Kod szkolenia: **J/CARD**

Tytuł szkolenia: **Programowanie kart Java Card**

Dni: 5

Opis:

Adresaci szkolenia

Szkolenie adresowane jest do osób pragnących poznać zagadnienia związane wykorzystaniem elektronicznych kart inteligentnych Java Card do budowy bezpiecznych systemów.

Cel szkolenia

Karty inteligentne (ang. *smart cards*) wykorzystywane są jako bezpieczny nośnik informacji. Uczestnicy zapoznają się z podstawowymi algorytmami i protokołami kryptograficznymi używanymi w systemach kartowych. Poznają architekturę Java Card, dostępne API oraz zasady tworzenia apletów w oparciu o symulator i rzeczywistą kartę. Uczestnicy zapoznają się również z API obsługującym czytniki kart poprzez interfejs PC/SC w językach C, C++, Java oraz C# na platformach Windows i Linux. Podczas szkolenia omówione zostaną również praktyczne zagadnienia związane z dobrymi praktykami w zakresie tworzenia bezpiecznych systemów kartowych na przykładach takich jak karta jako nośnik biletów elektronicznych, podpis elektroniczny, karty dostępu, systemy płatnicze oraz lojalnościowe.

Mocne strony szkolenia

Podczas warsztatów uczestnicy:

- utworzą własne aplety dla Java Card oraz umieszczą je w symulatorze i rzeczywistej karcie,
- dokonają ataku na nieprawidłowo zabezpieczony system kartowy,
- zaimplementują protokół wzajemnego uwierzytelnienia pomiędzy kartą i aplikacją oraz pomiędzy dwiema kartami,
- zrealizują w praktyce mechanizm zabezpieczonej komunikacji pomiędzy terminalem a kartą,
- oprogramują wykorzystanie czytnika zgodnego z PC/SC.

Wymagania

Od uczestników szkolenia wymagana jest umiejętność programowania na poziomie podstawowym w Java oraz w C lub C++ lub C#.

sages

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 kart elektronicznych
    - klasyfikacje kart
    - budowa fizyczna, wymiary, interfejsy komunikacyjne
    - techniki komunikacji z kartami, czytniki kart
    - karty pamięciowe i inteligentne
    - karty natywne i programowalne
    - zastosowania kart elektronicznych
    - ogólna charakterystyka kart Java Card

2. Algorytmy i protokoły kryptograficzne
    - podstawowe usługi ochrony informacji
    - integralność, funkcje skrótu
    - poufność
    - algorytmy symetryczne (3DES, AES)
    - algorytmy uzgadniania klucza (DH, ECDH)
    - algorytmy asymetryczne (RSA, ECDSA)
    - uwierzytelnienie
    - kody uwierzytelniające wiadomość (ang. *message authentication code*, MAC)
    - podpis elektroniczny
    - przechowywanie i przekazywanie danych kryptograficznych
    - ceremonia wymiany klucza
    - notacja ASN.1, kodowanie DER i PEM
    - problem bezpiecznego przechowywania informacji
    - sprzętowe moduły bezpieczeństwa (ang. *hardware security module*, HSM)
    - dostęp do urządzeń kryptograficznych (biblioteki PKCS #11, CSP)
    - aktualne zalecenia dotyczące parametrów wykorzystywanych algorytmów kryptograficznych
    - protokół wyzwanie-odpowiedź
    - zabezpieczanie komunikacji

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

3. Karty inteligentne Java Card

    - architektura kart Java Card
    - wersje platformy Java Card, Java Card Kit
    - Java Card Virtual Machine
    - Java Card Runtime Environment
    - Java Card API
    - identyfikatory (AID) pakietów i instancji, RID i PIX
    - środowisko rozwoju apletów
    - symulator Java Card Platform Simulator (cref)
    - działanie Card Managera
    - skrypty dla GPShell, zarządzanie kartą
    - obsługa komend APDU
    - obsługa pamięci nieulotnej i ulotnej
    - obsługa kodu PIN
    - obsługa transakcji atomowych
    - obsługa struktur danych TLV (ang. *tag, length, value*)
    - generatory liczb losowych
    - wykorzystanie algorytmów kryptograficznych w kartach
    - funkcje skrótu
    - kody uwierzytelniające wiadomość
    - algorytmy symetryczne i asymetryczne, generowanie kluczy
    - szyfrowanie i deszyfrowanie
    - składanie podpisu elektronicznego
    - techniki biometryczne
    - zabezpieczanie komunikacji z kartami
    - zalecenia dotyczące tworzenia wydajnych apletów Java Card
    - optymalizacja wykorzystania pamięci
    - techniki i zalecenia dotyczące testowania apletów Java Card

4. Aplikacje wykorzystujące karty

    - czytniki kart inteligentnych
    - interfejs PC/SC
    - obsługa zdarzeń w czytniku
    - typowe problemy związane z obsługą kart stykowych i bezstykowych

5. Karta jako bezpieczny nośnik informacji

    - techniki dystrybucji kluczy
    - moduły SAM (ang. *secure access module*)
    - przechowywanie i zarządzanie danymi użytkowników na przykładzie biletów

elektronicznych
- generowanie i przechowywanie kluczy prywatnych, składanie podpisu elektronicznego
- system płatniczy EMV
- systemy lojalnościowe
- dobre praktyki tworzenia systemów kartowych i wykorzystania kart elektronicznych