

Contents

1	Introduction	1
1.1	Motivation	1
1.2	Objectives	3
1.3	Approach	4
1.4	Contributions	5
1.5	Publications	5
1.6	Outline	7
	References	8
2	Basics	13
2.1	Smartcards	13
2.1.1	Protocol Stack	14
2.1.2	Contact versus Contactless Smartcards	15
2.1.3	Smartcard Software	17
2.1.4	Data Structures Used on Smartcards	18
2.1.5	PC/SC	19
2.2	Near Field Communication	19
2.2.1	NFC Forum	20
2.2.2	Operating Modes	20
2.2.3	NFC Tags	21
2.2.4	NFC Data Exchange Format (NDEF)	22
2.2.5	NFC Record Type Definition (RTD)	24
2.2.6	Card Emulation	27
2.3	EMV	28
	References	29
3	Exemplary Use-Cases	33
3.1	Improving Efficiency in Automotive Environments	34
3.1.1	Personalization in a Multi-user/Multi-car Environment	34

3.1.2	Transmission of Data Generated by Vehicle Sensors	36
3.1.3	Intelligent Cloud-Based Multimedia Applications	38
3.2	Generalized Use-Cases	39
3.2.1	Out-of-Band Pairing with NFC	39
3.2.2	Secure Element.	40
3.3	Identification of Security Aspects	42
3.3.1	Peer-to-Peer Mode	42
3.3.2	Reader/Writer Mode	43
3.3.3	Card Emulation Mode	43
	References.	44
4	Related Work.	47
4.1	Communication Protocol	47
4.2	Flaws in Legacy Contactless Chip Card Systems	48
4.3	Attacks on Contactless Smartcards	49
4.4	Security and Privacy Aspects of NFC Devices	51
4.4.1	Tagging and Peer-to-Peer Communication	52
4.4.2	Protection for Tagging and Peer-to-Peer Communication	53
4.4.3	Integration of Secure Elements into Mobile Phones. . .	54
4.4.4	Mobile Phones as Attack Platforms.	55
4.5	Mobile Phone and Smart Phone Security	56
4.6	Combining NFC with Trusted Platform Concepts	59
4.7	Flaws in Existing Mobile Wallet Implementations.	59
4.8	Summary.	61
	References.	62
5	Tagging	69
5.1	Security Issues	69
5.2	Digital Signature for NDEF Messages	72
5.2.1	Attaching a Signature to an NDEF Message.	73
5.2.2	Maintaining Backwards Compatibility	73
5.2.3	Signing Individual Records	74
5.2.4	Scope of a Signature	74
5.2.5	Limitations of NDEF APIs.	77
5.2.6	Recommended Practice	78
5.3	Establishing Trust in Digitally Signed Content	79
5.3.1	Public-Key Infrastructure	79
5.3.2	Mapping Content Issuer Certificates to Content	81
5.3.3	Partial Signatures	82
5.3.4	Managing Content Issuer Private Keys	84
5.3.5	Lifespan of Certificates and Signatures	86

5.4	The NFC Forum Signature RTD	88
5.4.1	Signature Record	88
5.4.2	Attaching a Signature to NDEF Messages	90
5.4.3	Signature Coverage	90
5.5	Weaknesses of the Signature RTD	90
5.5.1	Establishing Trust	91
5.5.2	Using Remote Signatures and Certificates	91
5.5.3	Insufficient Signature Coverage	92
5.5.4	Record Composition Attack	96
5.6	Possible Solutions to the Discovered Weaknesses	98
	References.	100
6	Card Emulation	103
6.1	Current Perspective on Security	103
6.2	APIs for Access to the Secure Element	104
6.2.1	JSR 177	105
6.2.2	Nokia Extensions to JSR 257	106
6.2.3	BlackBerry.	107
6.2.4	Android.	107
6.2.5	Open Mobile API	109
6.2.6	Secure Element Access Control	111
6.2.7	Comparison of Access Control Schemes	112
6.2.8	Impact of Rooting and Jail Breaking	114
6.3	New Attack Scenarios	114
6.3.1	Denial-of-Service (DoS).	115
6.3.2	Software-Based Relay Attack	118
6.4	Viability of the Software-Based Relay Attack	122
6.4.1	Constraints of the Protocol Layers	122
6.4.2	Building a Card Emulator	124
6.4.3	Prototype Implementation of the Relay System.	126
6.4.4	Test Setup for Measurement of Communication Delays.	130
6.4.5	Measurement Results.	135
6.5	Possible Solutions.	141
	References.	143
7	Software-Based Relay Attacks on Existing Applications	147
7.1	Google Wallet	148
7.1.1	Preparing for an In-depth Analysis	148
7.1.2	Static Structure.	149
7.1.3	Interacting with the Google Wallet On-card Component	150

7.1.4	Google Prepaid Card: A MasterCard PayPass Card	151
7.2	Performing a Software-Based Relay Attack	154
7.3	Viability, Limitations and Improvements	155
7.3.1	Getting the Relay App on Devices	156
7.3.2	Transaction Limits	156
7.3.3	Optimizing the Relayed Data	156
7.4	Possible Workarounds	157
7.4.1	Timeouts of POS Terminals	157
7.4.2	Google Wallet PIN Verification	157
7.4.3	Disabling Internal Mode for Payment Applets	158
7.5	Reporting and Industry Response	159
7.6	Analysis of the Relay-Immune Google Wallet	159
	References.	160
8	Summary and Outlook	163
8.1	Tagging.	163
8.2	Card Emulation	164
8.3	Conclusion.	166
8.4	The Bigger Picture	166
8.5	Future Research	167
	References.	168
	Appendix A: Google's Secure Element API.	171
	Appendix B: Modifications to Google's Secure Element API Library.	175
	Index	183

<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