Mobile Platform Security

Synthesis Lectures on Information Security, Privacy, & Trust

The Synthesis Lectures Series on Information Security, Privacy, and Trust publishes 50- to 100-page publications on topics pertaining to all aspects of the theory and practice of Information Security, Privacy, and Trust. The scope largely follows the purview of premier computer security research journals such as ACM Transactions on Information and System Security, IEEE Transactions on Dependable and Secure Computing and Journal of Cryptology, and premier research conferences, such as ACM CCS, ACM SACMAT, ACM AsiaCCS, ACM CODASPY, IEEE Security and Privacy, IEEE Computer Security Foundations, ACSAC, ESORICS, Crypto, EuroCrypt and AsiaCrypt. In addition to the research topics typically covered in such journals and conferences, the series also solicits lectures on legal, policy, social, business, and economic issues addressed to a technical audience of scientists and engineers. Lectures on significant industry developments by leading practitioners are also solicited.

Privacy for Location-based Services
Gabriel Ghinita
2013

Enhancing Information Security and Privacy by Combining Biometrics with Cryptography
Sanjay G. Kanade, Dijana Petrovska-Delacrétaz, and Bernadette Dorizzi
2012

Analysis Techniques for Information Security
Anupam Datta, Somesh Jha, Ninghui Li, David Melski, and Thomas Reps
2010

Operating System Security
Trent Jaeger
2008

Mobile Platform Security

N. Asokan, Lucas Davi, Alexandra Dmitrienko, Stephan Heuser, Kari Kostiainen, Elena Reshetova, and Ahmad-Reza Sadeghi

ISBN: 978-3-031-01213-6 paperback
ISBN: 978-3-031-02341-5 ebook

DOI 10.1007/978-3-031-02341-5

A Publication in the Springer series
SYNTHESIS LECTURES ON INFORMATION SECURITY, PRIVACY, & TRUST

Lecture #9
Series Editors: Elisa Bertino, *Purdue University*
Ravi Sandhu, *University of Texas, San Antonio*
Series ISSN
Synthesis Lectures on Information Security, Privacy, & Trust
Print 1945-9742 Electronic 1945-9750

Mobile Platform Security

N. Asokan
Aalto University and University of Helsinki, Finland

Lucas Davi
Intel Collaborative Research Institute for Secure Computing at TU Darmstadt, Germany

Alexandra Dmitrienko
Fraunhofer Institute for Secure Information Technology, Germany

Stephan Heuser
Intel Collaborative Research Institute for Secure Computing at TU Darmstadt, Germany

Kari Kostiainen
ETH Zurich, Switzerland

Elena Reshetova
Intel Open Source Technology Center, Finland

Ahmad-Reza Sadeghi
TU Darmstadt, Germany

SYNTHESIS LECTURES ON INFORMATION SECURITY, PRIVACY, & TRUST #9

ABSTRACT

Recently, mobile security has garnered considerable interest in both the research community and industry due to the popularity of smartphones. The current smartphone platforms are open systems that allow application development, also for malicious parties. To protect the mobile device, its user, and other mobile ecosystem stakeholders such as network operators, application execution is controlled by a platform security architecture. This book explores how such mobile platform security architectures work. We present a generic model for mobile platform security architectures: the model illustrates commonly used security mechanisms and techniques in mobile devices and allows a systematic comparison of different platforms. We analyze several mobile platforms using the model. In addition, this book explains hardware-security mechanisms typically present in a mobile device. We also discuss enterprise security extensions for mobile platforms and survey recent research in the area of mobile platform security. The objective of this book is to provide a comprehensive overview of the current status of mobile platform security for students, researchers, and practitioners.

KEYWORDS

mobile devices, platform security architectures, operating system security, hardware security

Contents

Preface

Personal mobile devices only started appearing outside the laboratory in the early 1990s. In the span of two decades, they have gone from curiosities used by the technically savvy to a mass-market that is fast reaching saturation. Mobile security research caught the attention of the academic research community only during the last decade, when smartphones and mobile applications and services became widely available. However, mobile security as a discipline dates back to the beginning of the mobile communication era in the early 1990s. Today there exists a large body of literature on mobile security and privacy investigating various threats to the existing smartphone platforms and proposing solutions at different levels of system abstraction (hardware, middleware, OS, and applications).

The work that led to this book began three years ago. All of us (authors of this book) were already engaging in active research in mobile platform security, in academia as well as in industry. This book began as an attempt to put the sudden spurt of academic research in mobile security into context, by explaining how and why mobile platform security became so widely deployed. An early version was presented in keynotes at the ACM CODASPY 2011 and at ESORICS 2012. The very positive feedback we received at both conferences, as well as on many other academic and industry related occasions where we presented the work, convinced us that both the research community and practitioners of mobile security would benefit from an expanded, systematic treatment of mobile platform security. This book is the result.

This book consists of three parts. In the first part (Chapters 2–5), we build up a general model for software platform security. We then use the model to conduct a comparative analysis of several representative mobile platform security architectures. We also use the model to derive hardware security requirements and use them to describe widely deployed hardware security architectures. In the second part (Chapter 6) we focus on security extensions targeted for enterprise scenarios. In the third part (Chapter 7), we survey recent research.

We intend this book to be useful to students, active researchers, and practitioners such as application developers. We hope that this book serves as an introduction to mobile platform security for application developers and students, giving them an understanding of the design rationales behind platform security features with which they might already be familiar. Researchers beginning their research on mobile platform security can use the book to familiarize themselves with the state-of-the-art in practice and research.

We are grateful for the valuable feedback from Sini Ruohomaa, Claudio Marforio, and Nikolaos Karapanos on previous drafts of this book. We thank our reviewers, Bilal Shebaro and Aditi Gupta, for carefully reading the final draft. Their feedback led to several improvements in

this version. We thank Prof. Elisa Bertino for inviting us to write the book and Diane Cerra for her gentle reminders to keep us to our schedule.

N. Asokan, Lucas Davi, Alexandra Dmitrienko, Stephan Heuser, Kari Kostiainen, Elena Reshetova, and Ahmad-Reza Sadeghi
December 2013