CARL VON OSSIETZKY universität OLDENBURG

Fakultät II - Informatik, Wirtschafts- und Rechtswissenschaften

Oldenburger Schriften zur Wirtschaftsinformatik
Hrsg.: Prof. Dr.-Ing. Jorge Marx Gómez

Basel Hasan

A Conceptual Framework for Mobile Security Supporting Enterprises in Adopting Mobility

Abteilung Wirtschaftsinformatik
Carl von Ossietzky Universität Oldenburg

CARL VON OSSIETZKY universität OLDENBURG

Carl von Ossietzky Universität Oldenburg

Fakultät II – Informatik, Wirtschafts- und Rechtswissenschaften
Department für Informatik

A Conceptual Framework for Mobile Security Supporting Enterprises in Adopting Mobility

Dissertation

Submitted in fulfillment of the requirements for the degree of

Doktors der Ingenieurwissenschaften (Dr.-Ing.)

Submitted by

M.Sc. Basel Hasan

Supervisors:

Prof. Dr.-Ing. Jorge Marx Gómez

Prof. Dr. Hermann Strack

Disputation Date: 15.05.2019

Oldenburg, Germany

Oldenburger Schriften zur Wirtschaftsinformatik

Band 26

Basel Hasan

A Conceptual Framework for Mobile Security Supporting Enterprises in Adopting Mobility

Shaker Verlag
Düren 2019

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Zugl.: Oldenburg, Univ., Diss., 2019

Printed in Germany.

ISBN 978-3-8440-6799-6
ISSN 1863-8627

Shaker Verlag GmbH • Am Langen Graben 15a • 52353 Düren
Phone: 0049/2421/99011-0 • Telefax: 0049/2421/99011-9
Internet: www.shaker.de • e-mail: info@shaker.de

Acknowledgements

This dissertation would not have been possible without the support I always received from my first supervisor Prof. Dr.-Ing. Jorge Marx Gómez, who always gave me invaluable comments, advices and suggestions regarding the content as well as regarding the formal structure of this thesis. I am also thankful for my second supervisor Prof. Dr. Hermann Strack. Through him, I received lot of comments that enriched the thesis. I would also like to thank Dr. Joachim Kurzhöfer for the interesting discussion sessions at LHIND. He was always available for me during the last years. My gratitude extends also to the PhD examination committee members Prof. Dr.-Ing. Jürgen Sauer and Dr.-Ing. Sven Rosinger. Thanks also go to my colleagues at the VLBA department. It has been a pleasure to work with them and to supervise students doing their bachelors' and masters' theses.

Special thanks go to Tishreen University for funding my study by a scholarship for master and PhD. Here, I would also like to thank Dr. Nasser Nasser for giving me the support I was highly needed.

I am grateful to my parents and to my sisters for their encouragement and support within whole my life. They always believed in me, which has helped me to get where I am now. I am waiting with highest patience to see you soon!

I am grateful to my beautiful family, my wife Ola and my children Zeinab and Karam. I will never forget your invaluable support and endless love you are giving to me. I am waiting with highest patience to see you soon!

To the strong persons who gave their souls to save my home, Syria. Without you, we would not have been able to protect our home. You made the history and I will be always telling about your heroic victories. My brother **Alaa**, I miss you in everything, you remain inside my heart and I will never forget you, Rest in Peace.

Thanks God for everything.

Basel Hasan

Oldenburg, May 2019

Zusammenfassung

Heutzutage fordern Unternehmen die Mobilität und Flexibilität ihrer Mitarbeiter als unerlässliche Erfolgsfaktoren ein. Die Integration von mobilen Endgeräten, wie Smartphones und Tablets, gibt den Mitarbeitern der Unternehmen die Möglichkeit, produktiver zu arbeiten. Diese Integration birgt allerdings auch neue Sicherheitsherausforderungen und Risiken. Trotz aller Vorteile dieser Mobilität scheuen viele Unternehmen diese Umsetzung, da sie ihre Sicherheitsrisiken nicht einschätzen können. Mobile Endgeräte sind einer Vielzahl von Bedrohungen ausgesetzt, denen begegnet werden muss. Eine einfache Portierung der Informationssicherheitsstandards von Workstations, Notebooks und Serverdomänen auf mobile Endgeräte ist jedoch nicht wirkungsvoll. Aus Unternehmenssicht sind die Schutzstufen auf mobilen Endgeräten daher nicht eindeutig. Einerseits kann eine hohe Schutzstufe auf mobilen Endgeräten durch ein hohes Maß an Einschränkungen erreicht werden. Andererseits kann dies die Akzeptanz und Zufriedenheit der Nutzer minimieren.

Um die oben genannten Probleme anzusprechen, wird ein konzeptionelles Framework vorgeschlagen, welches Unternehmen bei der Einführung von mobilen Unternehmensapplikationen unterstützt. Es wird eine Risikoanalyse mit Fokus auf mobile Endgeräte durchgeführt. Bei der Risikoanalyse werden potenzielle Sicherheitsbedrohungen sowie deren Eintrittswahrscheinlichkeit und Auswirkungen auf das Unternehmen ermittelt und in einer Liste zusammengefasst. Jede Sicherheitsbedrohung wird einer oder mehreren Sicherheitsmaßnahmen und deren Konsequenzen für mobile Benutzer zugeordnet. Darüber hinaus wird das vorgeschlagene Framework mit einer Sicherheitsüberprüfungsmethode unterstützt, die überprüft, ob das Sicherheitskonzept einer mobilen Unternehmensapplikation den Sicherheitsanforderungen entspricht, welche zum Erreichen einer vordefinierten Schutzstufe erforderlich sind.

Diese Forschung soll Unternehmen hauptsächlich bei der Entscheidungsfindung bei dem Design von mobilen Unternehmensapplikationen unterstützen und ihnen helfen, Problembereiche der mobilen Sicherheit zu verstehen. Somit bietet das vorgeschlagene Framework ein Konzept für den Wissenstransfer im Bereich der Sicherheit, um das Sicherheitswissen von Sicherheitsexperten auf Nicht-Sicherheitsexperten zu übertragen. Darüber hinaus fördert die durch das Framework geschaffene Sicherheitstransparenz die vertrauenswürdige Nutzung von mobilen Endgeräten im Geschäftsbereich. Das

Framework wird unter Berücksichtigung seinen Leitfäden entwickelt und mit einem Metamodell angereichert, welches seine Komponenten und ihre Beziehungen beschreibt. Schließlich wird das Framework (das Artefakt) deskriptiv durch detaillierte Szenarien evaluiert, um seine Nutzbarkeit zu demonstrieren.

Abstract

Nowadays enterprises demand mobility and flexibility of their employees as inevitable success factors. Integrating mobile devices, namely smartphones and tablets, into the enterprise gives the employees the ability to work more productively. However, this integration has also brought new security challenges and risks. Despite all the advantages of mobility, many enterprises continue to be doubtful about it due to security concerns. Mobile devices are exposed to wide range of threats that have to be countered. Simply porting information security standards from workstations, notebooks, and server domains to mobile devices is unlikely to be effective. Thus, from an enterprise point of view, security levels are unclear on mobile devices. Generally, a high level of security might be attained on mobile devices by setting a high level of restrictions. On the other hand, this might minimize user acceptance and satisfaction factors.

To address the issues mentioned above, a conceptual framework that supports enterprises in adopting Mobile Enterprise Applications (MEAs) is proposed. A risk analysis with focus on mobile devices is conducted. During risk analysis, potential security threats are determined and assembled in a list, along with their likelihood of occurrence and harm impact on business. Each security threat is mapped to one or more security measures along with their consequences for mobile users. Furthermore, the proposed framework is enriched with a security check method, which checks if the security concept of MEA meets the security requirements needed to achieve a predefined security level.

This research is mainly intended to support enterprises in a decision-making process when designing MEAs and will help them to understand mobile security issues and classify the MEAs into security levels. Thus, the proposed framework provides a security knowledge transfer concept to transfer security knowledge from security experts to non-security experts. Moreover, the security transparency provided by the proposed framework promotes trustworthy usage of mobile devices in the business sector. The framework is developed along with its guidelines and enhanced with a meta-model that describes its components and their relations. Finally, the framework (the artifact) is evaluated descriptively by constructing detailed scenarios around it to demonstrate its utility.

Table of Contents

List of Abbreviations IX
List of Figures XIII
List of Tables XV
1 Introduction 1
1.1 Motivation 2
1.2 Problem Definition 5
1.3 Thesis Objectives 8
1.4 Thesis Structure 9
2 Background and Related Concepts 11
2.1 Mobile Technologies 11
2.1.1 Mobile Devices 11
2.1.2 Mobile Infrastructure 13
2.1.3 Mobile Operating Systems 14
2.2 Enterprise Mobility 16
2.2.1 Mobile Business Applications 16
2.2.2 Strategic Management and Mobile Strategies 19
2.2.3 IT Security in Enterprises 21
2.2.4 Information Security Standards and Catalogues 22
2.2.5 Mobile Security 24
2.2.6 Enterprise Mobility Management 28
2.3 Knowledge Management 33
2.3.1 Knowledge Classifications 33
2.3.2 Knowledge Conversion Modes 34
2.3.3 Knowledge Transfer 35
2.4 Summary 36
3 Research Methodology 37
3.1 Information Systems Research Framework 37
3.2 Employing Design Science in Research 39
3.3 Employing Behavioral Science in Research 44
3.4 Literature Review 44
3.4.1 Guidelines for Literature Review 45
3.5 Summary 47
4 Conception of Framework for Adopting Secure Mobile Enterprise Applications 48
4.1 Methodology 48
4.2 Framework Structure 50
4.2.1 Framework Meta-Model 52
4.2.2 Framework Guidance Model 52
4.2.3 Framework Decision Model 54
4.3 Framework Workflow and Guidelines 54
4.4 Requirement Definition 59

4.4.1 General Requirements 59
4.4.2 Functional Requirements 60
4.4.3 Non-functional Requirements 63
4.5 Framework User: Role Definition 64
4.6 Concept of Security Knowledge Transfer 65
4.7 Summary 67
5 Framework Data Structure 69
5.1 Risk Catalogue for Mobile Enterprise Applications 69
5.1.1 Overview 69
5.1.2 Mobile Business Scenarios 70
5.1.2.1 Mobile Customer Relationship Management 71
5.1.2.2 Other Use Cases for Mobile Enterprise Applications 72
5.1.3 Assets in Relevance to Mobile Enterprise Applications 73
5.1.4 Risk Catalogue Structure 76
5.1.5 Risk Estimation 77
5.1.6 Threats Categorization and Overview 78
5.1.6.1 Mobile Device Category 78
5.1.6.2 Mobile Applications Category 80
5.1.6.3 Mobile Operating System Category 82
5.1.6.4 Wireless Networks Category 85
5.1.6.5 Mobile User Category 87
5.1.7 Summary 89
5.2 Mobile Security Measures 90
5.2.1 Mobile Security Measures and their Consequences for Mobile Users 90
5.2.1.1 Authentication 91
5.2.1.2 Encryption 93
5.2.1.3 Containerization 97
5.2.1.4 Protection Software 99
5.2.1.5 Other Security Measures 99
5.2.2 Proposed Model for User Acceptance of Mobile Security Measures 103
5.2.2.1 Overview 103
5.2.2.2 Methodology 105
5.2.2.3 Proposed User Acceptance Model 107
5.2.2.4 Discussion 108
5.2.3 Summary 108
5.3 Security Levels for Mobile Enterprise Applications 109
5.3.1 Mobile Security Requirements 109
5.3.2 Security Level Definition 113
5.3.3 Summary 122
6 Prototypical Implementation and Evaluation 123
6.1 General Overview of the Prototypical Implementation 123
6.1.1 UML Class Diagram of CFMS Meta-Model 125
6.1.2 Main CFMS Interactions 127

6.1.3 Database Model of CFMS 129
6.2 CFMS Demonstration 130
6.2.1 CFMS Guidance Model 133
6.2.2 CFMS Decision Model 136
6.3 Evaluation 137
6.3.1 Functional Testing and Conducted Workshops 137
6.3.2 Business Scenarios from Praxis 140
6.3.3 Utilization of CFMS in Smart Cities Applications 143
6.3.3.1 Privacy Concerns in Smart Cities Applications 144
6.3.3.2 Problem Definition 146
6.3.3.3 Possible Utilization of CFMS in Smart Cities 147
6.4 Summary 150
7 Conclusion and Outlook 151
7.1 Research Summary 151
7.2 Outlook and Future Work 153
References 155
Publications 175
Appendix A 176
Appendix B 182
Appendix C 184
Appendix D 186

List of Abbreviations

4G	Fourth Generation
AES	Advanced Encryption Standard
AJAX	Asynchronous JavaScript and XML
API	Application Programming Interface
AWC	Application-Wrapping Container
B2C	Business-to-Customer
B2E	Business-to-Employee
BI	Business Intelligence
BSI	Bundesamts für Sicherheit in der Informationstechnik
BYOD	Bring Your Own Device
CC	Common Criteria
CEMIS	Corporate Environmental Management Information Systems
CFMS	Conceptual Framework for Mobile Security
CIA	Confidentiality, Integrity and Availability
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and Related Technologies
COBO	Corporate Owned, Business Only
COPE	Company Owned, Personally Enabled
CPU	Central Processing Unit
CRM	Customer Relationship Management
CSS	Cascading Style Sheets
CYOD	Choose Your Own Device
DDoS	Distributed Denial of Service
DNS	Domain Name System
DOM	Document Object Model
DoS	Denial of Service
EDGE	Enhanced Data Rates for GSM Evolution
EED	Enterprise-Enabled Device
EFS	Enterprise File Sharing
EMM	Enterprise Mobility Management
ENISA	European Union Agency for Network and Information Security
ERP	Enterprise Resource Planning

ESC	Encrypted Space Container
FAR	False Acceptance Rate
FDE	Full Disk Encryption
FIBS	Federal Information Processing Standards
FRR	False Rejection Rate
GDPR	General Data Protection Regulation
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
HR	Human Resource
HSDPA	High Speed Downlink Packet Access
HTML	Hypertext Markup Language
IDC	International Data Corporation
IDE	Integrated Development Environment
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IMAP	Internet Message Access Protocol
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
iOS	iPhone Operating System
IoT	Internet of Things
IP	Internet Protocol
IS	Information Systems
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Standards Organization
IT	Information Technology
ITU	Intention to Use
KM	Knowledge Management
LTE	Long Term Evolution
MAM	Mobile Application Management
MANET	Mobile Adhoc Network
MCM	Mobile Content Management
MDM	Mobile Device Management

MEA	Mobile Enterprise Application
MitM	Man-in-the-Middle
MMS	Multimedia Messaging Service
MNOs	Mobile Network Operators
MSM	Mobile Security Management
MSP	Mobile Service Provider
MTM	Mobile Trusted Module
MVC	Model-View-Controller
MVP	Mobile Virtualization Platform
NFC	Near-Field Communication
NGOs	Non-Governmental Organizations
NIST	National Institute of Standards and Technology
OHA	Open Handset Alliance
ORM	Object-Relational Mapping
OS	Operating System
OWASP	Open Web Application Security Project
PC	Personal Computer
PCI DSS	Payment Card Industry Data Security Standards
PDA	Personal Digital Assistant
PDCA	Plan-Do-Check-Act
PDF	Portable Document Format
PEOU	Perceived Ease of Use
PIM	Personal Information Manager
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
POP	Post Office Protocol
PR	Perceived Restriction
PU	Perceived Usefulness
QR	Quick Response
RAM	Random Access Memory
RIM	Research In Motion
SD	Secure Digital
SECI	Socialization, Externalization, Combination and Internalization
SIM	Subscriber Identity Module
SMS	Short Message Service

SOAD	Service-Oriented Architecture Decision Modeling
SPs	Special Publications
SPSS	Statistical Package for the Social Sciences
SQL	Structured Query Language
SSL	Secure Sockets Layer
TAM	Technology Acceptance Model
TCG	Trusted Computing Group
TLS	Transport Layer Security
TPM	Trusted Platform Module
UI	User Interface
UML	Unified Modeling Language
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
USB	Universal Serial Bus
UX	User Experience
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
XML	Extensible Markup Language

List of Figures

Figure 1. Security professionals' biggest sources of concern related to cyber attacks 4
Figure 2. User satisfaction and security.....6
Figure 3. Thesis structure 9
Figure 4. Main mobile technologies 11
Figure 5. Mobile device communication mechanisms 13
Figure 6. Classification of apps in business 17
Figure 7. Types of strategies.....19
Figure 8. Factors that affect the adoption of MEAs 26
Figure 9. EMM overview 29
Figure 10. SECI model 34
Figure 11. Information systems research framework 38
Figure 12. Design science research process model 42
Figure 13. Framework for literature review 45
Figure 14. Risk management process 49
Figure 15. CFMS structure 51
Figure 16. Workflow of the CFMS 56
Figure 17. UML use case diagram of the guidance model.....62
Figure 18. UML use case diagram of the decision model 63
Figure 19. Concept of security knowledge transfer within CFMS.....65
Figure 20. Mobile enterprise infrastructure.....71
Figure 21. Android version market share distribution among smartphone owners as of September, 2016 84
Figure 22. Share of Apple devices by iOS version worldwide in 2016 84
Figure 23. Abstract encryption model 95
Figure 24. App sandboxing. 98
Figure 25. Original technology acceptance model 104
Figure 26. Mobile devices' usage for work.....106
Figure 27. Proposed user acceptance model.....107
Figure 28. Multi-dimensional view of security levels.....116
Figure 29. CFMS meta-model as UML class diagram.....125
Figure 30. Main interactions to create a new project 128
Figure 31. Main interactions to refine the guidance model.....129
Figure 32. Database relational model of the CFMS 130
Figure 33. CFMS home page.....131
Figure 34. CFMS login screen.....131

Figure 35. Main page after logging as security expert 132
Figure 36. Main page after logging as non-security expert 132
Figure 37. Main page after logging as security expert 133
Figure 38. CFMS versions administration.....134
Figure 39. Management of guidance model versions.....134
Figure 40. Screenshot of administrating the content of the guidance model 135
Figure 41. Project list in the decision model 136
Figure 42. CFMS decision model – create a new project.....141
Figure 43. CFMS decision model – choosing a security level 141
Figure 44. CFMS decision model – presenting the security requirements.....142
Figure 45. CFMS decision model – overview on the project being created 143
Figure 46. Need of communications between public and private sectors 147
Figure 47. CFMS as communication interface between public and private sectors.....148

List of Tables

Table 1. Worldwide smartphone OS market share (share in unit shipments) 15
Table 2. MEA examples 18
Table 3. Most work-related information security standards and publications 22
Table 4. Smartphone secure development guidelines 27
Table 5. MDM functions 30
Table 6. MAM functions 31
Table 7. MCM functions 31
Table 8. MSM functions 32
Table 9. Design-science research guidelines 39
Table 10. Outputs of design science research 43
Table 11. Taxonomy of literature reviews 46
Table 12. CFMS guidance model's version types 62
Table 13. CFMS roles definition 65
Table 14. Excerpt of the results of the Statista's survey 66
Table 15. Potential assets associated to the usage of MEAs 74
Table 16. Risk catalogue structure 76
Table 17. Risk levels estimation matrix 77
Table 18. Adverse impact estimation matrix 78
Table 19. Potential consequences of applying mobile security measures and restrictions 103
Table 20. Internal consistency for the investigated factors 106
Table 21. Correlations between the constructs 107
Table 22. Interviewed enterprises 109
Table 23. Security requirements related to mobile communications 110
Table 24. Security requirements related to mobile OS 112
Table 25. Security requirements related to mobile applications 113
Table 26. Potential impact definitions for security objectives 114
Table 27. Possible definition of security levels 117
Table 28. Examples of personal information with assigned protection level 118
Table 29. Access matrix of an MEA regarding the possible access of personal data 119
Table 30. Security levels considering the legal dimension – an example 119
Table 31. Mapping security levels to security requirements 122
Table 32. Used software products for CFMS prototype 124