SZKOLENIE ŚREDNIO ZAAWANSOWANE

Programowanie kart Java Card

J/CARD

Czas trwania: 5 dni (40h)

Programowanie i wykorzystanie kart Java Card w celu zabezpieczenia systemów

Cele szkolenia

- Poznanie architektury i możliwości Java Card oraz zasad tworzenia apletów z użyciem symulatora i rzeczywistej karty
- Poznanie i wykorzystanie algorytmów i protokołów kryptograficznych używanych w systemach kartowych
- Praktyczna umiejętność obsługi czytników kart w aplikacjach poprzez interfejs PC/SC w językach C/C++ i Java na platformach Windows, Linux i macOS
- Poznanie zasad i dobrych praktyk w zakresie tworzenia bezpiecznych systemów kartowych na przykładach takich jak podpis elektroniczny, dostęp do systemów, systemy płatności oraz dystrybucja i udostępnianie kluczy

Zalety

- Podczas warsztatów uczestnicy przygotują własne aplety dla Java Card oraz umieszcza je w symulatorze i rzeczywistej karcie
- Uczestnicy dokonają ataku na nieprawidłowo zabezpieczony system kartowy
- W trakcie szkolenia zaimplementujemy protokół wzajemnego uwierzytelnienia pomiędzy kartą i aplikacją oraz pomiędzy dwiema kartami
- Elementem warsztatów jest realizacja mechanizmu zabezpieczonej komunikacji pomiędzy terminalem a kartą
- Uczestnicy przygotują aplikację wykorzystującą czytnik zgodny z PC/SC
- Praktyka przed teorią - wszystkie szkolenia technologiczne prowadzone są w formie warsztatowej. Konieczna teoria jest wyjaśniana na przykładzie praktycznych zadań
- Konkretne umiejętności - w ramach każdego szkolenia rozwijamy praktyczne umiejętności związane z daną technologią i tematyką
- Nauka z praktykami - wszyscy trenerzy na co dzień pracują w projektach, gwarantuje to dostęp do eksperckiej wiedzy i praktycznego know-how

Dla kogo?

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

Wymagania

- Od uczestników szkolenia wymagana jest umiejętność programowania na poziomie podstawowym w Java oraz (opcjonalnie) C/C++

Program

1. Wprowadzenie do kart elektronicznych
    a. Klasyfikacje kart
    b. Budowa fizyczna, wymiary
    c. Interfejsy komunikacyjne
    d. Karty stykowe
    e. Karty bezstykowe, NFC (near-field communication)
    f. Techniki komunikacji z kartami, czytniki kart
    g. Karty pamięciowe i inteligentne
    h. Karty natywne i programowalne
    i. Zastosowania kart elektronicznych
    j. Ogólna charakterystyka kart Java Card
2. Algorytmy i protokoły kryptograficzne
    a. Podstawowe usługi ochrony informacji
    b. Integralność, uwierzytelnienie, niezaprzeczalność i poufność
    c. Funkcje skrótu: rodzina SHA, SHA3
    d. Algorytmy symetryczne: AES, 3DES
    e. Kody uwierzytelniające wiadomość (message authentication code, MAC): CMAC, HMAC
    f. Tryby uwierzytelnionego szyfrowania (authenticated encryption with associated data, AEAD)
    g. Ceremonia wymiany klucza
    h. Krzywe eliptyczne w kryptografii: krzywe NIST, SECG i Brainpool, Curve25519, Curve448
    i. Algorytmy uzgadniania klucza: DH, ECDH, X25519, X448
    j. Algorytmy asymetryczne: RSA, ECDSA, EdDSA, Ed25519, Ed448
    k. Podpis cyfrowy (digital signature)
    l. Generatory liczb losowych i ich zastosowania
    m. Podstawy notacji ASN.1
    n. Kodowanie DER (Distinguished Encoding Rules) i PEM (Privacy-Enhanced Mail)
    o. Problem bezpiecznego przechowywania informacji
    p. Przechowywanie i przekazywanie danych kryptograficznych
    q. Sprzętowe moduły bezpieczeństwa (hardware security module, HSM)
    r. Dostęp do urządzeń kryptograficznych (biblioteki PKCS #11, CSP)
    s. Zalecenia dotyczące parametrów algorytmów kryptograficznych
    t. Protokół wyzwanie-odpowiedź
    u. Zabezpieczanie komunikacji
3. Karty inteligentne Java Card
    a. Architektura kart Java Card
    b. Wersje platformy Java Card, Java Card Kit
    c. Java Card Virtual Machine
    d. Java Card Runtime Environment

e. Java Card API
f. Identyfikatory (AID) pakietów i instancji, RID i PIX
g. Środowisko rozwoju apletów
h. Symulator Java Card Platform Simulator (cref)
i. Działanie Card Managera
j. Aplikacje GPShell i GlobalPlatformPro
k. Obsługa komend APDU
l. Obsługa pamięci nieulotnej i ulotnej
m. Obsługa kodu PIN
n. Obsługa transakcji atomowych
o. Bufory z danymi o szczególnym znaczeniu
p. Obsługa ciągów znaków
q. Obsługa upływu czasu
r. Liczniki
s. Obsługa struktur danych TLV
t. Generatory liczb losowych
u. Sumy kontrolne
v. Wykorzystanie algorytmów kryptograficznych w kartach
w. Funkcje skrótu
x. Kody uwierzytelniające wiadomość
y. Algorytmy symetryczne i asymetryczne, generowanie kluczy
z. Szyfrowanie i deszyfrowanie
aa. Składanie podpisu elektronicznego
ab. Techniki biometryczne
ac. Zabezpieczanie komunikacji z kartami
ad. Komunikacja pomiędzy apletami
ae. Serwisy
af. Komunikacja z Card Manager
ag. Dostęp do zasobów zewnętrznych
ah. Zalecenia dotyczące tworzenia wydajnych apletów Java Card
ai. Optymalizacja wykorzystania pamięci
aj. Techniki i zalecenia dotyczące testowania apletów Java Card

4. Aplikacje wykorzystujące karty
   a. Czytniki kart inteligentnych
   b. Interfejs PC/SC
   c. Obsługa zdarzeń w czytniku
   d. Typowe problemy związane z obsługą kart stykowych i bezstykowych
5. Karta jako bezpieczny nośnik informacji
   a. Cykl życia karty
   b. Personalizacja kart
   c. Techniki dystrybucji kluczy
   d. Moduły SAM (secure access module)
   e. Przechowywanie i zarządzanie danymi użytkowników
   f. Karty w systemach podpisu elektronicznego

g. System płatniczy EMV
h. Systemy dostępu
i. Dobre praktyki tworzenia systemów kartowych i wykorzystania kart elektronicznych