T-Labs Series in Telecommunication Services

More information about this series at http://www.springer.com/series/10013

Michael Roland

Security Issues in Mobile NFC Devices

Springer

Michael Roland
School of
Informatics/Communications/Media
University of Applied Sciences
Upper Austria
Hagenberg
Austria

ISSN 2192-2810 ISSN 2192-2829 (electronic)
T-Labs Series in Telecommunication Services
ISBN 978-3-319-15487-9 ISBN 978-3-319-15488-6 (eBook)
DOI 10.1007/978-3-319-15488-6

Library of Congress Control Number: 2015930733

Springer Cham Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media (www.springer.com)

Preface

The recent emergence of Near Field Communication (NFC)-enabled smartphones led to an increasing interest in NFC technology and its applications by equipment manufacturers, service providers, developers, and end-users. Nevertheless, frequent media reports about security and privacy issues of electronic passports, contactless credit cards, asset tracking systems, NFC-enabled mobile phones, and proprietary contactless technologies suggest that NFC is a potentially unsafe technology whose main beneficiaries are thieves. While these weaknesses are often bound to specific applications and products, they boost the fear that NFC technology as a whole is dangerous, threatens our privacy, and helps identity theft and fraud. In order to defend their own products and services, manufacturers and service providers often position themselves on the opposite extreme, stating that their products and services incorporate sufficient countermeasures.

This book is a revised version of my Ph.D. thesis. It is written for researchers, engineers, and students interested in security aspects of mobile devices and Near Field Communication. This book contains the results of my research conducted between late 2009 and early 2013 at the NFC Research Lab Hagenberg (a research group at the University of Applied Sciences Upper Austria) in close cooperation with the Department of Computational Perception at the Johannes Kepler University Linz.

My research aims for assessing the actual state of NFC security, for discovering new attack scenarios, and for providing concepts and solutions to overcome any identified unresolved issues. Based on exemplary use-case scenarios, this work focuses on the security requirements for the interaction with NFC tags and the use of NFC card emulation. For each of these two modes of NFC, existing security concepts are identified, new attack scenarios that are possible despite these existing concepts are revealed, and solutions to overcome these issues are proposed. With the introduction of NFC to iOS (on the iPhone 6 in late 2014)—the last smartphone platform with significant market share that did not yet include NFC technology—the results of my research gained new importance.

The original thesis was finished in January 2013 and was submitted to Johannes Kepler University Linz for review in February 2013. The viva voce was

successfully held in March 2013. Compared to my original thesis, this book contains updates, clarifications, and additions based on recent events.

The three years of researching, preparing, and writing this thesis were a journey with many ups and downs. I would like to thank my colleagues at the NFC Research Lab Hagenberg (Josef Langer, Christian Saminger, and Stefan Grünberger) for supporting me in many ways. I would like to thank my advisor, Josef Scharinger, and my second advisor, René Mayrhofer, for their guidance, advice, and criticism. Josef and René took the time to read this Ph.D. thesis and to provide valuable feedback. Further, I would like to thank the participants of the seminar for Ph.D. students at the Department of Computational Perception (Johannes Kepler University Linz) for giving valuable hints and starting interesting discussions. Moreover, I would also like to thank the team of First Data Austria for providing a credit card terminal for my tests.

Last, but not least, I would like to thank my family for their love and support; and I would like to thank my friends for making my life enjoyable and sociable.

Linz, Austria, December 2014 Michael Roland

Acknowledgments

This research was conducted as part of the project “4EMOBILITY” (Energy-efficient Economic and Ecological Mobility) within the EU programme “Regionale Wettbewerbsfähigkeit OÖ 2007–2013 (Regio 13)” funded by the European Regional Development Fund (ERDF) and the Province of Upper Austria (Land Oberösterreich).

Contents

Acronyms

ACE	Access Control Entry
ACF	Access Control File
ACL	Access Control List
AID	Application Identifier
APDU	Application Protocol Data Unit
API	Application Programming Interface
ARA	Access Rule Applet
ARF	Access Rule File
ATC	Application Transaction Counter
ATM	Automatic Teller Machine
ATR	Answer-to-Reset
ATS	Answer-to-Select
BER-TLV	Basic Encoding Rules Tag-Length-Value Format
C-APDU	Command APDU
CA	Certification Authority
CF	Chunk Flag
CVC3	Card Verification Code 3
CVM	Cardholder Verification Method
DF	Dedicated File
DoS	Denial-of-Service
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
ECQV	Elliptic Curve Qu-Vanstone
EMV	Europay, MasterCard and Visa
FCI	File Control Information Template
FDT	Frame Delay Time
EF	Elementary File
FWT	Frame Waiting Time
GCF	Generic Connection Framework
GPS	Global Positioning System

HTTP	Hyper Text Transfer Protocol
IANA	Internet Assigned Numbers Authority
IC	Integrated Circuit
ID	Identifier
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IL	ID-Length Present
IP	Internet Protocol
ISD	Issuer Security Domain
ISO	International Organization for Standardization
JAR	Java Archive
Java ME	Java Platform, Micro Edition
Java SE	Java Platform, Standard Edition
JCRMI	Java Card Remote Method Invocation
JSR	Java Specification Request
KVM	K Virtual Machine
LFSR	Linear Feedback Shift Register
LLCP	Logical Link Control Protocol
MB	Message Begin
ME	Message End
MIME	Multipurpose Internet Mail Extensions
MTM	Mobile Trusted Module
NDEF	NFC Data Exchange Format
NFC	Near Field Communication
NFC-DEP	NFC Data Exchange Protocol
ObC	On-board Credentials
OBEX	Object Exchange
OPEN	GlobalPlatform Environment
PAN	Primary Account Number
PC	Personal Computer
PC/SC	Personal Computer/Smart Card Interface
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Card
PIN	Personal Identification Number
PKI	Public-Key Infrastructure
POS	Point-of-Sale
PPSE	Proximity Payment System Environment
PUPI	Pseudo Unique PICC Identifier
R-APDU	Response APDU
RF	Radio Frequency
RFID	Radio Frequency Identification
RTD	Record Type Definition
SATSA	Security and Trust Services API
SDK	Software Development Kit
SE	Secure Element

SEEK	Secure Element Evaluation Kit
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SMS	Short Message Service
SNEP	Simple NDEF Exchange Protocol
SR	Short Record
SWP	Single Wire Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TLV	Tag-Length-Value Format
TNF	Type Name Format
UHF	Ultra High Frequency
UICC	Universal Integrated Circuit Card
UID	Unique Identifier
UN	Unpredictable Number
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WTX	Frame Waiting Time Extension
XML	Extensible Markup Language

Abstract

The recent emergence of Near Field Communication (NFC)-enabled smartphones led to an increasing interest in NFC technology and its applications by equipment manufacturers, service providers, developers, and end-users. Nevertheless, frequent media reports about security and privacy issues of electronic passports, contactless credit cards, asset tracking systems, NFC-enabled mobile phones, and proprietary contactless technologies suggest that NFC is a potentially unsafe technology whose main beneficiaries are thieves. While these weaknesses are often bound to specific applications and products, they boost the fear that NFC technology as a whole is dangerous, threatens our privacy, and helps identity theft and fraud. In order to defend their own products and services, manufacturers and service providers often position themselves on the opposite extreme, stating that their products and services incorporate sufficient countermeasures.

This work aims for assessing the actual state of NFC security, for discovering new attack scenarios and for providing concepts and solutions to overcome any identified unresolved issues. Based on exemplary use-case scenarios, application-specific security aspects of NFC are extracted. The current security architectures of NFC-enabled mobile phones are evaluated with regard to the identified security aspects. As a result of the exemplary use-cases, this research focuses on the interaction with NFC tags and on card emulation. For each of these two modes of NFC, this thesis reveals attack scenarios that are possible despite existing security concepts. For the interaction with NFC tags, a new attack scenario is introduced that allows modification of tag content even though its authenticity and integrity were supposedly guaranteed by a digital signature scheme. Moreover, potential privacy issues and remaining problems have been identified in the NFC Forum's signature scheme specification. For the card emulation scenario, the mobile phone itself is identified as a significant, yet unconsidered, threat. Specifically, the well-known concept of relay attacks on smartcards is extended to the mobile phone platform. By using the phone's processing capabilities and communication facilities, relay

attacks can be mounted in a significantly easier and less obvious way. These assumptions are verified through prototypical implementations. Possible solutions and workarounds to overcome these issues are outlined and evaluated with regard to their advantages and disadvantages.