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

http://www.springer.com/978-3-319-15487-9

Security Issues in Mobile NFC Devices

Roland, M.

2015, XVIII, 185 p. 44 illus., 17 illus. in color., Hardcover
ISBN: 978-3-319-15487-9