

1. Record Nr.	UNINA9910809381503321
Autore	Rhee Man Young
Titolo	Wireless mobile internet security // Man Young Rhee, Endowed Chair Professor, Kyung Hee University, Professor Emeritus, Hanyang University, Republic of Korea
Pubbl/distr/stampa	Chichester, West Sussex, United Kingdom : , : Wiley, A John Wiley & Sons Ltd., Publication, , 2013 [Piscataway, New Jersey] : , : IEEE Xplore, , [2013]
ISBN	1-118-51292-8 1-118-51294-4 1-299-44942-5 1-118-51299-5
Edizione	[2nd ed.]
Descrizione fisica	1 online resource (523 p.)
Disciplina	004.67/8
Soggetti	Wireless Internet - 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	-- Preface xiii -- About the Author xxi -- Acknowledgments xxiii -- 1 Internetworking and Layered Models 1 -- 1.1 Networking Technology 2 -- 1.2 Connecting Devices 5 -- 1.3 The OSI Model 8 -- 1.4 TCP/IP Model 12 -- 2 TCP/IP Suite and Internet Stack Protocols 15 -- 2.1 Network Layer Protocols 15 -- 2.2 Transport Layer Protocols 41 -- 2.3 World Wide Web 47 -- 2.4 File Transfer 49 -- 2.5 E-Mail 50 -- 2.6 Network Management Service 52 -- 2.7 Converting IP Addresses 53 -- 2.8 Routing Protocols 54 -- 2.9 Remote System Programs 55 -- 2.10 Social Networking Services 56 -- 2.11 Smart IT Devices 57 -- 2.12 Network Security Threats 58 -- 2.13 Internet Security Threats 58 -- 2.14 Computer Security Threats 59 -- 3 Global Trend of Mobile Wireless Technology 63 -- 3.1 1G Cellular Technology 63 -- 3.2 2G Mobile Radio Technology 64 -- 3.3 2.5G Mobile Radio Technology 67 -- 3.4 3G Mobile Radio Technology (Situation and Status of 3G) 70 -- 3.5 3G UMTS Security-Related Encryption Algorithm 75 -- 4 Symmetric Block Ciphers 81 -- 4.1 Data Encryption Standard (DES) 81 -- 4.2 International Data Encryption Algorithm (IDEA) 99 -- 4.3 RC5 Algorithm 108 -- 4.4 RC6 Algorithm 123 -- 4.5 AES (Rijndael) Algorithm 135 --

5 Hash Function, Message Digest, and Message Authentication Code 161 -- 5.1 DMDC Algorithm 161 -- 5.2 Advanced DMDC Algorithm 171 -- 5.3 MD5 Message-Digest Algorithm 176 -- 5.4 Secure Hash Algorithm (SHA-1) 188 -- 5.5 Hashed Message Authentication Codes (HMAC) 195 -- 6 Asymmetric Public-Key Cryptosystems 203 -- 6.1 Diffie / Hellman Exponential Key Exchange 203 -- 6.2 RSA Public-Key Cryptosystem 207 -- 6.3 ElGamal's Public-Key Cryptosystem 215 -- 6.4 Schnorr's Public-Key Cryptosystem 222 -- 6.5 Digital Signature Algorithm 227 -- 6.6 The Elliptic Curve Cryptosystem (ECC) 230 -- 7 Public-Key Infrastructure 249 -- 7.1 Internet Publications for Standards 250 -- 7.2 Digital Signing Techniques 251 -- 7.3 Functional Roles of PKI Entities 258 -- 7.4 Key Elements for PKI Operations 263 -- 7.5 X.509 Certificate Formats 271. 7.6 Certificate Revocation List 282 -- 7.7 Certification Path Validation 287 -- 8 Network Layer Security 291 -- 8.1 IPsec Protocol 291 -- 8.2 IP Authentication Header 299 -- 8.3 IP ESP 301 -- 8.4 Key Management Protocol for IPsec 308 -- 9 Transport Layer Security: SSLv3 and TLSv1 325 -- 9.1 SSL Protocol 325 -- 9.2 Cryptographic Computations 338 -- 9.3 TLS Protocol 339 -- 10 Electronic Mail Security: PGP, S/MIME 353 -- 10.1 PGP 353 -- 10.2 S/MIME 372 -- 11 Internet Firewalls for Trusted Systems 387 -- 11.1 Role of Firewalls 387 -- 11.2 Firewall-Related Terminology 388 -- 11.3 Types of Firewalls 392 -- 11.4 Firewall Designs 398 -- 11.5 IDS Against Cyber Attacks 401 -- 11.6 Intrusion Detections Systems 404 -- 12 SET for E-Commerce Transactions 415 -- 12.1 Business Requirements for SET 415 -- 12.2 SET System Participants 417 -- 12.3 Cryptographic Operation Principles 418 -- 12.4 Dual Signature and Signature Verification 420 -- 12.5 Authentication and Message Integrity 424 -- 12.6 Payment Processing 427 -- 13 4G Wireless Internet Communication Technology 439 -- 13.1 Mobile WiMAX 440 -- 13.2 WiBro (Wireless Broadband) 448 -- 13.3 UMB (Ultra Mobile Broadband) 452 -- 13.4 LTE (Long Term Evolution) 457 -- Acronyms 467 -- Bibliography 473 -- Index 481.

Sommario/riassunto

The mobile industry for wireless cellular services has grown at a rapid pace over the past decade. Similarly, Internet service technology has also made dramatic growth through the World Wide Web with a wire line infrastructure. Realization for complete wired/wireless mobile Internet technologies will become the future objectives for convergence of these technologies through multiple enhancements of both cellular mobile systems and Internet interoperability. Flawless integration between these two wired/wireless networks will enable subscribers to not only roam worldwide, but also to solve the ever increasing demand for data/Internet services. In order to keep up with this noteworthy growth in the demand for wireless broadband, new technologies and structural architectures are needed to greatly improve system performance and network scalability while significantly reducing the cost of equipment and deployment. Dr. Rhee covers the technological development of wired/wireless internet communications in compliance with each iterative generation up to 4G systems, with emphasis on wireless security aspects. By progressing in a systematic matter, presenting the theory and practice of wired/wireless mobile technologies along with various security problems, readers will gain an intimate sense of how mobile internet systems operate and how to address complex security issues. Features: . Written by a top expert in information security. Gives a clear understanding of wired/wireless mobile internet technologies. Presents complete coverage of various cryptographic protocols and specifications needed for 3GPP: AES, KASUMI, Public-key and Elliptic curve cryptography. Forecast new features and promising 4G packet-switched wireless internet

technologies for voice and data communications. Provides MIMO/OFDMA-based for 4G systems such as Long Term Evolution (LTE), Ultra Mobile Broadband (UMB), Mobile WiMax or Wireless Broadband (WiBro). Deals with Intrusion Detection System against worm/virus cyber attacks The book ideal for advanced undergraduate and postgraduate students enrolled in courses such as Wireless Access Networking, Mobile Internet Radio Communications. Practicing engineers in industry and research scientists can use the book as a reference to get reacquainted with mobile radio fundamentals or to gain deeper understanding of complex security issues.
