1. Record Nr. UNINA9910784359303321

Autore	Chandra Praphul
Titolo	Bulletproof wireless security [[electronic resource]] : GSM, UMTS, 802.11 and ad hoc security / / by Praphul Chandra
Pubbl/distr/stampa	Amsterdam ; ; Oxford, : Newnes, 2005
ISBN	1-281-00975-X 9786611009755 0-08-047631-7
Edizione	[1st edition]
Descrizione fisica	1 online resource (272 p.)
Collana	Communications engineering series
Disciplina	005.8
Soggetti	Wireless communication systems - Security measures Wireless LANs - Security measures Global system for mobile communications - Security measures Universal Mobile Telecommunications System - Security measures IEEE 802.11 (Standard)
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 (p. 229-230) and index.
Nota di contenuto	1.7 Beyond Cryptography1.7.1 Firewalls; 1.7.2 Denial of Service Attacks; 1.7.3 Code Security; 1.7.4 Steganography; 1.8 Conclusion; Chapter 2: Network Security Protocols; 2.1 Introduction; 2.2 Key Establishment Protocols; 2.2.1 Key Generation in SKC; 2.2.2 Key Distribution in SKC; 2.2.3 Key Establishment in PKC; 2.2.4 Diffie-Hellman Key Exchange; 2.2.5 Enhanced Diffie-Hellman Key Exchange; 2.2.6 RSA; 2.3 Authentication Protocols; 2.3.1 Address-Based Authentication; 2.3.2 Passwords for Local Authentication (Login); 2.3.3 Passwords for Network Authentication; 2.3.4 Authentication Using SKC 2.3.5 Authentication Using PKC2.3.6 What to Use for Authentication: SKC or PKC?; 2.3.7 Session Hijacking; 2.3.8 Needham Schroeder; 2.3.9 Kerberos; 2.4 Encryption Protocols; 2.4.1 DES; 2.4.2 TripleDES or 3DES; 2.4.3 AES; 2.4.4 RC4; 2.5 Integrity Protocols; 2.5.1 CBC Residue; 2.5.2 CRC32; 2.5.3 MD5; Chapter 3: Security and the Layered Architecture; 3.1 Introduction; 3.2 Security at Layer 1; 3.3 Security at Layer 2; 3.3.1 Extensible Authentication Protocol (EAP); 3.3.2 EAPoL: EAP Over LAN; 3.3.3 EAP-TLS: TLS Handshake Over EAP; 3.4 Security at Layer 3; 3.5

Security at Layer 4: SSL/TLS

3.6 Security at Layer 5+Chapter 4: Voice-Oriented Wireless Networks; 4.1 The Wireless Medium; 4.1.1 Radio Propagation Effects; 4.1.2 Hidden Terminal Problem; 4.1.3 Exposed Terminal Problem; 4.1.4 Bandwidth; 4.1.5 Other Constraints; 4.2 The Cellular Architecture; 4.3 TWNs: First Generation; 4.3.1 Addresses in AMPS; 4.3.2 Call Setup in AMPS; 4.4 TWNs: Second Generation; 4.4.1 Addresses in GSM; 4.4.2 Call Setup in GSM; 4.5 TWNs: Third Generation; 4.5.1 Connection Setup in UMTS; 4.6 The Overall Picture; Chapter 5: Data-Oriented Wireless Networks; 5.1 WLANs; 5.1.1: Addresses in 802.11
5.1.2 Connection Setup in 802.115.1.3 Media Access; 5.1.4 Spectrum Efficiency in 802.11; 5.2 MANETs; 5.2.1 MAC for MANETs; 5.2.2 Routing in MANETs.; 5.2.3 Address Allocation in MANETs; 5.2.4 Security in MANETs; 5.3 Wireless Networks in the Near Future; Chapter 6: Security in Traditional Wireless Networks; 6.1 Security in First Generation TWNs; 6.2 Security in Second Generation TWNs; 6.2.1 Anonymity in GSM; 6.2.2 Key Establishment in GSM; 6.2.3 Authentication in GSM; 6.2.4 Confidentiality in GSM; 6.2.5 What's Wrong with GSM Security?; 6.3 Security in 2.5 Generation TWNs; 6.3.1 WAP
6.3.2 Code Security

Sommario/riassunto

Finally--a single volume guide to really effective security for both voice and data wireless networks!More and more data and voice communications are going via wireless at some point between the sender and intended recipient. As a result, truly ""bulletproof"" wireless security is now more than a desirable feature--instead, it's a necessity to protect essential personal and business data from hackers and eavesdroppers.In this handy reference, Praphul Chandra gives you the conceptual and practical tools every RF, wireless, and network engineer needs for high-security wireless ap