1. Record Nr. UNINA9910135023703321

Autore	Penttinen Jyrki T. J.
Titolo	Wireless communications security : solutions for the internet of things / / Jyrki T.J. Penttinen, Giesecke & Devrient, USA
Pubbl/distr/stampa	The Atrium, Southern Gates, Chichester, West Sussex, United Kingdom : , : John Wiley & Sons, Ltd, , 2017 [Piscataqay, New Jersey] : , : IEEE Xplore, , [2016]
ISBN	1-119-08441-5 1-119-08440-7
Edizione	[1st edition]
Descrizione fisica	1 online resource (306 pages)
Disciplina	005.8
Soggetti	Wireless communication systems - Security measures Internet - Security measures Computer networks - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	-- About the Author xii -- Preface xiii -- Acknowledgements xv -- Abbreviations xvi -- 1 Introduction 1 -- 1.1 Introduction 1 -- 1.2 Wireless Security 2 -- 1.2.1 Background and Advances 2 -- 1.2.2 Statistics 2 -- 1.2.3 Wireless Threats 4 -- 1.2.4 M2M Environment 9 -- 1.3 Standardization 10 -- 1.3.1 The Open Mobile Alliance (OMA) 10 -- 1.3.2 The International Organization for Standardization (ISO) 12 -- 1.3.3 The International Telecommunications Union (ITU) 14 -- 1.3.4 The European Telecommunications Standards Institute (ETSI) 14 -- 1.3.5 The Institute of Electrical and Electronics Engineers (IEEE) 15 -- 1.3.6 The Internet Engineering Task Force (IETF) 16 -- 1.3.7 The 3rd Generation Partnership Project (3GPP) 16 -- 1.3.8 The 3rd Generation Partnership Project 2 (3GPP2) 25 -- 1.3.9 The GlobalPlatform 25 -- 1.3.10 The SIMalliance 26 -- 1.3.11 The Smartcard Alliance 27 -- 1.3.12 The GSM Association (GSMA) 27 -- 1.3.13 The National Institute of Standards and Technology (NIST) 28 -- 1.3.14 The National Highway Transportation and Safety Administration (NHTSA) 28 -- 1.3.15 Other Standardization and Industry Forums 28 -- 1.3.16 The EMV Company (EMVCo) 29 -- 1.3.17 The Personal Computer/Smartcard (PC/SC) 29 -- 1.3.18 The Health Insurance Portability and Accountability Act (HIPAA)

29 -- 1.3.19 The Common Criteria (CC) 29 -- 1.3.20 The Evaluation Assurance Level (EAL) 30 -- 1.3.21 The Federal Information Processing Standards (FIPS) 31 -- 1.3.22 Biometric Standards 31 -- 1.3.23 Other Related Entities 32 -- 1.4 Wireless Security Principles 32 -- 1.4.1 General 32 -- 1.4.2 Regulation 33 -- 1.4.3 Security Architectures 33 -- 1.4.4 Algorithms and Security Principles 33 -- 1.5 Focus and Contents of the Book 36 -- References 38 -- 2 Security of Wireless Systems 42 -- 2.1 Overview 42 -- 2.1.1 Overall Security Considerations in the Mobile Environment 42 -- 2.1.2 Developing Security Threats 43 -- 2.1.3 RF Interferences and Safety 45 -- 2.2 Effects of Broadband Mobile Data 46 -- 2.2.1 Background 46.
2.2.2 The Role of Networks 47 -- 2.2.3 The Role of Apps 50 -- 2.2.4 UE Application Development 52 -- 2.2.5 Developers 55 -- 2.2.6 The Role of the SIM/UICC 56 -- 2.2.7 Challenges of Legislation 57 -- 2.2.8 Updating Standards 58 -- 2.2.9 3GPP System Evolution 58 -- 2.3 GSM 59 -- 2.3.1 The SIM 60 -- 2.3.2 Authentication and Authorization 62 -- 2.3.3 Encryption of the Radio Interface 63 -- 2.3.4 Encryption of IMSI 65 -- 2.3.5 Other GSM Security Aspects 65 -- 2.4 UMTS/HSPA 66 -- 2.4.1 Principles of 3G Security 66 -- 2.4.2 Key Utilization 68 -- 2.4.3 3G Security Procedures 69 -- 2.5 Long Term Evolution 71 -- 2.5.1 Protection and Security Principles 71 -- 2.5.2 X.509 Certificates and Public Key Infrastructure (PKI) 71 -- 2.5.3 IPsec and Internet Key Exchange (IKE) for LTE Transport Security 72 -- 2.5.4 Traffic Filtering 73 -- 2.5.5 LTE Radio Interface Security 74 -- 2.5.6 Authentication and Authorization 78 -- 2.5.7 LTE/SAE Service Security / Case Examples 79 -- 2.5.8 Multimedia Broadcast and Multicast Service (MBMS) and enhanced MBMS (eMBMS) 83 -- 2.6 Security Aspects of Other Networks 91 -- 2.6.1 CDMA (IS‐95) 91 -- 2.6.2 CDMA2000 93 -- 2.6.3 Broadcast Systems 94 -- 2.6.4 Satellite Systems 94 -- 2.6.5 Terrestrial Trunked Radio (TETRA) 95 -- 2.6.6 Wireless Local Area Network (WLAN) 96 -- 2.7 Interoperability 102 -- 2.7.1 Simultaneous Support for LTE/SAE and 2G/3G 102 -- 2.7.2 VoLTE 105 -- 2.7.3 CS Fallback 105 -- 2.7.4 Inter‐operator Security Aspects 106 -- 2.7.5 Wi‐Fi Networks and Offload 106 -- 2.7.6 Femtocell Architecture 108 -- References 109 -- 3 Internet of Things 112 -- 3.1 Overview 112 -- 3.2 Foundation 113 -- 3.2.1 Definitions 113 -- 3.2.2 Security Considerations of IoT 115 -- 3.2.3 The Role of IoT 115 -- 3.2.4 IoT Environment 117 -- 3.2.5 IoT Market 120 -- 3.2.6 Connectivity 121 -- 3.2.7 Regulation 122 -- 3.2.8 Security Risks 123 -- 3.2.9 Cloud 128 -- 3.2.10 Cellular Connectivity 129 -- 3.2.11 WLAN 133 -- 3.2.12 Low‐Range Systems 133 -- 3.3 Development of IoT 140.
3.3.1 GSMA Connected Living 140 -- 3.3.2 The GlobalPlatform 141 -- 3.3.3 Other Industry Forums 141 -- 3.4 Technical Description of IoT 142 -- 3.4.1 General 142 -- 3.4.2 Secure Communication Channels and Interfaces 143 -- 3.4.3 Provisioning and Key Derivation 144 -- 3.4.4 Use Cases 144 -- References 148 -- 4 Smartcards and Secure Elements 150 -- 4.1 Overview 150 -- 4.2 Role of Smartcards and SEs 151 -- 4.3 Contact Cards 153 -- 4.3.1 ISO/IEC 7816‐1 154 -- 4.3.2 ISO/IEC 7816‐2 155 -- 4.3.3 ISO/IEC 7816‐3 155 -- 4.3.4 ISO/IEC 7816‐4 157 -- 4.3.5 ISO/IEC 7816‐5 157 -- 4.3.6 ISO/IEC 7816‐6 157 -- 4.3.7 ISO/IEC 7816‐7 157 -- 4.3.8 ISO/IEC 7816‐8 157 -- 4.3.9 ISO/IEC 7816‐9 158 -- 4.3.10 ISO/IEC 7816‐10 158 -- 4.3.11 ISO/IEC 7816‐11 158 -- 4.3.12 ISO/IEC 7816‐12 158 -- 4.3.13 ISO/IEC 7816‐13 158 -- 4.3.14 ISO/IEC 7816‐15 158 -- 4.4 The SIM/UICC 159 -- 4.4.1 Terminology 159 -- 4.4.2 Principle 159 -- 4.4.3 Key Standards

160 -- 4.4.4 Form Factors 161 -- 4.5 Contents of the SIM 164 -- 4.5.1 UICC Building Blocks 164 -- 4.5.2 The SIM Application Toolkit (SAT) 167 -- 4.5.3 Contents of the UICC 168 -- 4.6 Embedded SEs 168 -- 4.6.1 Principle 168 -- 4.6.2 M2M Subscription Management 169 -- 4.6.3 Personalization 172 -- 4.6.4 M2M SIM Types 173 -- 4.7 Other Card Types 174 -- 4.7.1 Access Cards 174 -- 4.7.2 External SD Cards 175 -- 4.8 Contactless Cards 175 -- 4.8.1 ISO/IEC Standards 175 -- 4.8.2 NFC 176 -- 4.9 Electromechanical Characteristics of Smartcards 178 -- 4.9.1 HW Blocks 178 -- 4.9.2 Memory 178 -- 4.9.3 Environmental Classes 179 -- 4.10 Smartcard SW 181 -- 4.10.1 File Structure 181 -- 4.10.2 Card Commands 183 -- 4.10.3 Java Card 184 -- 4.11 UICC Communications 184 -- 4.11.1 Card Communications 184 -- 4.11.2 Remote File Management 185 -- References 186 -- 5 Wireless Payment and Access Systems 188 -- 5.1 Overview 188 -- 5.2 Wireless Connectivity as a Base for Payment and Access 188 -- 5.2.1 Barcodes 189 -- 5.2.2 RFID 191 -- 5.2.3 NFC 192 -- 5.2.4 Secure Element 196 -- 5.2.5 Tokenization 198.
5.3 E‐commerce 200 -- 5.3.1 EMV 200 -- 5.3.2 Google Wallet 200 -- 5.3.3 Visa 201 -- 5.3.4 American Express 201 -- 5.3.5 Square 201 -- 5.3.6 Other Bank Initiatives 201 -- 5.3.7 Apple Pay 201 -- 5.3.8 Samsung Pay 202 -- 5.3.9 MCX 202 -- 5.3.10 Comparison of Wallet Solutions 202 -- 5.4 Transport 203 -- 5.4.1 MiFare 204 -- 5.4.2 CiPurse 204 -- 5.4.3 Calypso 204 -- 5.4.4 FeliCa 205 -- 5.5 Other Secure Systems 205 -- 5.5.1 Mobile ID 205 -- 5.5.2 Personal Identity Verification 205 -- 5.5.3 Access Systems 206 -- References 206 -- 6 Wireless Security Platforms and Functionality 208 -- 6.1 Overview 208 -- 6.2 Forming the Base 208 -- 6.2.1 Secure Service Platforms 209 -- 6.2.2 SEs 209 -- 6.3 Remote Subscription Management 210 -- 6.3.1 SIM as a Basis for OTA 210 -- 6.3.2 TSM 212 -- 6.3.3 TEE 213 -- 6.3.4 HCE and the Cloud 216 -- 6.3.5 Comparison 219 -- 6.4 Tokenization 219 -- 6.4.1 PAN Protection 219 -- 6.4.2 HCE and Tokenization 221 -- 6.5 Other Solutions 221 -- 6.5.1 Identity Solutions 221 -- 6.5.2 Multi‐operator Environment 222 -- References 222 -- 7 Mobile Subscription Management 223 -- 7.1 Overview 223 -- 7.2 Subscription Management 223 -- 7.2.1 Development 223 -- 7.2.2 Benefits and Challenges of Subscription Management 225 -- 7.3 OTA Platforms 226 -- 7.3.1 General 226 -- 7.3.2 Provisioning Procedure 227 -- 7.3.3 SMS‐based SIM OTA 227 -- 7.3.4 HTTPS‐based SIM OTA 230 -- 7.3.5 Commercial Examples of SIM OTA Solutions 231 -- 7.4 Evolved Subscription Management 232 -- 7.4.1 GlobalPlatform 233 -- 7.4.2 SIMalliance 233 -- 7.4.3 OMA 233 -- 7.4.4 GSMA 235 -- References 240 -- 8 Security Risks in the Wireless Environment 242 -- 8.1 Overview 242 -- 8.2 Wireless Attack Types 243 -- 8.2.1 Cyber‐attacks 243 -- 8.2.2 Radio Jammers and RF Attacks 244 -- 8.2.3 Attacks against SEs 245 -- 8.2.4 IP Breaches 245 -- 8.2.5 UICC Module 246 -- 8.3 Security Flaws on Mobile Networks 247 -- 8.3.1 Potential Security Weaknesses of GSM 247 -- 8.3.2 Potential Security Weaknesses of 3G 254 -- 8.4 Protection Methods 254.
8.4.1 LTE Security 254 -- 8.4.2 Network Attack Types in LTE/SAE 255 -- 8.4.3 Preparation for the Attacks 256 -- 8.5 Errors in Equipment Manufacturing 259 -- 8.5.1 Equipment Ordering 259 -- 8.5.2 Early Testing 260 -- 8.6 Self‐Organizing Network Techniques for Test and Measurement 264 -- 8.6.1 Principle 264 -- 8.6.2 Self‐configuration 265 -- 8.6.3 Self‐optimizing 266 -- 8.6.4 Self‐healing 266 -- 8.6.5 Technical Issues and Impact on Network Planning 266 -- 8.6.6 Effects on Network Installation, Commissioning and Optimization 267 -- 8.6.7 SON and Security 268

-- References 268 -- 9 Monitoring and Protection Techniques 270 -- 9.1 Overview 270 -- 9.2 Personal Devices 271 -- 9.2.1 Wi‐Fi Connectivity 271 -- 9.2.2 Firewalls 271 -- 9.3 IP Core Protection Techniques 272 -- 9.3.1 General Principles 272 -- 9.3.2 LTE Packet Core Protection 272 -- 9.3.3 Protection against Roaming Threats 275 -- 9.4 HW Fault and Performance Monitoring 276 -- 9.4.1 Network Monitoring 277 -- 9.4.2 Protection against DoS/DDoS 277 -- 9.4.3 Memory Wearing 277 -- 9.5 Security Analysis 278 -- 9.5.1 Post‐processing 278 -- 9.5.2 Real‐time Security Analysis 278 -- 9.6 Virus Protection 279 -- 9.7 Legal Interception 281 -- 9.8 Personal Safety and Privacy 283 -- 9.8.1 CMAS 283 -- 9.8.2 Location Privacy 285 -- 9.8.3 Bio‐effects 286 -- References 287 -- 10 Future of Wireless Solutions and Security 288 -- 10.1 Overview 288 -- 10.2 IoT as a Driving Force 288 -- 10.3 Evolution of 4G 289 -- 10.4 Development of Devices 291 -- 10.4.1 Security Aspects of Smartcards 291 -- 10.4.2 Mobile Device Considerations 291 -- 10.4.3 IoT Device Considerations 292 -- 10.4.4 Sensor Networks and Big Data 293 -- 10.5 5G Mobile Communications 294 -- 10.5.1 Standardization 294 -- 10.5.2 Concept 295 -- 10.5.3 Industry and Investigation Initiatives 297 -- 10.5.4 Role of 5G in IoT 297 -- References 297 -- Index 299.

Sommario/riassunto

This book describes the current and most probable future wireless security solutions. The focus is on the technical discussion of existing systems and new trends like Internet of Things (IoT). It also discusses existing and potential security threats, presents methods for protecting systems, operators and end-users, describes security systems attack types and the new dangers in the ever-evolving Internet. The book functions as a practical guide describing the evolvement of the wireless environment, and how to ensure the fluent continuum of the new functionalities, whilst minimizing the potential risks in network security.

2. Record Nr. UNIORUON00294395

Titolo	Anthologie du Minnesang : Textes / avec introduction, notes et glossaire par André Moret
Pubbl/distr/stampa	Paris, : Aubier, éditions Montaigne, 1949
Descrizione fisica	305 p. ; 19 cm.
Disciplina	831.1
Lingua di pubblicazione	Tedesco Francese
Formato	Materiale a stampa
Livello bibliografico	Monografia