Kod szkolenia: **PKI**

Tytuł szkolenia: **Infrastruktura Klucza Publicznego (PKI)**

Dni: 3

Opis:

Adresaci szkolenia

Szkolenie adresowane jest do osób pragnących poznać zagadnienia związane z Infrastrukturą Klucza Publicznego (ang. *Public Key Infrastructure*, PKI). Szczególnie zalecane dla programistów, administratorów oraz specjalistów bezpieczeństwa, którzy będą zajmować się tematyką podpisu cyfrowego oraz innych usług bazujących na PKI.

Cel szkolenia

Uczestnicy zapoznają się z podstawowymi usługami ochrony informacji oraz sposobem ich wykorzystania do budowy Infrastruktury Klucza Publicznego. Omówione zostaną mechanizmy kryptograficzne oraz ich przeznaczenie. Przedstawione zostaną aspekty prawne związane z usługami wykorzystującymi PKI obowiązujące w Polsce i Unii Europejskiej. Uczestnicy zapoznają się też w praktyce z usługami związanymi z PKI takimi jak podpis cyfrowy, uwierzytelnienie w protokole SSL/TLS, serwer weryfikacji statusu certyfikatów (OCSP), serwer znakowania czasem (TSA).

Mocne strony szkolenia

Podczas szkolenia uczestnicy:

- skonfigurują i uruchomią własne centrum certyfikacji wykorzystując bibliotekę OpenSSL,
- przygotują i obsłużą zgłoszenia certyfikacyjne,
- wystawią certyfikaty dla kluczy publicznych algorytmów RSA oraz ECDSA o różnym przeznaczeniu,
- przygotują karty inteligentne (ang. *smart cards*) z kluczami i certyfikatami,
- wykorzystają przygotowane karty oraz certyfikaty do realizacji usług bezpiecznej poczty elektronicznej i uwierzytelnienia w protokole SSL/TLS.

Wymagania

Od uczestników szkolenia wymagana jest umiejętność obsługi komputera w systemie Windows lub Linux.

Specjalne wymagania techniczne

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

Parametry szkolenia

3 * 8 godzin (3 * 7 godzin netto) wykładów i warsztatów.

Program szkolenia:

1. Wprowadzenie
    - podstawowe usługi ochrony informacji
    - integralność, uwierzytelnienie, niezaprzeczalność i poufność
    - czym jest bezpieczeństwo informacji
    - podpis cyfrowy i jego zastosowania
    - 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
    - integralność, funkcje skrótu
    - poufność
    - algorytmy symetryczne (3DES, AES)
    - algorytmy uzgadniania klucza (DH, ECDH)
    - algorytmy asymetryczne (RSA, ECDSA)
    - problem autentyczności klucza
    - uwierzytelnienie i autoryzacja
    - kody uwierzytelniające wiadomość (ang. *message authentication code*, MAC)
    - podpis cyfrowy, generowanie kluczy, tworzenie podpisu i jego weryfikacja
    - przechowywanie i przekazywanie danych kryptograficznych
    - notacja ASN.1, kodowanie DER i PEM
    - problem bezpiecznego przechowywania danych
    - 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

    - architektura PKI
    - 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 atrybutów
    - certyfikaty rozszerzonej walidacji
    - certyfikaty CVC (ang. *card verifiable certificate*)
    - certyfikaty kwalifikowane i niekwalifikowane
    - odcisk klucza certyfikatu
    - polityka certyfikacji
    - cykl życia certyfikatu
    - ścieżka certyfikacji
    - repozytorium certyfikatów
    - usługi PKI w aspekcie usług ochrony informacji
    - 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)
    - urząd znacznika czasu (ang. *time stamping authority*, TSA)
    - przykładowe wdrożenia PKI, hierarchia CA
    - zalecenia grupy roboczej PKIX

4. Praktyczne wykorzystanie Infrastruktury Klucza Publicznego

    - cyfrowe podpisywanie i weryfikacja dokumentów
    - bezpieczna poczta elektroniczna, podpisywanie i szyfrowanie wiadomości
    - uwierzytelnienie serwera i klienta w protokole SSL/TLS