security is taken from the ISO/IEC 17799 standard that defined it as follows: "Information security is the protection of information from a wide range of threat in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities" [9]. Although mobile devices face a wide range of potential security threats [8, 10, 11], mobile applications are developed often without implementing proper security measures [2]. The major security threats related to mobile environments include, but are not limited to: device loss/theft, data interception and tampering, malware, vulnerable applications, compromised devices, mobile operation system vulnerability, and social engineering. Some of these threats are similar to those in a traditional desktop environment. However, the more prominent threats in mobile environments are malware, data interception and tampering, and device loss or theft [2]. Due to the small size and high portability of mobile devices, they can easily get lost or stolen [12]. According to McAfee report, 40% of the surveyed companies had mobile devices lost or stolen and half of these lost/stolen devices contained critical business data [13]. Consequently, unauthorized third parties can make use of these critical data [8]. Moreover, the disclosure of such kind of data might have harmful consequences on enterprise like financial loss or even the loss of its reputation [10, 14].

Integrating mobile devices into enterprises means that sensitive business data could be accessed everywhere and anytime using mobile devices. Conforming to Bring-Your-Own-Device (BYOD) trend [15], where mobile workers use their personal mobile devices, critical and sensitive business information might be located on these personal devices. The

 ISBN: 978-1-61208-313-1

more sensitive the data are the higher security level is required. In general, to achieve a certain level of security, appropriate countermeasures must be applied and that might restrict the use of mobile devices. Therefore, mobile workers have to accept all the restrictions on their own devices. As a result, mobile security solutions must hold a balance between the private and business use.

The key concern in MEAs is the mobile application security including information confidentiality, integrity, and availability. This comes from the issue that communications via mobile networks, in which security threats can take place anywhere, are more vulnerable to be attacked than wired networks [6]. Kelton Research had shown that 75% of 250 surveyed companies, which their revenues are up to $100M across the United States and United Kingdom, considered security the major factor that prevents companies from adopting mobile applications [7].

The research in this paper focusses on security issues in mobile environments with emphasis on MEAs. It represents a work in progress to discuss and investigate new ways towards building a framework for secure MEAs. The rest of this paper is structured as follows: Section II presents the research problem. Then, the adopted research process is presented in Section III. Section IV proposes and presents the details of the secure mobile enterprise applications design framework. Related work is then presented in Section V. Finally, the paper sums up with a conclusion and future work in Section VI.

II. PROBLEM DEFINITION

Mobile devices are exposed to a wide range of threats that have to be countered. The vital point in this regard is finding and applying appropriate security countermeasures. According to T. Wright et al. [16]: due to the significant resource constrains of the mobile devices, many security countermeasures from traditional computing domains are not translated well to mobile devices. In other words, simply porting standard information security tools from stationary computers, notebooks, and server domains to mobile devices is unlikely to be effective [16–18]. In order to achieve a certain level of security, the mobile user has to accept some restrictions on the features and functions supported by mobile devices. Examples for such restrictions are: specifying exactly which applications are permitted to be installed, or restricting the types of connections that a third-party application can establish. The employee, who wants to access very critical information using mobile devices, might accept a wide range of limitations. However, these limitations might be not accepted in the case that the employee doesn't need to access this critical information. Generally, a high level of security might be reached on mobile devices by setting a high level of restrictions. On the other hand, this might minimize user acceptance and satisfaction factors. Thus, there is an opposition between security and usability. A balance between them should be carefully taken into account [19]. Achieving a balance between smart phone effective security countermeasures and employee acceptance is a serious dilemma for CIOs and security professionals [17].

Another important issue to be considered in this context is the types of enterprise data. They are normally classified into private or public data. The importance of private data can be defined by the level of security attached to it [20]. Particularly, with regard to the use of MEAs, experts agree that the boundaries between security levels are not clear in the business sectors. Based on the aforementioned security-related problems, the research behind this paper tries to answer the following research questions:

- To what extent can MEAs be protected?
- Which security level can be applied?
- Which security countermeasures can achieve the applied security levels?
- Which data, under which conditions, can enterprises transfer to mobile devices?
- What are the accompanied consequences or restrictions?
- Will these consequences be accepted by the mobile users?

The following section gives a short overview of the research process followed by this work and briefly explains the main outcomes behind the conducted research.

III. RESEARCH PROCESS

This work follows the Information Systems Research Framework that is based on seven guidelines provided by A. Hevner et al. [21]. The work began with the business needs, to define the problem and to ensure that this research meets the goal of relevance. This is achieved by the discussion with the experts in the German Lufthansa systems company. The discussion revealed that enterprises need to execute business processes remotely from the mobile devices in a known level of security. The research relies on existing knowledge base within two main fields namely information security and enterprise mobility. The suitable use of this knowledge ensures the rigor of the research. The expected artifact of this research is a generic framework that helps developers to design secure MEAs. Based on that, this research mainly aims at coming up with a framework to guide developers in designing secure mobile applications. The whole process encompasses conducting risk analysis in the mobile environments and classifying MEAs in security levels considering the user acceptance of the consequences arising in each level. Eventually, using this framework will make the boundaries between these levels as clear as possible. This framework is considered as the artifact behind the conducted research. To evaluate this artifact, it will be firstly implemented as a proof of concept. After that, the resulted prototype will be evaluated descriptively by constructing detailed scenarios around the artifact to demonstrate its utility.

IV. FRAMEWORK TO DESIGN SECURE MOBILE ENTERPRISE APPLICATIONS

To answer the abovementioned research-related questions, risk analysis has been conducted to determine the potential mobile security threats and the applicable security countermeasures which overcome them. As a method to analyze the risks, assessment methodology provided by G. Stoneburner et al. [22] is employed, taking into consideration

 ISBN: 978-1-61208-313-1

the following three standards: ISO/IEC 27005 [23], BSI-Standard 100-3 [24] and Risk Management Guide for Information Technology Systems [22]. In the proposed framework, each threat defines a mobile security issue that might be overcome by applying one or more security countermeasures called "alternatives". The security issues and their alternatives are determined based on literature and best practices. The alternatives define a set of reusable decisions made in previous projects that concern mobile application development. The proposed framework is developed based on Service-Oriented Architecture Decision Modeling (SOAD) framework [25], which aims at enhancing the SOA's architectural style. To reuse the structure of SOAD framework in security and enterprise mobility domains, adaptations have to be made to come up with a new framework, which introduces a security knowledge base to support developers in designing the Security Concept (SC) of MEAs.

A. Structure Overview

The structure consists of three models namely: the guidance model, the decision model and the meta-model. This structure is depicted in Fig. 1. The framework's meta-model is instantiated into two models: the guidance model to identify required decisions and the decision model to log the decision that had been made [25]. The relations between these two models are the tailoring and harvesting decision log. These relations are considered similar to those used in the SOAD framework. On the one hand, the tailoring relation initiates the creation of the decision model. This relation represents an activity in which the developer of a MEA selects the relevant security threats and its alternatives (security countermeasures) to build a decision model that forms the security concept of MEA. On the other hand, the harvesting decision log relation is about feeding information regarding the decision (or result) made in the decision model back to the guidance model to get it refined in the next version.

B. The Guidance Model

As illustrated in Fig. 1, this model contains a list of security issues that are already identified during the risk analysis process. A security issue informs the developer that a particular security threat exists and a decision is needed. Each threat is accompanied with its likelihood of occurrence and harm consequences on the enterprise. According to G. Stoneburner et al. [22], three likelihood levels: high, medium, and low are defined based on the threat-source motivation and capability, nature of the vulnerability besides the existence and effectiveness of current security countermeasures. Each security issue has a reference to one or more alternatives along with their consequences on the mobile user and known uses in the previous mobile applications. The mobile user acceptance of those consequences is a very important factor to be considered during MEAs design. Evidently, it is insufficient to use a strong technical solution that enhances the security when such solution doesn't satisfy the user. User acceptance scale can take one of these five values: strongly accepted, accepted, neutral, rejected, and strongly rejected. This model is enhanced with a security evaluation method to classify MEAs in security levels as well.

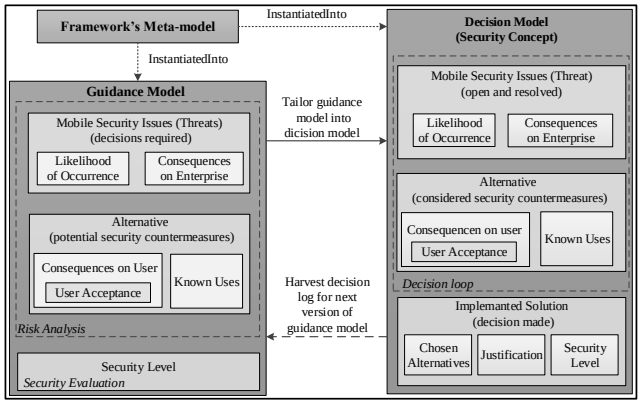

Figure 1. Structure Overview of the proposed Framework (adapted from O. Zimmermann [25])

C. The Decision Model

The decision model is created in a tailoring step, which might involve deleting irrelevant security issues, adding new issues and enhancing relevant ones. After selecting the relevant security threats and one alternative for each threat, the MEAs is evaluated and classified into a specific security level. If the resulted security level does not meet the security requirements, other alternatives can be selected. Therefore, a decision loop is enabled to select other alternatives. Ending the loop means that the decision has been made. This decision (the lower right corner of Fig. 1) contains the chosen alternatives along with justification and security level. After tailoring the guidance model into a decision model, the decision model can feed information about the made decision (result) back to the guidance model in a formal or informal lessons-learned review. The new mobile security issues, which were not considered in the guidance model, besides the enhanced ones could be harvested and integrated back to the guidance model to improve it in the next version.

D. The Meta-model

The meta-model of the proposed framework is shown in Fig. 2 as a UML class diagram. The determined threats during risk analysis are described in the entity Threat and classified into ThreatGroup. Each threat is solved by one or more alternatives which are described in the entity Alternative.

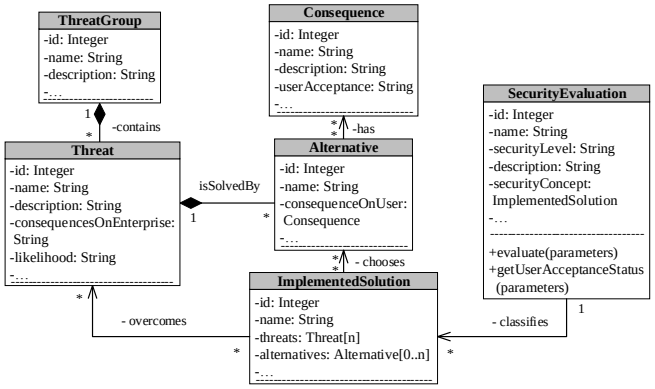

Figure 2. The Framework's Meta-model

The consequences caused by the alternatives and their user acceptance are described in two entities namely: Consequences and UserAcceptance respectively. The selected threats and their chosen alternative are grouped in the ImplementedSolution entity which represents the security concept of the MEA. At the end, this security concept is classified into security levels provided in SecurityLevel entity.

V. RELATED WORK

Based on an adapted version of SOAD framework, a guidance model to architect secure mobile applications has been created [12]. This model supports decision making process and covers security-related architectural issues during architecting mobile applications. However, in that work, risk analysis is not conducted and the research behind this paper considered such analysis as a vital prerequisite to address and understand all security issues in the mobile environment. A framework to develop MEAs has been presented in [6] to offer a systematic solution for the development and maintenance of mobile application, but it has just highlighted the security as a major concern for the enterprise in developing mobile application without providing more in-depth analysis about it. With regard to security knowledge in the field of software engineering, security patterns are often essential. Security patterns are basically built from best practices and help to solve recurring security problems. However, security patterns don't support developers in making a proper design decision even if the available patterns can cover all security-related issues [26]. This work addresses such challenge by providing more concrete details about each security-related aspect so that the developers will always have enough arguments to make a proper design decision while designing their secure MEAs.

VI. CONCLUSION AND FUTURE WORK

This paper presented the ways towards building a generic framework to design secure MEAs. Insights to the internal structure of the framework and its building models had been detailed as well. This framework is supposed to provide enterprises and MEAs developers with a security knowledge base needed to comprehend the mobile security issues and their accompanied challenges. Furthermore, this framework will help developers in making proper decisions and keeping a balance between mobile security solutions and user acceptance. Such comprehension tries to make the mobile security issues and challenges as transparent as possible to promote the trustworthy use of mobile technologies in business sectors. The study will be furthered to provide a fully-fledged framework with step-by-step guidelines to show how it works. As a proof of concept, a prototype will be implemented to show the practicability of the overall concept.

REFERENCES

[1] R. Basole and W. Rouse, "Mobile Enterprise Readiness and Transformation," Idea Group Inc. IGI, 2006.

[2] A. Jain and D. Shanbhag, "Addressing Security and Privacy Risks in Mobile Applications," IT Professional, 2012, pp. 28–33.

[3] J. Ranjan and V. Bhatnagar, "A holistic framework for mCRM – data mining perspective," Information Management & Computer Security, 2009, pp. 151–165.

[4] ISEC7 - Mobility for SAP - Mobile SAP. Available: http://www.isec7.com/en/products/mobile-sap, [retrieved: Sep, 2013].

[5] A. Giessmann, K. Stanoevska Slabeva, and B. de Visser, "Mobile Enterprise Applications--Current State and Future Directions," 45th Hawaii International Conference on System Science (HICSS), 2012, pp. 1363–1372.

[6] B. Unhelkar and S. Murugesan, "The Enterprise Mobile Applications Development Framework," IT Professional, 2010, pp. 33-39.

[7] H. Hurley, E. Lai, and L. Piquet, Enterprise mobility guide 2011. Sybase, 2011.

[8] K. Detken, G. Diederich, and S. Heuser, "Sichere Plattform zur Smartphone-Anbindung auf Basis von TNC," D.A.CH Security 2011: Bestandsaufnahme, Konzepte, Anwendungen und Perspektiven; syssec Verlag; Oldenburg, 2011.

[9] ISO/IEC 17799, Information technology - Security techniques - Code of practice for information security management. ISO/IEC, 2005.

[10] W. Copeland and C. C. Chiang, "Securing Enterprise Mobile Information," Computer, Consumer and Control (IS3C). IEEE, 2012, pp. 80–83.

[11] L. Qing and G. Clark, "Mobile Security: A Look Ahead," Security & Privacy. IEEE, 2013, pp. 78–81.

[12] W. Schwittek, A. Diermann, and S. Eicker, "A Guidance Model for Architecting Secure Mobile Applications," in 4th International ICST Conference on Security and Privacy in Mobile Information and Communication Systems, Springer, 2012, pp.12-23.

[13] R. Power, "Mobility and Security: Dazzling Opportunities, Profound Challenges". Available: http://www.mcafee.com/us/resources/reports/rp-cylab-mobile-security.pdf, [retrieved: Sep, 2013].

[14] BSI, BSI-Standard 100-1: Information Security Management Systems (ISMS). Available: https://www.bsi.bund.de/, [retrieved: Sep, 2013].

[15] P. Rubens, "4 Steps to Securing Mobile Devices and Apps in the Workplace". Available: http://www.esecurityplanet.com/mobile-security/4-steps-to-securing-mobile-devices-and-apps-in-the-workplace-mdm-byod.html, [retrieved: Sep, 2013].

[16] T. Wright and C. Poellabauer, "Improved Mobile Device Security through Privacy Risk Assessment and Visualization," Data Engineering Workshops (ICDEW), IEEE 28th International Conference on, 2012, pp. 255–258.

[17] M. Landman, "Managing smart phone security risks," Information Security Curriculum Development Conference, ACM, 2010, pp. 145-155.

[18] J. Oberheide and F. Jahanian, "When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments," Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications. ACM, 2010, pp. 43-48.

[19] N. Daswani, C. Kern, and A. Kesavan, Foundations of security: What every programmer needs to know. Apress, 2007.

[20] A. Tsolkas and K. Schmidt, Rollen und Berechtigungskonzepte: Ansätze für das Identity- und Access-Management im Unternehmen, 1st ed. Wiesbaden: Vieweg + Teubner, 2010.

[21] A. Hevner, S. March, J. Park, and S. Ram, "Design science in information systems research," MIS Quarterly, 2004, pp. 75-105.

[22] G. Stoneburner, A. Goguen, and A. Feringa, "SP 800-30. Risk Management Guide for Information Technology Systems." Technical Report, NIST, 2002.

[23] S. Klipper, "ISO/IEC 27005," Information Security Risk Management. Vieweg+Teubner, 2011, pp. 63–97.

[24] BSI, BSI-Standard 100-3: Risk analysis based on IT-Grundschutz. Available: https://www.bsi.bund.de/, [retrieved: Sep, 2013].

[25] O. Zimmermann, "Architectural Decisions as Reusable Design Assets," IEEE Software, 2011, pp. 64–69.

[26] M. Schumacher, Security engineering with patterns: Origins, theoretical models, and new applications. Springer, 2003.

 ISBN: 978-1-61208-313-1