SZKOLENIE PODSTAWOWE

Praktyczne aspekty stosowania kryptografii w systemach komputerowych

KRYPT/F

Czas trwania: 5 dni (40h)

Przegląd mechanizmów kryptograficznych wykorzystywanych w celu zapewnienia bezpieczeństwa systemów komputerowych

Cele szkolenia

- Poznanie i praktyczne wykorzystanie różnorodnych technik kryptograficznych, które używane są przy implementacji zabezpieczeń w systemach komputerowych
- Poznanie prawidłowych zasad użycia między innymi algorytmów szyfrujących (symetrycznych i asymetrycznych), funkcji skrótu, kodów uwierzytelniających wiadomość, algorytmów podpisu cyfrowego oraz wybranych protokołów kryptograficznych
- Umiejętne unikanie typowych ataków na systemy wykorzystujące techniki kryptograficzne
- Zrozumienie problemów związanych z zarządzaniem kluczami kryptograficznymi oraz przechowywaniem i przekazywaniem danych poufnych dzięki wielu praktycznym przykładom i warsztatom
- Samodzielne zastosowanie poznanych mechanizmów do konfiguracji i uruchomienia centrum certyfikacji, zabezpieczonej poczty elektronicznej oraz komunikacji klient-serwer

Zalety

- Podczas szkolenia uczestnicy użyją wybranych algorytmów kryptograficznych w celu zapewnienia usług integralności, uwierzytelnienia, niezaprzeczalności oraz poufności
- Uczestnicy zaatakują nieprawidłowo zabezpieczone systemy oraz sprawdzą odporność swoich rozwiązań na ataki
- Zajęcia warsztatowe obejmują między innymi implementację protokołu wzajemnego uwierzytelnienia pomiędzy kartą elektroniczną i aplikacją
- Uczestnicy samodzielnie skonfigurują własny ośrodek certyfikacji, uruchomią zabezpieczoną pocztę elektroniczną w oparciu o S/MIME oraz bezpieczną komunikację wykorzystując protokół SSL/TLS
- Podczas szkolenia wykorzystujemy biblioteki zaimplementowane w C oraz Java, między innymi Bouncy Castle, OpenSSL, Mbed TLS i TinyCrypt
- W wersji dedykowanej szkolenie może być zrealizowane w oparciu o biblioteki, języki programowania lub platformy wybrane przez uczestników

- Praktyka przed teorią - wszystkie szkolenia technologiczne prowadzone są w formie warsztatowej. Konieczna teoria jest wyjaśniana na przykładzie praktycznych zadań
- Konkretne umiejętności - w ramach każdego szkolenia rozwijamy praktyczne umiejętności związane z daną technologią i tematyką
- Nauka z praktykami - wszyscy trenerzy na co dzień pracują w projektach, gwarantuje to dostęp do eksperckiej wiedzy i praktycznego know-how

Dla kogo?

- Programiści i architekci chcący poznać zagadnienia związane z prawidłowym wykorzystaniem mechanizmów kryptograficznych do budowy bezpiecznych systemów

Wymagania

- Od uczestników wymagana jest znajomość obsługi komputera, pracy z wierszem poleceń oraz znajomość podstawowych zasad programowania i podstaw składni języków C i Java

Program

1. Wprowadzenie do ochrony informacji
   a. Czym jest bezpieczeństwo informacji
   b. Pojęcia i relacje w bezpieczeństwie
   c. Podstawowe usługi ochrony informacji
   d. Integralność, uwierzytelnienie, niezaprzeczalność i poufność
   e. Kryptologia, kryptografia i kryptoanaliza
   f. Podstawowe zasady stosowane w kryptografii
   g. Kryptografia klasyczna
   h. Bezpieczeństwo obliczeniowe i siła klucza
   i. Standaryzacja i zalecenia: RFC, ISO/IEC, CEN/CENELEC, ETSI, PKCS, FIPS, ANSI, ITSEC/Common Criteria
   j. Biblioteki kryptograficzne w Java i C/C++
2. Algorytmy symetryczne
   a. Usługa poufności
   b. Szyfr z kluczem jednorazowym (one-time pad, OTP)
   c. Szyfrowanie a kodowanie
   d. Szyfry blokowe i ich parametry
   e. AES, 3DES i inne szyfry blokowe
   f. Podstawowe tryby pracy szyfrów blokowych: ECB, CBC, CTR
   g. Techniki oceny bezpieczeństwa algorytmów kryptograficznych
   h. Podstawy kryptoanalizy
   i. Szyfrowanie i kompresja
   j. Szyfry strumieniowe: ChaCha20
3. Funkcje skrótu
   a. Usługa integralności
   b. Cechy funkcji skrótu

   c. Rodzina SHA, SHA3 i algorytm Keccak
   d. Ataki na funkcje skrótu
   e. Procedury i algorytmy niszczenia informacji
4. Uwierzytelnienie i identyfikacja, kody uwierzytelniające wiadomość
   a. Usługa uwierzytelnienia i identyfikacji
   b. Kody uwierzytelniające wiadomość: HMAC, KMAC, CBC-MAC, CMAC
   c. Uwierzytelnienie a autoryzacja
5. Generatory liczb losowych
   a. Pojęcie losowości, typy generatorów liczb losowych
   b. Entropia i jej rola
   c. Bezpieczne kryptograficznie generatory ciągów pseudolosowych
6. Szyfrowanie z uwierzytelnieniem
   a. Zasady łączenia różnych usług ochrony informacji
   b. Tryby uwierzytelnionego szyfrowania (authenticated encryption, AE)
   c. Tryby uwierzytelnionego szyfrowania z danymi dodatkowymi (authenticated encryption with associated data, AEAD)
   d. Tryby: CCM, GCM i EAX
7. Algorytmy asymetryczne
   a. Problem wymiany i ustanawiania klucza
   b. Ceremonia wymiany klucza
   c. Algorytm Diffiego-Hellmana-Merkla (DH)
   d. Algorytm RSA
   e. Podpis cyfrowy i problem autentyczności klucza
   f. Algorytm podpisu cyfrowego DSA
   g. Krzywe eliptyczne w kryptografii: krzywe NIST, SECG i Brainpool, Curve25519, Curve448
   h. Algorytmy oparte o krzywe eliptyczne: ECDH, X25519, X448, ECDSA, EdDSA, Ed25519, Ed448
   i. Formaty podpisu cyfrowego
   j. Szyfrowanie za pomocą algorytmów asymetrycznych
   k. Porównanie algorytmów symetrycznych i asymetrycznych
8. Hasła
   a. Hasła, frazy hasłowe a klucze kryptograficzne
   b. Wymagania wobec haseł
   c. Numery PIN
   d. Tworzenie kluczy z haseł
   e. Szyfrowanie z hasłem (password based encryption, PBE)
   f. Przechowywanie haseł: Argon2, bcrypt, PBKDF2
   g. Szyfrowanie nośników danych
9. Protokoły kryptograficzne
   a. Protokół zobowiązania bitowego
   b. Protokół wyzwanie-odpowiedź
   c. Współdzielenie sekretów i schematy progowe
   d. Dowody wiedzy zerowej
10. Zarządzanie kluczami
   a. Metody zarządzania kluczami w systemach kryptograficznych

b. Repozytoria kluczy: PKCS #12, JKS, JCEKS, BC i BCFKS
c. Dywersyfikacja kluczy
d. Unikalność klucza, klucze sesyjne (efemeryczne)
e. Funkcje wyprowadzania klucza (key derivation function, KDF)
f. Zarządzanie kluczami w systemach kart elektronicznych
g. Zarządzanie kluczami w systemach płatniczych
h. Karty inteligentne (smart cards)
i. Elementy zabezpieczające (security elements, SE)
j. Sprzętowe moduły zabezpieczeń (hardware security module, HSM)
k. Interfejs PKCS #11
l. Dostawcy usług kryptograficznych w Java
m. Biblioteki CSP

11. Zastosowania kryptografii
    a. Zalecenia dotyczące algorytmów kryptograficznych, długości kluczy i innych parametrów
    b. Podstawy notacji ASN.1
    c. Kodowanie DER (Distinguished Encoding Rules) i PEM (Privacy-Enhanced Mail)
    d. Znaczenie zaufania, zaufana trzecia strona (trusted third party, TTP)
    e. Infrastruktura klucza publicznego (public key infrastructure, PKI)
    f. Usługi PKI w kontekście usług ochrony informacji
    g. Generowanie kluczy oraz zgłoszenia certyfikacyjnego
    h. Certyfikaty X.509
    i. Łańcuch i ścieżka certyfikacji (certificate chain, certificate path)
    j. Repozytoria certyfikatów
    k. Pola certyfikatów i ich ustawienia
    l. Ograniczanie użycia klucza
    m. Lista certyfikatów unieważnionych (certificate revocation list, CRL)
    n. Protokół weryfikacji statusu certyfikatu (online certificate status protocol, OCSP)
    o. Bezpieczna poczta elektroniczna S/MIME
    p. Działanie i parametry protokołu SSL/TLS
    q. Jednostronne i obustronne uwierzytelnienie w protokole SSL/TLS
    r. Doskonałe utajnienie z wyprzedzeniem (perfect forward secrecy, PFS)
    s. Wykorzystanie kryptografii do budowy blockchain
12. Ataki na systemy wykorzystujące kryptografię
    a. Klasy ataków i ich cele
    b. Atak brutalny
    c. Atak słownikowy
    d. Atak typu man in the middle (MITM)
    e. Atak powtórzeniowy
    f. Inicjalizacja generatora liczb pseudolosowych
    g. Nieprawidłowe użycie kluczy i trybów szyfrowania
    h. Błędy w implementacji algorytmów
    i. Ataki socjotechniczne