Przedmowa (7)

- WWW - obietnice i zagrożenia (8)
- Kilka słów o książce (9)
- Konwencje typograficzne (15)
- Komentarze i pytania (16)
- Informacje dostępne w Internecie (16)
- Podziękowania (16)

I. Wprowadzenie (19)
1. Bezpieczeństwo WWW w zarysie (21)

- Bezpieczeństwo WWW w pigułce (21)
- Problem bezpieczeństwa WWW (27)
- Karty kredytowe, szyfrowanie i WWW (31)
- Firewall jako element rozwiązania problemu (38)
- Zarządzanie ryzykiem (42)

II. Bezpieczeństwo użytkownika (43)
2. "Dziurawe" przeglądarki, czyli ewolucja zagrożeń (45)

- Historia przeglądarek (45)
- Ataki poprzez dane (51)
- Litania błędów, czyli usterki implementacyjne (54)

3. Java i JavaScript (57)

- Java (57)
- JavaScript (72)
- Ataki typu blokady usługi (74)
- Podszywanie się przy użyciu JavaScriptu (79)
- Wnioski (83)

4. Kopiowanie kodu maszynowego - komponenty ActiveX i moduły rozszerzające (85)

- Kiedy dobre przeglądarki schodzą na złą drogę (85)
- Moduły rozszerzające dla przeglądarki Netscape Communicator (87)
- ActiveX i Authenticode (91)
- Zagrożenia wiążące się z kopiowaniem kodu (95)
- Czy Authenticode jest dobrym rozwiązaniem? (98)
- Zwiększanie bezpieczeństwa kopiowanego kodu (103)

5. Prywatność (105)

- Pliki dzienników (105)
- Cookies (108)
- Informacje o charakterze osobistym (112)
- Anonimizacja (114)
- Niepożądane ujawnianie informacji (116)

III. Certyfikaty cyfrowe (117)
6. Metody identyfikacji cyfrowej (119)

- Identyfikacja (119)
- Infrastruktura kluczy publicznych (129)
- Problemy napotykane przy tworzeniu infrastruktury kluczy publicznych (136)
- Dziesięć pytań o strategię (143)

7. Urzędy certyfikacji i certyfikaty serwerów (149)

- Certyfikaty dziś (149)
- Certyfikaty urzędów certyfikacji (151)
- Certyfikaty serwerów (154)
- Wnioski (169)

8. Certyfikaty cyfrowe użytkownika (171)

- Certyfikaty użytkownika (171)
- Wycieczka po witrynie VeriSign Digital ID Center (173)

9. Podpisywanie kodu i technologia Authenticode (189)

- Komu potrzebne jest podpisywanie kodu? (189)
- Technologia Authenticode firmy Microsoft (192)
- Uzyskanie certyfikatu wydawcy oprogramowania (201)
- Inne metody podpisywania kodu (202)

IV. Kryptografia (203)
10. Podstawy kryptografii (205)

- Co to jest kryptografia? (205)
- Algorytmy oparte o klucz symetryczny (211)
- Algorytmy oparte o klucz publiczny (217)
- Skróty wiadomości (220)
- Infrastruktura kluczy publicznych (225)

11. Kryptografia i WWW (227)

- Kryptografia a bezpieczeństwo w sieci WWW (227)
- Współczesne systemy kryptograficzne (230)
- Prawne ograniczenia stosowania kryptografii w USA (237)
- Prawne ograniczenia stosowania kryptografii na świecie (246)

12. Protokoły SSL i TLS (251)

- Czym jest SSL? (251)
- Rozwój standardu TLS (261)
- SSL z punktu widzenia użytkownika (262)

V. Bezpieczeństwo serwerów WWW (269)
13. Bezpieczeństwo hosta i witryny (271)

- Zagrożenia wczoraj i dziś (271)
- Współczesne problemy bezpieczeństwa hostów (273)
- Minimalizacja ryzyka poprzez ograniczanie dostępnych usług (286)
- Bezpieczna aktualizacja zawartości (288)
- Bazy danych (291)
- Bezpieczeństwo fizyczne (291)

14. Kontrola dostępu do serwera (293)

- Strategie kontroli dostępu (293)
- Implementacja kontroli dostępu za pomocą znaczników (298)
- Prosty system kontroli dostępu (304)

15. Bezpieczne programowanie CGI i API (311)

- Zagrożenia płynące z rozszerzalności (312)
- Reguły dobrego programowania (318)
- Reguły dla konkretnych języków programowania (323)
- Jak pisać skrypty CGI wykonywane z rozszerzonymi uprawnieniami? (326)
- Wnioski (328)

VI. Handel a społeczeństwo (329)
16. Płatności cyfrowe (331)

- Charga-plates, Diner's Club i karty kredytowe (331)
- Internetowe systemy płatnicze (340)
- Jak ocenić system płatniczy oparty na kartach kredytowych? (350)

17. Oprogramowanie blokujące i cenzura w Internecie (353)

- Oprogramowanie blokujące (354)
- System PICS (357)
- System RSACi (364)

VII. Dodatki (367)
A. Tworzenie i instalowanie certyfikatów serwera WWW (369)

- Pobranie i instalacja serwera WWW (370)
- Serwer Apache-SSL (371)

B. Protokół SSL 3.0 (387)

- Historia (387)
- Warstwa rekordów protokołu SSL 3.0 (388)
- Protokoły składowe SSL 3.0 (389)
- Faza uzgadniania w protokole SSL 3.0 (391)
- Rozdział 1: Pakiet SSLeay (398)

C. Specyfikacja PICS (413)

- Urzędy klasyfikacji (413)
- Etykiety PICS (415)

D. Materiały źródłowe (421)

- Materiały elektroniczne (421)
- Grupy dyskusyjne Usenet (425)
- Materiały drukowane (435)

Skorowidz (441)