

Wstęp (9)

Rozdział 1. Zagrożenia czyhające na programistów (11)

- 1.1. Dawno, dawno temu w świecie gier (11)
- 1.2. Moje przygody z grą Metal Knights (14)
- 1.3. Niebezpieczny edytor map, czyli słabe punkty (16)
- 1.4. A jak to robią w Diablo... czyli coś o bezpieczeństwie aplikacji sieciowych (19)
- 1.5. Rodzaje oszustw i naruszeń bezpieczeństwa (21)
 - o 1.5.1. Nieuprawnione użycie bądź kopiowanie programu (21)
 - o 1.5.2. Nielegalna podmiana autorstwa kodu (23)
 - o 1.5.3. Nieuprawniona modyfikacja kodu (23)
- 1.6. Pirat, Robin Hood, kraker? (24)
- 1.7. Czy ja także mam myśleć o zabezpieczeniach? (25)
- 1.8. Czym się różni kraker od złodzieja samochodów? (27)
- Zadania do samodzielnego wykonania (30)
- Pytania kontrolne (31)

Rozdział 2. Proste metody zabezpieczenia programów (33)

- 2.1. Wstęp (33)
- 2.2. Numer seryjny (33)
- 2.3. CrackMe - przykłady słabości prostych zabezpieczeń przed nieuprawnionym użytkowaniem programu (35)
 - o 2.3.1. CrackMe1 (35)
 - o 2.3.2. CrackMe2 (42)
- 2.4. Gotowe systemy zabezpieczania aplikacji przed nieuprawnionym użyciem (44)
 - o Przegląd systemów zabezpieczających dostępnych na rynku (47)
- 2.5. Zakończenie (50)
- Zadania do samodzielnego wykonania (51)
- Pytania kontrolne (51)

Rozdział 3. Teoria szyfrowania. Algorytmy szyfrujące w praktyce (53)

- 3.1. Wstęp (53)
- 3.2. Szyfrowanie i kodowanie informacji (53)
- 3.3. Historyczne algorytmy szyfrowania i kodowania (54)
 - o 3.3.1. Początki (54)
 - o 3.3.2. Szyfry przestawieniowe i podstawieniowe, szyfr Cezara (55)
 - o 3.3.3. Szyfry polialfabetyczne (55)
 - o 3.3.4. Zasada Kerckhoffs'a (56)
- 3.4. Współczesne algorytmy szyfrowania (56)
 - o 3.4.1. Rozwój algorytmów szyfrowania (56)
 - o 3.4.2. Algorytmy symetryczne. Algorytm RC4 (57)
 - o 3.4.3. Szyfrowanie symetryczne, algorytm DES (61)
 - o 3.4.4. Szyfrowanie symetryczne, algorytm AES (61)
 - o 3.4.5. Szyfrowanie asymetryczne, algorytm RSA (61)
 - o 3.4.6. Podpis cyfrowy (63)
 - o 3.4.7. Szyfr z kluczem jednorazowym (63)
- 3.5. Algorytmy wyznaczające sygnatury (skrót) danych (64)
 - o 3.5.1. Algorytm wyznaczania CRC (64)

- o 3.5.2. Algorytm MD5 (65)
 - o 3.5.3. Algorytm SHA-1 (65)
- 3.6. Generatory liczb pseudolosowych (69)
- 3.7. Do czego może służyć szyfrowanie w zabezpieczaniu programów? (70)
- Zadania do samodzielnego wykonania (71)
- Pytania kontrolne (71)

Rozdział 4. Zabezpieczanie programów sieciowych na przykładzie języka PHP (73)

- 4.1. Wstęp (73)
- 4.2. Obsługa danych z zewnątrz (74)
- 4.3. Przekazywanie danych między skryptami (75)
- 4.4. Uwierzytelnianie w PHP (76)
- 4.5. Niebezpieczne konstrukcje języka (79)
 - o 4.5.1. Konstrukcja include (\$plik) (80)
 - o 4.5.2. eval(\$code), konstrukcja \$\$ (81)
 - o 4.5.3. fopen(\$url) (82)
- 4.6. Bezpieczna obsługa błędów (83)
- 4.7. Bezpieczeństwo systemu plików (84)
- 4.8. Cross site scripting (85)
- 4.9. Wstrzykiwanie kodu SQL (86)
 - o 4.9.1. Wstrzykiwanie kodu SQL - przykład 1. (87)
 - o 4.9.2. Wstrzykiwanie kodu SQL - przykład 2. (90)
 - o 4.9.3. Użycie PDO (91)
 - o 4.9.4. Ataki wielofazowe (92)
 - o 4.9.5. Sposoby ochrony (92)
- 4.10. Wstrzykiwanie poleceń systemowych (shell injection) (93)
- 4.11. Wstrzykiwanie zawartości e-mail (e-mail injection) (94)
- 4.12. Cross site request forgery (95)
- 4.13. Przejęcie kontroli nad sesją (session fixation) (97)
- 4.14. Session poisoning (101)
 - o 4.14.1. Przechowywanie stanu aplikacji w niezabezpieczonych miejscach (101)
 - o 4.14.2. Przypisanie wartości do zmiennej sesyjnej o nazwie stworzonej na podstawie danych od użytkownika (104)
 - o 4.14.3. Podmiana sekwencji wywołań przez włamywacza. Problem wyścigu (105)
 - o 4.14.4. Używanie tych samych zmiennych sesyjnych do różnych celów (106)
 - o 4.14.5. Zmienne sesyjne nie są gwarancją bezpieczeństwa (108)
- 4.15. Ataki typu DOS i DDOS (110)
- 4.16. Dyrektywa register_globals (112)
- 4.17. Narzędzie zaciemniające kod źródłowy języka PHP (114)
- Zakończenie (116)
- Zadania do samodzielnego wykonania (116)
- Pytania kontrolne (116)

Rozdział 5. Zaawansowane metody zabezpieczania programów (121)

- 5.1. Wstęp (121)
- 5.2. Klucze rejestracyjne przypisane do użytkownika (122)

- o 5.2.1. Idea kluczy rejestracyjnych przypisanych do użytkownika (122)
 - o 5.2.2. Typowe techniki (124)
 - o 5.2.3. Tworzenie kluczy rejestracyjnych w aplikacjach sieciowych (125)
- 5.3. Samotestujący się program (126)
 - o 5.3.1. Testowanie integralności programu gwarancją jego oryginalności (126)
 - o 5.3.2. Przykład - weryfikacja integralności pliku wykonywalnego (127)
 - o 5.3.3. Przykład - weryfikacja integralności kodu programu (132)
- 5.4. Sprawdzanie integralności danych (135)
 - o 5.4.1. Ukryj moje dane (136)
 - o 5.4.2. Testowanie integralności danych ulegających zmianom (137)
 - o 5.4.3. Wersje czasowe oprogramowania - kłopoty z shareware (138)
 - o 5.4.4. Bezpieczne przechowywanie danych - przykład (140)
- 5.5. Samomodyfikujący się program (144)
 - o 5.5.1. Samomodyfikujący się program. Brzydka sztuczka czy eleganckie zabezpieczenie? (144)
 - o 5.5.2. Sabotaż, czyli jak ukarać krakera? (146)
 - o 5.5.3. "Za 5 sekund ten program ulegnie samozniszczeniu" - automatyczna deinstalacja programu (147)
 - o 5.5.4. "Kod o ograniczonej przydatności do wykonania" (148)
- 5.6. Klucz programowy (150)
 - o 5.6.1. Klucz programowy - przykład (151)
 - o 5.6.2. Deszyfrowanie fragmentów programu w trakcie jego działania (156)
 - o 5.6.3. Przykład programu deszyfrującego się w trakcie działania (158)
- 5.7. Zaciemnianie kodu i danych programu (161)
 - o 5.7.1. Czy to wciąż open source? Zaciemnianie kodu jako metoda obronna (161)
- 5.8. Zabezpieczenia. Jak to w praktyce wprowadzić w życie (163)
 - o 5.8.1. Zabezpieczenia a etapy produkcji (163)
 - o 5.8.2. Generator zabezpieczeń (164)
- Zadania do samodzielnego wykonania (165)
- Pytania kontrolne (166)

Rozdział 6. Zabezpieczenie programów przed debuggerami (167)

- 6.1. Wstęp (167)
- 6.2. Wykrywanie debuggerów (168)
- 6.3. Utrudnianie debugowania (169)
 - o 6.3.1. Wstawki kodu utrudniające debugowanie (169)
 - o 6.3.2. Generator wstawek kodu utrudniających debugowanie (172)
- Zadania do samodzielnego wykonania (175)
- Pytania kontrolne (175)

Rozdział 7. Wykorzystanie internetu do zabezpieczania programów (177)

- 7.1. Wstęp (177)
- 7.2. Rejestracja programu przez internet (178)
- 7.3. Aktywacja numeru seryjnego przez internet (179)
- 7.4. Kontrola użytkownika aplikacji z częściowym dostępem do internetu (180)
- 7.5. Weryfikacja prawidłowej pracy aplikacji przez sieć (181)
- 7.6. Przechowywanie poufnych danych użytkownika (182)

- 7.7. Deszyfrowanie programu w trakcie działania a internet (183)
- 7.8. Fragmentaryczne dane pobierane z internetu (185)
- 7.9. Przesyłanie informacji o programie do centralnego serwera (186)
 - o 7.9.1. Totalna inwigilacja? Rejestrowanie informacji o zachowaniu programu i użytkownika (186)
 - o 7.9.2. Zdalne sprawdzanie tożsamości użytkownika (188)
 - o 7.9.3. Zdalne i lokalne blokowanie działania programu sterowanego danymi z centralnego serwera (191)
- 7.10. Wirtualne wybory (192)
- Zadania do samodzielnego wykonania (196)
- Pytania kontrolne (196)

Rozdział 8. Zabezpieczanie programów przy użyciu kluczy sprzętowych oraz technik biometrycznych (197)

- 8.1. Wstęp (197)
- 8.2. Zabezpieczenie aplikacji za pomocą kluczy sprzętowych (198)
 - o 8.2.1. Karty magnetyczne i elektroniczne (198)
 - o 8.2.2. Podpis cyfrowy na trwałym nośniku (199)
 - o 8.2.3. Klucze sprzętowe w zabezpieczaniu oprogramowania (200)
- 8.3. Technologie GPS i RFID, geolokalizacja (201)
 - o 8.3.1. Technologie GPS i RFID (201)
 - o 8.3.2. Problemy etyczne i moralne postępu technicznego związanego z lokalizacją i kontrolą użytkowników (202)
- 8.4. Weryfikacja tożsamości za pomocą technik biometrycznych (203)
 - o 8.4.1. Techniki biometryczne (203)
 - o 8.4.2. Indywidualne oprogramowanie (204)
- 8.5. Szpiegostwo elektroniczne (204)
 - o 8.5.1. Włamania do sieci bezprzewodowych (204)
 - o 8.5.2. Przechwytywanie fal elektromagnetycznych (205)
- Pytania kontrolne (206)

Rozdział 9. Tworzenie bezpiecznych aplikacji w środowisku .NET (207)

- 9.1. Wstęp (207)
- 9.2. Autoryzacja oparta na uprawnieniach i rolach (Role-Based Authorization) (208)
 - o 9.2.1. Uprawnienia, interfejs IPermission, klasa Principal (209)
 - o 9.2.2. Autoryzacja nakazowa oparta na rolach (Imperative Role-Based Security) (210)
 - o 9.2.3. Autoryzacja deklaracyjna oparta na rolach (Declarative Role-Based Security) (213)
- 9.3. Zabezpieczenie dostępu kodu do zasobów (Code Access Security) (215)
 - o 9.3.1. Nakazowe zabezpieczenie dostępu kodu do zasobów (Imperative Code Access Security) (215)
 - o 9.3.2. Deklaracyjne zabezpieczenie dostępu kodu do zasobów (Declarative Code Access Security) (219)
 - o 9.3.3. Poziomy reguł bezpieczeństwa (Security Policy Level) (220)
 - o 9.3.4. Narzędzie The Code Access Security Policy Utility - caspol.exe (221)
- 9.4. Bezpieczeństwo ASP.NET (222)
 - o 9.4.1. Metody uwierzytelniania w ASP.NET (222)

- o 9.4.2. Dostęp anonimowy (223)
- o 9.4.3. Uwierzytelnianie systemu Windows (223)
- o 9.4.4. Uwierzytelnianie przy użyciu formularza (226)
- o 9.4.5. Uwierzytelnianie za pomocą .NET Passport (228)
- o 9.4.6. Bezpieczna komunikacja za pomocą SSL (228)
- 9.5. Tworzenie silnych nazw podzespołom (230)
- Zadania do samodzielnego wykonania (231)
- Pytania kontrolne (232)

Rozdział 10. Bezpieczny Program (235)

- 10.1. Wstęp (235)
- 10.2. Opis programu (236)
- 10.3. Przegląd kodu źródłowego (238)
 - o 10.3.1. BezpiecznyProgram.exe (238)
 - o 10.3.2. ZabezpieczBP.exe (245)
 - o 10.3.3. StwórzKluczBP.exe (246)
- 10.4. Wnioski (247)
- Zadania do samodzielnego wykonania (249)

Rozdział 11. Psychologiczna strona bezpieczeństwa (251)

- 11.1. Wstęp (251)
- 11.2. Wpływ architektury programu na jego bezpieczeństwo (251)
- 11.3. "Tylne wejścia" i kod tymczasowy (253)
- 11.4. Użycie gotowego kodu (254)
- 11.5. Open source (256)
- 11.6. Tańczące świnki kontra bezpieczeństwo (257)
- 11.7. Security by obscurity - zabezpieczanie przez zaciemnianie (258)
- 11.8. Karanie włamywacza (260)
- 11.9. Brzytwa Ockhama (261)
- 11.10. Użycie socjotechniki (261)
- 11.11. Nie poprawiaj włamywacza (262)
- 11.12. Walka ze script kiddies (263)
- 11.13. Ochrona przed automatami (264)
- 11.14. Ataki z wewnątrz (267)
- 11.15. Łącuch a sieć zabezpieczeń (267)
- 11.16. Całościowe spojrzenie na problem bezpieczeństwa (268)
- Pytania kontrolne (270)

Podsumowanie (273)

Odpowiedzi do pytań kontrolnych (281)

Słowniczek pojęć (293)

Skorowidz (301)