

1. Record Nr.	UNINA9910808998003321
Autore	Perez Andre
Titolo	Network security / / Andre Perez
Pubbl/distr/stampa	London, [England] ; ; Hoboken, New Jersey : , : ISTE Limited : , : John Wiley & Sons, , 2014 ©2014
ISBN	1-119-04395-6 1-119-04394-8 1-119-04396-4
Descrizione fisica	1 online resource (310 p.)
Disciplina	005.8
Soggetti	Computer networks - Security measures Computers - Security
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	Cover Page; Half-Title Page; Title Page; Copyright Page; Contents; Preface; Abbreviations; 1: Introduction to Cryptography; 1.1. The encryption function; 1.1.1. 3DES algorithm; 1.1.2. AES algorithm; 1.1.3. RSA algorithm; 1.1.4. ECC algorithm; 1.2. Hash function; 1.2.1. MD5 algorithm; 1.2.2. SHA algorithm; 1.2.2.1. SHA-1 algorithm; 1.2.2.2. SHA-2 algorithm; 1.2.3. HMAC mechanism; 1.3. Key exchange; 1.3.1. Secret-key generation; 1.3.2. Public key distribution; 2: 802.1x Mechanism; 2.1. General introduction; 2.2. EAPOL protocol; 2.2.1. EAPOL-Start message; 2.2.2. EAPOL-Logoff message; 2.2.3. EAPOL-Key message; 2.2.4. EAPOL-Encapsulated-ASF-Alert message; 2.2.5. EAPOL-MKA message; 2.2.6. EAPOL-Announcement message; 2.2.7. EAPOL-Announcement-Req message; 2.3. EAP protocol; 2.3.1. EAP-Method Identity; 2.3.2. EAP-Method Notification; 2.3.3. EAP-Method NAK; 2.4. RADIUS protocol; 2.4.1. RADIUS messages; 2.4.1.1. Access-Request message; 2.4.1.2. Access-Challenge message; 2.4.1.3. Access-Accept message; 2.4.1.4. Access-Reject message; 2.4.2. RADIUS attributes; 2.4.2.1. EAP-Message attribute; 2.4.2.2. Message-Authenticator attribute; 2.4.2.3. Password-Retry attribute

2.4.2.4. User-Name attribute; 2.4.2.5. User-Password attribute; 2.4.2.6. NAS-IP-Address attribute; 2.4.2.7. NAS-Port attribute; 2.4.2.8. Service-Type attribute; 2.4.2.9. Vendor-Specific attribute; 2.4.2.10. Session-Timeout attribute; 2.4.2.11. Idle-Timeout attribute; 2.4.2.12. Termination-Action attribute; 2.5. Authentication procedures; 2.5.1. EAP-MD5 procedure; 2.5.2. EAP-TLS procedure; 2.5.3. EAP-TTLS procedure; 3: WPA Mechanisms; 3.1. Introduction to Wi-Fi technology; 3.2. Security mechanisms; 3.3. Security policies; 3.4. Key management; 3.4.1. Key hierarchy; 3.4.2. EAPOL-key messages; 3.4.3. Four-way handshake procedure; 3.4.4. Group key handshake procedure; 3.5. WEP protocol; 3.6. TKIP protocol; 3.7. CCMP protocol; 4: IPsec Mechanism; 4.1. Review of IP protocols; 4.1.1. IPv4 protocol; 4.1.2. IPv6 protocol; 4.2. IPsec architecture; 4.2.1. Security headers; 4.2.1.1. AH extension; 4.2.1.2. ESP extension; 4.2.1.3. Modes; 4.2.2. Security association; 4.2.3. PMTU processing; 4.3. IKEv2 protocol; 4.3.1. Message header; 4.3.2. Blocks; 4.3.2.1. SA block; 4.3.2.2. KE block; 4.3.2.3. IDi and IDr blocks; 4.3.2.4. CERT block; 4.3.2.5. CERTREQ block; 4.3.2.6. The AUTH block; 4.3.2.7. Ni and Nr blocks; 4.3.2.8. N block; 4.3.2.9. D block; 4.3.2.10. V block; 4.3.2.11. TS block; 4.3.2.12. SK block; 4.3.2.13. CP block; 4.3.2.14. EAP block; 4.3.3. Procedure; 4.3.3.1. IKE_SA_INIT exchange; 4.3.3.2. IKE_AUTH exchange; 4.3.3.3. CREATE_CHILD_SA exchange; 5: SSL, TLS and DTLS Protocols; 5.1. Introduction; 5.2. SSL/TLS protocols; 5.2.1. Record header; 5.2.2. Change_cipher_spec message; 5.2.3. Alert message; 5.2.4. Handshake messages; 5.2.4.1. Hello_request message; 5.2.4.2. Client_hello message; 5.2.4.3. Hello_server message; 5.2.4.4. Certificate message; 5.2.4.5. Server_key_exchange message

Sommario/riassunto

This book introduces the security mechanisms deployed in Ethernet, Wireless-Fidelity (Wi-Fi), Internet Protocol (IP) and MultiProtocol Label Switching (MPLS) networks. These mechanisms are grouped throughout the book according to the following four functions: data protection, access control, network isolation, and data monitoring. Data protection is supplied by data confidentiality and integrity control services. Access control is provided by a third-party authentication service. Network isolation is supplied by the Virtual Private Network (VPN) service. Data monitoring consists of applying