Kod szkolenia: **SSL/TLS**

Tytuł szkolenia: **Protokół SSL/TLS**

Dni: 4

Opis:

Adresaci szkolenia

Szkolenie adresowane jest do osób pragnących poznać zagadnienia związane z praktycznymi aspektami wykorzystania protokołu SSL/TLS do zabezpieczenia komunikacji w systemach informatycznych.

Cel szkolenia

Celem szkolenia jest poznanie i użycie w praktyce różnorodnych technik kryptograficznych, które wykorzystywane są w implementacji i konfiguracji protokołu SSL/TLS. Podczas szkolenia uczestnicy poznają prawidłowe zasady użycia między innymi algorytmów szyfrujących (symetrycznych i asymetrycznych), funkcji skrótu, kodów uwierzytelniających wiadomość oraz algorytmów podpisu cyfrowego. Omówiony zostanie tradycyjny mechanizm uwierzytelniania stron protokołu SSL/TLS bazujący na certyfikatach w infrastrukturze klucza publicznego (ang. *public key infrastructure*, PKI) oraz inne tryby pracy protokołu. Uczestnicy prześledzą przykładowe sesje SSL/TLS oraz skonfigurują i wykorzystają go w implementacji swojego systemu.

Mocne strony szkolenia

Podczas warsztatów uczestnicy:

- użyją wybranych algorytmów kryptograficznych w celu zapewnienia usług integralności, uwierzytelnienia oraz poufności,
- skonfigurują i uruchomią własne centrum certyfikacji wykorzystując bibliotekę OpenSSL,
- przygotują i obsłużą zgłoszenia certyfikacyjne wystawiając certyfikaty o różnym przeznaczeniu,
- prześledzą działanie protokołu SSL/TLS i poznają narzędzia ułatwiające rozwiązywanie problemów przy nawiązywaniu połączenia,
- uruchomią bezpieczną komunikację wykorzystując protokół SSL/TLS w różnych konfiguracjach,
- przygotują karty inteligentne (ang. *smart cards*) z kluczami i certyfikatami i użyją ich do realizacji wzajemnego uwierzytelnienia w protokole SSL/TLS.

sages

Wymagania

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

4 * 8 godzin (4 * 7 godzin netto) wykładów i warsztatów.

Program szkolenia:

1. Wprowadzenie
    - podstawowe usługi ochrony informacji
    - integralność, uwierzytelnienie, niezaprzeczalność i poufność
    - cele protokołu SSL/TLS, uwierzytelnienie witryn internetowych i protokół HTTPS
    - zaufanie i sposoby jego realizacji
    - rola zaufanej trzeciej strony (ang. *trusted third party*, TTP)
    - rozporządzenie w sprawie identyfikacji elektronicznej i usług zaufania (eIDAS)
    - listy statusu usług zaufania (ang. *trust service status list*, TSL)

2. Algorytmy, protokoły i urządzenia kryptograficzne
    - normy międzynarodowe i standardy przemysłowe
    - funkcje skrótu (MD5, rodzina SHA, algorytm Keccak)
    - algorytmy symetryczne (3DES, AES), ich parametry i tryby działania
    - algorytmy wykorzystujące krzywe eliptyczne
    - algorytmy ustanawiania klucza (DH, ECDH)
    - algorytmy asymetryczne (RSA, ECDSA)
    - problem autentyczności klucza
    - kody uwierzytelniające wiadomość (ang. *message authentication code*, MAC)
    - uwierzytelnione szyfrowanie (ang. *authenticated encryption*, AE)
    - uwierzytelnione szyfrowanie z danymi dodatkowymi (ang. *authenticated encryption with additional data*, AEAD)

- tryby AE i AEAD: CCM, GCM
- problem bezpiecznego przechowywania kluczy kryptograficznych
- repozytoria kluczy: JKS, JCEKS, PKCS#12, BC i BCFKS
- karty inteligentne (ang. *smart cards*)
- sprzętowe moduły bezpieczeństwa (ang. *hardware security module*, HSM)
- dostęp do urządzeń kryptograficznych (biblioteki PKCS#11, CSP)
- aktualne zalecenia dotyczące parametrów wykorzystywanych algorytmów kryptograficznych

3. Elementy i działanie Infrastruktury Klucza Publicznego

- rola infrastruktury klucza publicznego (ang. *public key infrastructure*, PKI)
- notacja ASN.1, kodowanie DER i PEM
- czym jest certyfikat klucza publicznego
- generowanie kluczy oraz zgłoszenia certyfikacyjnego
- rola punktu rejestracji (ang. *registration authority*, RA)
- centrum certyfikacji (ang. *certificate authority*, CA)
- certyfikaty X.509
- podstawowe pola certyfikatów
- rozszerzenia certyfikatów
- certyfikaty rozszerzonej walidacji
- certyfikaty kwalifikowane i niekwalifikowane
- odcisk klucza certyfikatu
- polityka certyfikacji
- cykl życia certyfikatu
- ścieżka certyfikacji
- repozytorium certyfikatów
- kompromitacja klucza i unieważnianie certyfikatów
- lista certyfikatów unieważnionych (ang. *certificate revocation list*, CRL, delta CRL)
- protokół weryfikacji statusu certyfikatu (ang. *online certificate status protocol*, OCSP)
- przykładowe wdrożenia PKI, hierarchia CA
- zalecenia grupy roboczej PKIX

4. Działanie i konfiguracja protokołu SSL/TLS

- cechy protokołu SSL/TLS oraz jego zastosowania
- wersje protokołu
- przebieg działania i elementy protokołu: SSL Handshake, SSL Change Cipher, SSL Alert Protocol, SSL Record Protocol
- pakiety algorytmów (ang. *cipher suites*)
- rozszerzenia protokołu SSL/TLS
- wybór metody uwierzytelnienia serwera i klienta

- jednostronne i obustronne uwierzytelnienie w protokole SSL/TLS
- pozyskanie certyfikatów
- wybór metody wymiany/uzgodnienia klucza, pojęcie PFS (ang. *perfect forward secrecy*)
- wpływ certyfikatu oraz parametrów protokołu na zachowanie przeglądarki internetowej
- działanie i wykorzystanie PSK (ang. *pre-shared key*)
- działanie i wykorzystanie SRP (ang. *secure remote password*)
- protokół DTLS
- wykorzystanie programowych i sprzętowych końcówek SSL/TLS
- testowanie działania protokołu
- weryfikacja poprawności konfiguracji

5. Protokół SSL/TLS w usłudze HTTPS

- mechanizm HSTS (ang. *HTTP Strict Transport Security*)
- mechanizm HPKP (ang. *HTTP Public Key Pinning*)
- wykorzystanie CSP (ang. *Content Security Policy*)

6. Bezpieczeństwo protokołu SSL/TLS

- przegląd wybranych ataków
- bezpieczeństwo wybranej konfiguracji protokołu
- protokół TLS 1.3

Sages sp. z o.o., ul. Nowogrodzka 62c, 02-002 Warszawa
tel. +48 22 203 56 00 fax: +48 22 203 56 01
e-mail: biuro@sages.com.pl web: www.sages.com.pl