Kod szkolenia: **KRYPT/F**

Tytuł szkolenia: **Praktyczne aspekty stosowania kryptografii w systemach komputerowych**

Dni: 5

Opis:

Adresaci szkolenia

Szkolenie adresowane jest do osób pragnących poznać zagadnienia związane z prawidłowym wykorzystaniem mechanizmów kryptograficznych do budowy bezpiecznych systemów.

Cel szkolenia

Celem szkolenia jest poznanie i praktyczne wykorzystanie różnorodnych technik kryptograficznych, które używane są przy implementacji zabezpieczeń w systemach komputerowych. Podczas szkolenia uczestnicy poznają prawidłowe zasady użycia między innymi algorytmów szyfrujących (symetrycznych i asymetrycznych), funkcji skrótu, kodów uwierzytelniających wiadomość, algorytmów podpisu cyfrowego oraz wybranych protokołów kryptograficznych. Dzięki wielu praktycznym przykładom i warsztatom uczestnicy zrozumieją problemy związane na przykład z generowaniem i zarządzaniem kluczami kryptograficznymi czy przechowywaniem i przekazywaniem danych wrażliwych. Ponadto samodzielnie zastosują poznane mechanizmy do konfiguracji i uruchomienia centrum certyfikacji, zabezpieczonej poczty elektronicznej oraz komunikacji klient-serwer.

Mocne strony szkolenia

Podczas warsztatów uczestnicy:

- użyją wybranych algorytmów kryptograficznych w celu zapewnienia usług integralności, uwierzytelnienia, niezaprzeczalności oraz poufności,
- dokonają ataków na nieprawidłowo zabezpieczone systemy,
- zaimplementują protokół wzajemnego uwierzytelnienia pomiędzy kartą elektroniczną i aplikacją,
- uruchomią zabezpieczoną pocztę elektroniczną w oparciu o S/MIME oraz bezpieczną komunikację wykorzystując protokół SSL/TLS.

Wymagania

Od uczestników wymagana jest podstawowa wiedza z zakresu programowania. Podczas szkolenia wykorzystujemy biblioteki zaimplementowane w C oraz Java, między innymi

Bouncy Castle, OpenSSL oraz mbed TLS. Szkolenie może być zrealizowane w oparciu o bibliotekę lub język programowania zaproponowany przez uczestników (na przykład C#).

Specjalne wymagania techniczne

Uczestnicy w trakcie zajęć korzystają z komputera z systemem Windows lub Linux. Niezbędne jest posiadanie co najmniej jednego czytnika kart elektronicznych zgodnego z PC/SC.

Parametry szkolenia

5 * 8 godzin (5 * 7 godzin netto) wykładów i warsztatów.

Program szkolenia:

1. Wprowadzenie do ochrony informacji
    - czym jest ochrona informacji i bezpieczeństwo
    - pojęcia i relacje w bezpieczeństwie
    - podstawowe usługi ochrony informacji: integralność, uwierzytelnienie, niezaprzeczalność i poufność
    - kryptologia, kryptografia i kryptoanaliza
    - podstawowe zasady stosowane w kryptografii
    - kryptografia klasyczna
    - bezpieczeństwo obliczeniowe i siła klucza
    - standaryzacja i zalecenia (RFC, ISO/IEC, CEN/CENELEC, ETSI, PKCS, FIPS, ANSI, ITSEC/Common Criteria)
    - biblioteki kryptograficzne w Java i C/C++

2. Algorytmy symetryczne
    - usługa poufności
    - szyfr z kluczem jednorazowym (ang. *one-time pad*, OTP)
    - szyfrowanie a kodowanie
    - szyfry blokowe i ich parametry
    - AES, DES, 3DES i inne szyfry blokowe
    - podstawowe tryby pracy szyfrów blokowych (ECB, CBC, CTR)
    - techniki oceny bezpieczeństwa algorytmów kryptograficznych
    - podstawy kryptoanalizy
    - szyfrowanie i kompresja
    - szyfry strumieniowe

3. Funkcje skrótu i kody uwierzytelniające wiadomość

    - usługa integralności
    - cechy funkcji skrótu
    - MD5, rodzina SHA, algorytm Keccak
    - ataki na funkcje skrótu
    - procedury i algorytmy niszczenia informacji

4. Uwierzytelnienie i identyfikacja

    - usługa uwierzytelnienia i identyfikacji
    - kody uwierzytelniające wiadomość: HMAC, CBC-MAC, CMAC
    - uwierzytelnienie a autoryzacja

5. Generatory liczb losowych

    - pojęcie losowości
    - entropia i jej rola
    - bezpieczne kryptograficznie generatory ciągów pseudolosowych

6. Szyfrowanie z uwierzytelnieniem

    - zasady łączenia różnych usług ochrony informacji
    - uwierzytelnione szyfrowanie (ang. *authenticated encryption*, AE)
    - uwierzytelnione szyfrowanie z danymi dodatkowymi (ang. *authenticated encryption with additional data*, AEAD)
    - tryby AE i AEAD: CCM, GCM

7. Algorytmy asymetryczne

    - problem wymiany i ustanawiania klucza
    - ceremonia wymiany klucza
    - algorytm Diffiego-Hellmana-Merkla (DH)
    - algorytm RSA
    - podpis cyfrowy i problem autentyczności klucza
    - algorytm podpisu cyfrowego DSA
    - algorytmy oparte o krzywe eliptyczne i ich parametry: ECIES, ECDH i ECDSA
    - formaty podpisu cyfrowego
    - szyfrowanie za pomocą algorytmów asymetrycznych
    - porównanie algorytmów symetrycznych i asymetrycznych

8. Hasła
    - hasła a klucze kryptograficzne
    - wymagania wobec haseł
    - numery PIN
    - tworzenie kluczy z haseł
    - szyfrowanie z hasłem (ang. *password based encryption*, PBE)
    - szyfrowanie nośników danych

9. Protokoły kryptograficzne
    - protokół zobowiązania bitowego
    - protokół wyzwanie-odpowiedź
    - współdzielenie sekretów i schematy progowe
    - dowody wiedzy zerowej

10. Zarządzanie kluczami
    - metody zarządzania kluczami w systemach kryptograficznych
    - repozytoria kluczy: JKS, JCEKS, PKCS#12, BC i BCFKS
    - dywersyfikacja kluczy
    - unikalność klucza, klucze sesyjne (efemeryczne)
    - zarządzanie kluczami w systemach kart elektronicznych
    - zarządzanie kluczami w systemach płatniczych
    - sprzętowe moduły bezpieczeństwa (ang. *hardware security module*, HSM)
    - dostęp do urządzeń kryptograficznych: interfejs PKCS#11 i CSP

11. Zastosowania kryptografii
    - aktualne zalecenia dotyczące mechanizmów kryptograficznych (wykorzystywane algorytmy, długości kluczy i inne parametry)
    - notacja ASN.1, kodowanie DER i PEM
    - znaczenie zaufania, zaufana trzecia strona (ang. *trusted third party*, TTP)
    - infrastruktura klucza publicznego (ang. *public key infrastructure*, PKI)
    - usługi PKI w kontekście usług ochrony informacji
    - generowanie kluczy oraz zgłoszenia certyfikacyjnego
    - certyfikaty X.509, rola pól i rozszerzeń certyfikatów, ścieżka certyfikacyjna
    - lista certyfikatów unieważnionych (ang. *certificate revocation list*, CRL, delta CRL)
    - protokół weryfikacji statusu certyfikatu (ang. *online certificate status protocol*, OCSP)
    - usługa znakowania czasem
    - działanie i parametry protokołu SSL/TLS

- jednostronne i obustronne uwierzytelnienie w protokole SSL/TLS
- bezpieczna poczta elektroniczna S/MIME
- wykorzystanie kryptografii do budowy blockchain

12. Ataki na systemy wykorzystujące kryptografię

- typy ataków
- podstawowe zasady stosowane przy użyciu metod kryptograficznych
- atak brutalny, atak słownikowy
- atak powtórzeniowy
- inicjalizacja generatora liczb pseudolosowych
- nieprawidłowe użycie kluczy i trybów szyfrowania
- błędy w implementacji algorytmów
- ataki socjotechniczne