SZKOLENIE PODSTAWOWE

Protokół SSL i TLS

TLS

Czas trwania: 4 dni

Działanie i wykorzystanie protokołu SSL/TLS do zabezpieczenia danych wymienianych pomiędzy aplikacjami

Cele szkolenia

- Uruchomienie bezpiecznej komunikacji wykorzystującej protokół SSL/TLS w różnych konfiguracjach
- Integracja protokołu SSL/TLS w aplikacji
- Zrozumienie mechanizmów uwierzytelniania stron protokołu SSL/TLS, zarówno bazujących na certyfikatach w infrastrukturze klucza publicznego (public key infrastructure, PKI), jak i bez użycia certyfikatów
- Poznanie i użycie w praktyce technik kryptograficznych, które wykorzystywane są w implementacji i konfiguracji protokołu SSL/TLS
- Poznanie prawidłowych zasad użycia i łączenia algorytmów szyfrujących, funkcji skrótu, kodów uwierzytelniających wiadomość oraz algorytmów podpisu cyfrowego

Zalety

- Uczestnicy zintegrują protokół SSL/TLS w przykładowych aplikacjach, wykorzystując między innymi karty inteligentne (smart cards) do uwierzytelnienia stron protokołu
- W trakcie warsztatów wykorzystane zostaną narzędzia umożliwiających śledzenie, namierzanie i rozwiązywanie problemów w sesjach SSL/TLS
- Podczas warsztatów uczestnicy samodzielnie skonfigurują i uruchomią własny ośrodek certyfikacji w oparciu o otwarte oprogramowanie
- Uczestnicy przygotują i obsłużą zgłoszenia certyfikacyjne wystawiając certyfikaty o różnym przeznaczeniu
- Szkolenie obejmuje różne wersje protokołu, również te, które obecnie nie są bezpieczne, ale muszą być utrzymywane w różnych systemach i zabezpieczane na inne sposoby
- W wersji dedykowanej szkolenie może być zrealizowane w oparciu o biblioteki, języki programowania lub platformy wybrane przez uczestników

Dla kogo?

- Programiści chcący poznać zagadnienia związane z praktycznym wykorzystania protokołu SSL/TLS do zabezpieczenia komunikacji w systemach informatycznych

Wymagania

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

Program

1. Wprowadzenie do ochrony informacji
   a. Czym jest bezpieczeństwo informacji
   b. Podstawowe usługi ochrony informacji
   c. Integralność, uwierzytelnienie, niezaprzeczalność i poufność
   d. Protokół SSL (Secure Sockets Layer)
   e. Rodzina protokołów TLS (Transport Layer Security)
   f. Cele stosowania protokołu SSL/TLS
   g. Zaufanie i sposoby jego budowania
   h. Rola zaufanej trzeciej strony (trusted third party, TTP)
   i. Uwierzytelnienie witryn internetowych i protokół HTTPS
   j. Rozporządzenie w sprawie identyfikacji elektronicznej i usług zaufania (eIDAS)
   k. Listy statusu usług zaufania (trust service status list, TSL)
   l. Normy międzynarodowe i standardy przemysłowe
2. Algorytmy i protokoły kryptograficzne
   a. Funkcje skrótu: rodzina MD, rodzina SHA, SHA3
   b. Algorytmy symetryczne: 3DES, AES
   c. Krzywe eliptyczne w kryptografii: krzywe NIST, SECG i Brainpool, Curve25519, Curve448
   d. Algorytmy uzgadniania klucza: DH, ECDH, X25519, X448
   e. Algorytmy asymetryczne: RSA, ECDSA, EdDSA, Ed25519, Ed448
   f. Problem autentyczności klucza
   g. Identyfikacja, uwierzytelnienie i autoryzacja
   h. Kody uwierzytelniające wiadomość (message authentication code, MAC)
   i. Tryby uwierzytelnionego szyfrowania (authenticated encryption, AE)
   j. Tryby uwierzytelnionego szyfrowania z danymi dodatkowymi (authenticated encryption with associated data, AEAD)
   k. Podstawy notacji ASN.1
   l. Kodowanie DER (Distinguished Encoding Rules) i PEM (Privacy-Enhanced Mail)
   m. Zalecenia dotyczące parametrów algorytmów kryptograficznych
3. Przechowywanie i przekazywanie kluczy kryptograficznych
   a. Problem bezpiecznego przechowywania kluczy
   b. Zarządzanie kluczami
   c. Cykl życia kluczy
   d. Karty inteligentne (smart cards)
   e. Sprzętowe moduły bezpieczeństwa (hardware security module, HSM)
   f. Dostęp do urządzeń kryptograficznych w systemach operacyjnych i przeglądarkach
   g. Interfejs PKCS #11
   h. Dostawcy usług kryptograficznych w Java
   i. Biblioteki CSP
   j. Repozytoria kluczy: PKCS #12, JKS, JCEKS, BC i BCFKS
4. Elementy i rola Infrastruktury Klucza Publicznego
   a. Generowanie kluczy oraz zgłoszenia certyfikacyjnego
   b. Ośrodek certyfikacji (certificate authority, CA)

c. Rola punktu rejestracji (registration authority, RA)
d. Certyfikaty X.509
e. Łańcuch i ścieżka certyfikacji (certificate chain, certificate path)
f. Repozytoria certyfikatów
g. Pola certyfikatów i ich ustawienia
h. Ograniczanie użycia klucza
i. Rozszerzenia certyfikatów
j. Profile certyfikatów
k. Certyfikaty rozszerzonej walidacji
l. Odcisk klucza certyfikatu
m. Cykl życia certyfikatu
n. Ustanawianie zaufania pomiędzy ośrodkami certyfikacji
o. Główne i pośrednie urzędy certyfikacji
p. Certyfikaty skrośne (cross certificate) i zakładkowe (link certificate)
q. Kompromitacja klucza i unieważnianie certyfikatów
r. Lista certyfikatów unieważnionych (certificate revocation list, CRL)
s. Protokół weryfikacji statusu certyfikatu (online certificate status protocol, OCSP)
t. Mechanizm CRLSets
u. Przejrzystość certyfikatów (certificate transparency, CT)
v. Znacznik SCT (signed certificate timestamp)
w. Architektury wdrożeń PKI
x. Zalecenia grupy roboczej PKIX

5. Działanie i konfiguracja protokołu SSL/TLS
   a. Wersje protokołu SSL (v2 i v3) i TLS (od 1.0 do 1.3)
   b. Przebieg działania i elementy protokołu
   c. Różnice w wersjach protokołu
   d. Pakiety algorytmów (cipher suites)
   e. Rozszerzenia protokołu SSL/TLS
   f. Jednostronne i obustronne uwierzytelnienie w protokole SSL/TLS
   g. Wybór metody uwierzytelnienia serwera i klienta
   h. Handshake typu 1-RTT i 0-RTT
   i. Wybór metody wymiany/uzgodnienia klucza
   j. Doskonałe utajnienie z wyprzedzeniem (perfect forward secrecy, PFS)
   k. Wpływ certyfikatu oraz parametrów protokołu na zachowanie przeglądarki internetowej
   l. Metoda współdzielonego klucza (pre-shared key, PSK)
   m. Uwierzytelnienie oparte o hasło (secure remote password, SRP)
   n. Datagramowy protokół TLS (Datagram Transport Layer Security, DTLS)
   o. Wykorzystanie programowych i sprzętowych końcówek SSL/TLS
   p. Testowanie działania protokołu
   q. Zalecenia dotyczące konfiguracji
6. Integracja SSL/TLS w aplikacjach
   a. Wbudowanie protokołu w aplikację
   b. Tunelowanie komunikacji
   c. Rozwiązania w systemach wbudowanych i internetu rzeczy (internet of things, IoT)

    d. Utrzymanie i zabezpieczanie niebezpiecznych konfiguracji SSL/TLS
7. Protokół SSL/TLS w usłudze HTTPS
    a. Mechanizm HSTS (HTTP Strict Transport Security)
    b. Mechanizm HPKP (HTTP Public Key Pinning)
    c. Wykorzystanie CSP (Content Security Policy)
8. Bezpieczeństwo protokołu SSL/TLS
    a. Przegląd wybranych ataków
    b. Bezpieczeństwo wybranej konfiguracji protokołu
    c. Narzędzia do testowania bezpieczeństwa ustawień
    d. Weryfikacja poprawności konfiguracji