

# Spis treści

|                                                                                     |           |
|-------------------------------------------------------------------------------------|-----------|
| Przedmowa.....                                                                      | 11        |
| Wstęp .....                                                                         | 15        |
| <b>1. Bezpieczna inicjalizacja.....</b>                                             | <b>25</b> |
| 1.1. Zabezpieczanie środowiska pracy programu.....                                  | 25        |
| 1.2. Ograniczanie uprawnień w systemach Windows.....                                | 32        |
| 1.3. Rezygnacja z uprawnień w programach setuid.....                                | 40        |
| 1.4. Ograniczanie ryzyka związanego z separacją uprawnień.....                      | 45        |
| 1.5. Bezpieczne zarządzanie deskryptorami plików.....                               | 48        |
| 1.6. Bezpieczne tworzenie procesu potomnego.....                                    | 50        |
| 1.7. Bezpieczne uruchamianie programów zewnętrznych w systemach Unix.....           | 53        |
| 1.8. Bezpieczne uruchamianie zewnętrznych programów w systemach Windows.....        | 58        |
| 1.9. Wylączenie rzutów pamięci w przypadku wystąpienia błędu.....                   | 60        |
| <b>2. Kontrola dostępu.....</b>                                                     | <b>63</b> |
| 2.1. Model kontroli dostępu w systemach Unix.....                                   | 63        |
| 2.2. Model kontroli dostępu w systemach Windows.....                                | 66        |
| 2.3. Określanie, czy dany użytkownik ma dostęp do danego pliku w systemie Unix..... | 68        |
| 2.4. Określanie, czy dany katalog jest bezpieczny.....                              | 70        |
| 2.5. Bezpieczne usuwanie plików.....                                                | 73        |
| 2.6. Bezpieczne uzyskiwanie dostępu do informacji o pliku.....                      | 79        |
| 2.7. Ograniczone prawa dostępu do nowych plików w systemach Unix.....               | 80        |
| 2.8. Blokowanie plików.....                                                         | 83        |
| 2.9. Synchronizacja dostępu procesów do zasobów w systemach Unix.....               | 85        |
| 2.10. Synchronizacja dostępu procesów do zasobów w systemach Windows.....           | 89        |
| 2.11. Tworzenie plików tymczasowych.....                                            | 91        |
| 2.12. Ograniczanie dostępu do systemu plików w systemach Unix.....                  | 94        |
| 2.13. Ograniczanie dostępu do systemu plików i sieci w systemie FreeBSD.....        | 95        |
| <b>3. Sprawdzanie poprawności danych wejściowych .....</b>                          | <b>97</b> |
| 3.1. Podstawowe techniki sprawdzania poprawności danych.....                        | 98        |
| 3.2. Zapobieganie atakom z wykorzystaniem funkcji formatujących.....                | 102       |
| 3.3. Zapobieganie przepełnieniom bufora.....                                        | 105       |

|                                                                                                                     |            |
|---------------------------------------------------------------------------------------------------------------------|------------|
| 3.4. Stosowanie biblioteki SafeStr                                                                                  | 113        |
| 3.5. Zapobieganie koercji liczb całkowitych i problemowi przekroczenia zakresu                                      | 116        |
| 3.6. Bezpieczne stosowanie zmiennych środowiskowych                                                                 | 120        |
| 3.7. Sprawdzanie poprawności nazw plików i ścieżek                                                                  | 125        |
| 3.8. Obsługa kodowania URL                                                                                          | 127        |
| 3.9. Sprawdzanie poprawności adresów poczty elektronicznej                                                          | 129        |
| 3.10. Ochrona przed atakami typu cross-site scripting (XSS)                                                         | 131        |
| 3.11. Ochrona przed atakami typu SQL injection                                                                      | 135        |
| 3.12. Wykrywanie nieprawidłowych znaków UTF-8                                                                       | 138        |
| 3.13. Zapobieganie przepełnieniom deskryptorów plików podczas stosowania funkcji select()                           | 140        |
| <b>4. Podstawy kryptografii symetrycznej</b>                                                                        | <b>145</b> |
| 4.1. Reprezentacje kluczy wykorzystywanych w algorytmach kryptograficznych                                          | 146        |
| 4.2. Generowanie losowych kluczy symetrycznych                                                                      | 148        |
| 4.3. Szesnastkowe reprezentacje kluczy binarnych (lub innych nieprzetworzonych danych)                              | 149        |
| 4.4. Przekształcanie szesnastkowych kluczy ASCII (lub innych szesnastkowych danych ASCII) na postać binarną         | 151        |
| 4.5. Kodowanie Base64                                                                                               | 152        |
| 4.6. Dekodowanie łańcucha zakodowanego zgodnie ze standardem Base64                                                 | 154        |
| 4.7. Reprezentowanie kluczy (lub dowolnych innych danych binarnych) w postaci tekstu zapisanego w języku angielskim | 157        |
| 4.8. Przekształcanie kluczy tekstowych na klucze binarne                                                            | 159        |
| 4.9. Stosowanie argumentów salt, jednorazowych identyfikatorów i wektorów inicjalizacji                             | 161        |
| 4.10. Generowanie kluczy symetrycznych na bazie hasel                                                               | 165        |
| 4.11. Algorytmiczne generowanie kluczy symetrycznych na bazie jednego tajnego klucza głównego                       | 171        |
| 4.12. Szyfrowanie okrojonego zbioru znaków                                                                          | 175        |
| 4.13. Bezpieczne zarządzanie materiałem klucza                                                                      | 178        |
| 4.14. Badanie czasu działania algorytmów kryptograficznych                                                          | 179        |
| <b>5. Szyfrowanie symetryczne</b>                                                                                   | <b>185</b> |
| 5.1. Podejmowanie decyzji w kwestii stosowania wielu algorytmów szyfrujących                                        | 185        |
| 5.2. Wybór najlepszego algorytmu szyfrującego                                                                       | 186        |
| 5.3. Wybór właściwej długości klucza                                                                                | 190        |
| 5.4. Wybór trybu pracy szyfru blokowego                                                                             | 193        |
| 5.5. Stosowanie podstawowych operacji szyfru blokowego                                                              | 203        |
| 5.6. Stosowanie ogólnej implementacji trybu CBC                                                                     | 207        |
| 5.7. Stosowanie ogólnej implementacji trybu CFB                                                                     | 217        |
| 5.8. Stosowanie ogólnej implementacji trybu OFB                                                                     | 224        |

|                                                                                                                                            |            |
|--------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 5.9. Stosowanie ogólnej implementacji trybu CTR                                                                                            | 228        |
| 5.10. Stosowanie trybu szyfrowania CWC                                                                                                     | 233        |
| 5.11. Ręczne dodawanie i sprawdzanie dopełniania szyfru                                                                                    | 237        |
| 5.12. Wyznaczanie z góry strumienia klucza w trybach OFB, CTR, CCM i CWC (oraz w szyfrach strumieniowych)                                  | 239        |
| 5.13. Zrównoleganie szyfrowania i deszyfrowania w trybach, które na takie działania zezwalają (bez wprowadzania ewentualnych niezgodności) | 240        |
| 5.14. Zrównoleganie szyfrowania i deszyfrowania w dowolnych trybach (a więc z możliwością wprowadzania ewentualnych niezgodności)          | 244        |
| 5.15. Szyfrowanie zawartości plików lub całych dysków                                                                                      | 245        |
| 5.16. Stosowanie wysokopoziomowych, odpornych na błędy interfejsów API dla operacji szyfrowania i deszyfrowania                            | 249        |
| 5.17. Konfiguracja szyfru blokowego (dla trybów szyfrowania CBC, CFB, OFB oraz ECB) w pakiecie OpenSSL                                     | 254        |
| 5.18. Stosowanie szyfrów ze zmienną długością klucza w pakiecie OpenSSL                                                                    | 259        |
| 5.19. Wyłączanie mechanizmu dopełniania w szyfrach pakietu OpenSSL pracujących w trybie CBC                                                | 260        |
| 5.20. Dodatkowa konfiguracja szyfrów w pakiecie OpenSSL                                                                                    | 261        |
| 5.21. Sprawdzanie właściwości konfiguracji szyfru w pakiecie OpenSSL                                                                       | 262        |
| 5.22. Wykonywanie niskopoziomowego szyfrowania i deszyfrowania w pakiecie OpenSSL                                                          | 264        |
| 5.23. Konfiguracja i stosowanie szyfru RC4                                                                                                 | 267        |
| 5.24. Stosowanie szyfrów z kluczem jednorazowym                                                                                            | 270        |
| 5.25. Stosowanie szyfrowania symetrycznego z wykorzystaniem CryptoAPI firmy Microsoft                                                      | 271        |
| 5.26. Tworzenie obiektu klucza interfejsu CryptoAPI na bazie dowolnych danych klucza                                                       | 277        |
| 5.27. Uzyskiwanie surowych danych klucza z obiektu klucza interfejsu CryptoAPI                                                             | 280        |
| <b>6. Funkcje skrótu i uwierzytelnianie wiadomości</b>                                                                                     | <b>283</b> |
| 6.1. Zrozumienie podstaw funkcji skrótu i kodu uwierzytelniającego wiadomość MAC                                                           | 283        |
| 6.2. Decydowanie, czy obsługiwać wiele skrótów wiadomości lub kodów MAC                                                                    | 287        |
| 6.3. Wybór kryptograficznego algorytmu skrótu                                                                                              | 288        |
| 6.4. Wybór kodu uwierzytelnienia wiadomości                                                                                                | 292        |
| 6.5. Przyrostowe tworzenie skrótów danych                                                                                                  | 296        |
| 6.6. Tworzenie skrótu z pojedynczego łańcucha znaków                                                                                       | 300        |
| 6.7. Używanie skrótu kryptograficznego                                                                                                     | 302        |
| 6.8. Wykorzystanie identyfikatora jednorazowego do obrony przed atakami wykorzystującymi paradoks dnia urodzin                             | 303        |
| 6.9. Sprawdzanie spójności wiadomości                                                                                                      | 307        |
| 6.10. Używanie HMAC                                                                                                                        | 309        |
| 6.11. Używanie OMAC (prostego kodu MAC opartego na szyfrze blokowym)                                                                       | 312        |

|                                                                                                                              |            |
|------------------------------------------------------------------------------------------------------------------------------|------------|
| 6.12. Używanie HMAC lub OMAC z identyfikatorem jednorazowym                                                                  | 317        |
| 6.13. Używanie kodu MAC, który jest wystarczająco szybki<br>w realizacji programowej i sprzętowej                            | 318        |
| 6.14. Używanie kodu MAC zoptymalizowanego<br>do szybszego działania w realizacji programowej                                 | 319        |
| 6.15. Konstruowanie funkcji skrótu z szyfru blokowego                                                                        | 322        |
| 6.16. Używanie szyfru blokowego do budowy mocnej funkcji skrótu                                                              | 325        |
| 6.17. Używanie mniejszych znaczników MAC                                                                                     | 329        |
| 6.18. Szyfrowanie z zachowaniem spójności wiadomości                                                                         | 329        |
| 6.19. Tworzenie własnego kodu MAC                                                                                            | 331        |
| 6.20. Szyfrowanie za pomocą funkcji skrótu                                                                                   | 332        |
| 6.21. Bezpieczne uwierzytelnianie kodu MAC (obrona przed atakami<br>związanymi z przechwytywaniem i powtarzaniem odpowiedzi) | 334        |
| 6.22. Przetwarzanie równoległe kodu MAC                                                                                      | 335        |
| <b>7. Kryptografia z kluczem publicznym</b>                                                                                  | <b>337</b> |
| 7.1. Określanie sytuacji, w których należy stosować techniki kryptografii<br>z kluczem publicznym                            | 339        |
| 7.2. Wybór algorytmu z kluczem publicznym                                                                                    | 342        |
| 7.3. Wybór rozmiarów kluczy publicznych                                                                                      | 343        |
| 7.4. Przetwarzanie wielkich liczb                                                                                            | 346        |
| 7.5. Generowanie liczby pierwszej i sprawdzanie<br>czy dana liczba jest liczbą pierwszą                                      | 355        |
| 7.6. Generowanie pary kluczy szyfru RSA                                                                                      | 358        |
| 7.7. Oddzielanie kluczy publicznych i prywatnych w pakiecie OpenSSL                                                          | 361        |
| 7.8. Konwertowanie łańcuchów binarnych na postać liczb całkowitych<br>na potrzeby szyfru RSA                                 | 362        |
| 7.9. Przekształcanie liczb całkowitych do postaci łańcuchów binarnych<br>na potrzeby szyfru RSA                              | 363        |
| 7.10. Podstawowa operacja szyfrowania za pomocą klucza publicznego<br>algorytmu RSA                                          | 364        |
| 7.11. Podstawowa operacja deszyfrowania za pomocą klucza prywatnego<br>algorytmu RSA                                         | 368        |
| 7.12. Podpisywanie danych za pomocą klucza prywatnego szyfru RSA                                                             | 370        |
| 7.13. Weryfikacja cyfrowo podpisanych danych za pomocą klucza publicznego<br>algorytmu RSA                                   | 374        |
| 7.14. Bezpieczne podpisywanie i szyfrowanie danych za pomocą algorytmu RSA                                                   | 376        |
| 7.15. Wykorzystywanie algorytmu DSA                                                                                          | 381        |
| 7.16. Reprezentowanie kluczy publicznych i certyfikatów<br>w postaci łańcuchów binarnych (zgodnie z regułami kodowania DER)  | 386        |
| 7.17. Reprezentowanie kluczy i certyfikatów w postaci tekstu<br>(zgodnie z regułami kodowania PEM)                           | 390        |

|                                                                                                           |            |
|-----------------------------------------------------------------------------------------------------------|------------|
| <b>8. Uwierzytelnianie i wymiana kluczy.....</b>                                                          | <b>397</b> |
| 8.1. Wybór metody uwierzytelniania                                                                        | 397        |
| 8.2. Uzyskiwanie informacji o użytkownikach i grupach w systemach uniksowych                              | 407        |
| 8.3. Uzyskiwanie informacji o użytkownikach i grupach w systemach Windows                                 | 410        |
| 8.4. Ograniczanie dostępu na podstawie nazwy maszyny lub adresu IP                                        | 413        |
| 8.5. Generowanie losowych haseł i wyrażeń hasłowych                                                       | 420        |
| 8.6. Sprawdzanie odporności haseł na ataki                                                                | 424        |
| 8.7. Monitorowanie o hasło                                                                                | 425        |
| 8.8. Kontrola nad nieudanymi próbami uwierzytelnienia                                                     | 430        |
| 8.9. Uwierzytelnianie oparte na hasłach z użyciem funkcji crypt()                                         | 432        |
| 8.10. Uwierzytelnianie oparte na hasłach z użyciem funkcji MD5-MCF                                        | 434        |
| 8.11. Uwierzytelnianie oparte na hasłach z użyciem funkcji PBKDF2                                         | 439        |
| 8.12. Uwierzytelnianie przy użyciu modułów PAM                                                            | 442        |
| 8.13. Uwierzytelnianie za pomocą systemu Kerberos                                                         | 445        |
| 8.14. Uwierzytelnianie z wykorzystaniem mechanizmu HTTP Cookies                                           | 449        |
| 8.15. Uwierzytelnianie oraz wymiana kluczy oparte na hasłach                                              | 452        |
| 8.16. Przeprowadzanie uwierzytelnionej wymiany klucza przy użyciu algorytmu RSA                           | 459        |
| 8.17. Użycie podstawowego protokołu uzgadniania klucza metodą Diffiego-Hellmana                           | 461        |
| 8.18. Wspólne użycie metody Diffiego-Hellmana i algorytmu DSA                                             | 466        |
| 8.19. Minimalizacja okresu podatności na ataki w przypadku uwierzytelniania bez użycia infrastruktury PKI | 467        |
| 8.20. Zapewnianie przyszłego bezpieczeństwa w systemie symetrycznym                                       | 473        |
| 8.21. Zapewnianie przyszłego bezpieczeństwa w systemie z kluczem publicznym                               | 474        |
| 8.22. Potwierdzanie żądań za pomocą wiadomości poczty elektronicznej                                      | 476        |
| <b>9. Komunikacja sieciowa.....</b>                                                                       | <b>483</b> |
| 9.1. Tworzenie klienta SSL                                                                                | 484        |
| 9.2. Tworzenie serwera SSL                                                                                | 486        |
| 9.3. Używanie mechanizmu buforowania sesji w celu zwiększenia wydajności serwerów SSL                     | 489        |
| 9.4. Zabezpieczanie komunikacji sieciowej na platformie Windows przy użyciu interfejsu WinInet API        | 492        |
| 9.5. Aktywowanie protokołu SSL bez modyfikowania kodu źródłowego                                          | 496        |
| 9.6. Używanie szyfrowania standardu Kerberos                                                              | 498        |
| 9.7. Komunikacja międzyprocesowa przy użyciu gniazd                                                       | 503        |
| 9.8. Uwierzytelnianie przy użyciu uniksowych gniazd domenowych                                            | 509        |
| 9.9. Zarządzanie identyfikatorami sesji                                                                   | 512        |
| 9.10. Zabezpieczanie połączeń bazodanowych                                                                | 513        |

|                                                                                                       |            |
|-------------------------------------------------------------------------------------------------------|------------|
| 9.11. Używanie wirtualnych sieci prywatnych<br>w celu zabezpieczenia połączeń sieciowych              | 516        |
| 9.12. Tworzenie uwierzytelnionych bezpiecznych kanałów bez użycia SSL                                 | 517        |
| <b>10. Infrastruktura klucza publicznego</b>                                                          | <b>527</b> |
| 10.1. Podstawy infrastruktury klucza publicznego                                                      | 527        |
| 10.2. Otrzymywanie certyfikatu                                                                        | 538        |
| 10.3. Używanie certyfikatów głównych                                                                  | 543        |
| 10.4. Podstawy metodologii weryfikacji certyfikatów X.509                                             | 546        |
| 10.5. Przeprowadzanie weryfikacji certyfikatów X.509 przy użyciu OpenSSL                              | 548        |
| 10.6. Przeprowadzanie weryfikacji certyfikatów X.509<br>przy użyciu interfejsu CryptoAPI              | 553        |
| 10.7. Weryfikowanie certyfikatu pochodzącego od partnera komunikacji SSL                              | 558        |
| 10.8. Dodawanie mechanizmu sprawdzania nazwy hosta<br>do procesu weryfikacji certyfikatu              | 562        |
| 10.9. Używanie list akceptacji w celu weryfikowania certyfikatów                                      | 566        |
| 10.10. Pobieranie list unieważnionych certyfikatów przy użyciu OpenSSL                                | 569        |
| 10.11. Pobieranie list unieważnionych certyfikatów przy użyciu CryptoAPI                              | 576        |
| 10.12. Sprawdzanie stanu unieważnienia poprzez protokół OCSP<br>przy wykorzystaniu OpenSSL            | 582        |
| <b>11. Liczby losowe</b>                                                                              | <b>587</b> |
| 11.1. Określanie charakteru liczb losowych, których należy użyć                                       | 587        |
| 11.2. Używanie ogólnego interfejsu API dla obsługi losowości i entropii                               | 592        |
| 11.3. Używanie standardowej infrastruktury losowości w systemach uniksowych                           | 594        |
| 11.4. Używanie standardowej infrastruktury losowości w systemach Windows                              | 598        |
| 11.5. Używanie generatora poziomu aplikacji                                                           | 600        |
| 11.6. Ponowna inicjalizacja ziarna generatora liczb pseudolosowych                                    | 609        |
| 11.7. Używanie rozwiązywania kompatybilnego z demonem zbierania entropii<br>przy użyciu pakietu EGADS | 612        |
| 11.8. Zbieranie entropii lub wartości pseudolosowych                                                  | 616        |
| 11.9. Używanie interfejsu API obsługi liczb losowych biblioteki OpenSSL                               | 620        |
| 11.10. Otrzymywanie losowych wartości całkowitych                                                     | 622        |
| 11.11. Otrzymywanie losowych wartości całkowitych z zadanego przedziału                               | 623        |
| 11.12. Otrzymywanie losowych wartości zmiennopozycyjnych<br>o rozkładzie jednorodnym                  | 625        |
| 11.13. Otrzymywanie wartości zmiennopozycyjnych o rozkładzie niejednorodnym                           | 626        |
| 11.14. Otrzymywanie losowych drukowalnych ciągów znaków ASCII                                         | 627        |
| 11.15. Uczciwe tasowanie                                                                              | 628        |
| 11.16. Kompresowanie danych z entropią do postaci ziarna o ustalonym rozmiarze                        | 629        |
| 11.17. Zbieranie entropii w momencie uruchamiania systemu                                             | 630        |
| 11.18. Testowanie statystyczne liczb losowych                                                         | 632        |

|                                                                                              |            |
|----------------------------------------------------------------------------------------------|------------|
| 11.19. Szacowanie i zarządzanie entropią                                                     | 637        |
| 11.20. Zbieranie entropii na podstawie interakcji z klawiaturą                               | 645        |
| 11.21. Zbieranie entropii na podstawie zdarzeń związanych z obsługą myszy w systemie Windows | 653        |
| 11.22. Zbieranie entropii na podstawie pomiarów czasowych wątków                             | 657        |
| 11.23. Zbieranie entropii na podstawie stanu systemu                                         | 659        |
| <b>12. Zapobieganie ingerencji</b>                                                           | <b>661</b> |
| 12.1. Podstawowe kwestie dotyczące problemu ochrony oprogramowania                           | 662        |
| 12.2. Wykrywanie modyfikacji                                                                 | 667        |
| 12.3. Zaciemnianie kodu                                                                      | 672        |
| 12.4. Przeprowadzanie zaciemniania na poziomie bitów i bajtów                                | 677        |
| 12.5. Przeprowadzanie przekształceń na zmiennych z użyciem wartości stałych                  | 679        |
| 12.6. Scalanie zmiennych skalarnych                                                          | 680        |
| 12.7. Rozdzielanie zmiennych                                                                 | 681        |
| 12.8. Ukrywanie wartości logicznych                                                          | 682        |
| 12.9. Używanie wskaźników do funkcji                                                         | 683        |
| 12.10. Zmiana struktury tablic                                                               | 684        |
| 12.11. Ukrywanie ciągów znaków                                                               | 689        |
| 12.12. Wykrywanie programów uruchomieniowych                                                 | 691        |
| 12.13. Wykrywanie programów uruchomieniowych w systemie Unix                                 | 693        |
| 12.14. Wykrywanie programów uruchomieniowych w systemie Windows                              | 695        |
| 12.15. Wykrywanie programu SoftICE                                                           | 696        |
| 12.16. Przeciwdziałanie deasemblacji                                                         | 698        |
| 12.17. Używanie kodu samomodyfikującego                                                      | 703        |
| <b>13. Inne zagadnienia</b>                                                                  | <b>709</b> |
| 13.1. Obsługa błędów                                                                         | 709        |
| 13.2. Bezpieczne usuwanie danych z pamięci                                                   | 713        |
| 13.3. Zapobieganie stronicowaniu pamięci na dysku                                            | 716        |
| 13.4. Poprawne używanie argumentów zmiennych                                                 | 717        |
| 13.5. Poprawna obsługa sygnałów                                                              | 720        |
| 13.6. Ochrona przed atakami rozbicia w systemie Windows                                      | 724        |
| 13.7. Ochrona przed uruchomieniem zbyt wielu wątków                                          | 726        |
| 13.8. Ochrona przed tworzeniem zbyt wielu gniazd sieciowych                                  | 731        |
| 13.9. Ochrona przed atakami wyczerpania zasobów w systemie Unix                              | 734        |
| 13.10. Ochrona przed atakami wyczerpania zasobów w systemie Windows                          | 737        |
| 13.11. Korzystanie ze sprawdzonych praktyk dotyczących rejestrowania nadzorczego             | 740        |
| <b>Skorowidz</b>                                                                             | <b>745</b> |