

Spis treści

Notacja (9)

Od redakcji wydania polskiego słów kilka (11)

Wstęp (13)

O autorze (19)

Część I: Zaufanie obustronne (21)

Rozdział 1. Zarządzanie kluczami i ich dystrybucja (21)

- 1.1. Dystrybucja kluczy przy użyciu kryptografii symetrycznej (23)
- 1.2. Dystrybucja kluczy przy użyciu kryptografii asymetrycznej (32)
- 1.3. Dystrybucja kluczy publicznych (35)
- 1.4. Standard X.509 (41)
- 1.5. Infrastruktura kluczy publicznych (50)
- 1.6. Zalecane materiały uzupełniające (53)
- 1.7. Kluczowe terminy, pytania przeglądowe i problemy (54)

Rozdział 2. Uwierzytelnianie użytkowników (59)

- 2.1. Zasady uwierzytelniania zdalnych użytkowników (60)
- 2.2. Uwierzytelnianie zdalnych użytkowników przy użyciu kryptografii symetrycznej (64)
- 2.3. Kerberos (68)
- 2.4. Uwierzytelnianie zdalnych użytkowników przy użyciu kryptografii asymetrycznej (89)
- 2.5. Zarządzanie tożsamością federacyjną (93)
- 2.6. Zalecane materiały uzupełniające (99)
- 2.7. Kluczowe terminy, pytania przeglądowe i problemy (101)
- Dodatek 2A Mechanizmy szyfrowania w Kerberosie (104)

Część II: Bezpieczeństwo sieci i internetu (109)

Rozdział 3. Bezpieczeństwo transportu danych (109)

- 3.1. Elementy bezpieczeństwa sieci (110)
- 3.2. Secure Socket Layer (SSL) (113)
- 3.3. Transport Layer Security (129)
- 3.4. HTTPS (134)
- 3.5. Secure Shell (SSH) (136)
- 3.6. Zalecane materiały uzupełniające (149)
- 3.7. Kluczowe terminy, pytania przeglądowe i problemy (149)

Rozdział 4. Bezpieczeństwo sieci bezprzewodowych (151)

- 4.1. Sieci bezprzewodowe IEEE 802.11 (153)

- 4.2. Bezpieczeństwo sieci bezprzewodowych IEEE 802.11i (160)
- 4.3. Protokół WAP (177)
- 4.4. Protokół WTLS - bezpieczeństwo bezprzewodowej warstwy transportowej (186)
- 4.5. Całościowe zabezpieczenie transmisji WAP (197)
- 4.6. Zalecane materiały uzupełniające (200)
- 4.7. Kluczowe terminy, pytania przeglądowe i problemy (201)

Rozdział 5. Bezpieczeństwo poczty elektronicznej (205)

- 5.1. PGP (207)
- 5.2. S/MIME (229)
- 5.3. DKIM (248)
- 5.4. Zalecane materiały uzupełniające (257)
- 5.5. Kluczowe terminy, pytania przeglądowe i problemy (258)
- Dodatek 5A Kodowanie radix-64 (259)

Rozdział 6. Bezpieczeństwo protokołu IP (263)

- 6.1. Ogólnie o IPsec (265)
- 6.2. Polityka bezpieczeństwa według IPsec (271)
- 6.3. Protokół ESP (278)
- 6.4. Komasaacja skojarzeń bezpieczeństwa (286)
- 6.5. Internetowa wymiana kluczy (IKE) (291)
- 6.6. Zestawy kryptograficzne (300)
- 6.7. Zalecane materiały uzupełniające (304)
- 6.8. Kluczowe terminy, pytania przeglądowe i problemy (304)

Część III: Bezpieczeństwo systemu (307)

Rozdział 7. Intruzi (307)

- 7.1. Intruzi (309)
- 7.2. Wykrywanie intruzów (316)
- 7.3. Zarządzanie hasłami (331)
- 7.4. Zalecane materiały uzupełniające (342)
- 7.5. Kluczowe terminy, pytania przeglądowe i problemy (345)
- Dodatek 7A Zaniedbywanie miarodajności (349)

Rozdział 8. Szkodliwe oprogramowanie (353)

- 8.1. Typy szkodliwego oprogramowania (355)
- 8.2. Wirusy (360)
- 8.3. Przeciwdziałanie wirusom (368)
- 8.4. Robaki (373)
- 8.5. Rozproszone ataki DoS (384)
- 8.6. Zalecane materiały uzupełniające (390)
- 8.7. Kluczowe terminy, pytania przeglądowe i problemy (392)

Rozdział 9. Firewall (397)

- 9.1. Zapotrzebowanie na firewalle (398)
- 9.2. Charakterystyka firewalli (399)
- 9.3. Typy firewalli (401)
- 9.4. Implementowanie firewalli (409)
- 9.5. Lokalizacja i konfiguracja firewalli (413)
- 9.6. Zalecane materiały uzupełniające (418)
- 9.7. Kluczowe terminy, pytania przeglądowe i problemy (418)

Rozdział 10. Prawne i etyczne aspekty bezpieczeństwa komputerowego (425)

- 10.1. Cyberprzestępczość i przestępstwa komputerowe (426)
- 10.2. Własność intelektualna (432)
- 10.3. Ochrona prywatności (439)
- 10.4. Infoetyka (443)
- 10.5. Zalecane materiały uzupełniające (452)
- 10.6. Kluczowe terminy, pytania przeglądowe i problemy (453)

Dodatki (457)

Dodatek A: Projekty dydaktyczne (457)

- A.1. System algebry komputerowej Sage (458)
- A.2. Projekt hackingu (459)
- A.3. Projekty związane z szyframi blokowymi (460)
- A.4. Ćwiczenia laboratoryjne (460)
- A.5. Projekty poszukiwawcze (461)
- A.6. Zadania programistyczne (461)
- A.7. Praktyczna ocena bezpieczeństwa (462)
- A.8. Wypracowania pisemne (462)
- A.9. Lektura tematu (463)

Dodatek B: Standardy i organizacje standaryzacyjne (465)

- B.1. Znaczenie standardów (466)
- B.2. Standardy internetowe i społeczność internetu (467)
- B.3. Narodowy Instytut Standaryzacji i Technologii (NIST) (471)

Dodatek C: Protokół TCP/IP i architektura OSI (473)

- C.1. Protokoły i architektury protokołów (474)
- C.2. Architektura protokołu TCP/IP (476)
- C.3. Rola protokołu IP (483)
- C.4. Protokół IP w wersji 4 (IPv4) (486)
- C.5. Protokół IP w wersji 6 (IPv6) (487)
- C.6. Architektura protokołów OSI (492)

Dodatek D: Algorytm ZIP (495)

- D.1. Algorytm kompresji (497)
- D.2. Algorytm dekompresji (498)

Dodatek E: Generowanie liczb losowych w PGP (501)

- E.1. Generowanie liczb prawdziwie losowych (502)
- E.2. Generowanie liczb pseudolosowych (502)

Dodatek F: Międzynarodowy alfabet wzorcowy (IRA) (505)

Słownik (511)

Bibliografia (521)

Skorowidz (537)