SZKOLENIE ZAAWANSOWANE

Sprzętowe układy zabezpieczeń dla urządzeń IoT

SAM/IOT

Czas trwania: 4 dni

Techniki wykorzystania sprzętowych układów zabezpieczeń dla urządzeń i systemów IoT na przykładzie układów A71CH i EdgeLock SE050

Cele szkolenia

- Poznanie możliwości układów A71CH i EdgeLock SE050 oraz technik ich wykorzystania do zabezpieczania platform IoT
- Zdobycie umiejętności praktycznej pracy z układami A71CH i EdgeLock SE050, zarówno w procesie rozwoju oprogramowania jak i jego produkcyjnego działania
- Zrozumienie celu i sposobu stosowania algorytmów i protokołów kryptograficznych do zabezpieczania pracy i komunikacji urządzeń IoT
- Poznanie dobrych praktyk związanych z procesem wdrożenia i wykorzystania sprzętowych układów zabezpieczeń

Zalety

- Podczas warsztatów uczestnicy samodzielnie uruchomią i spersonalizują układy A71CH oraz EdgeLock SE050
- Efektem szkolenia będzie implementacja różnorodnych scenariuszy użycia modułów m. in. zabezpieczenia komunikacji sieciowej, ochrony firmware za pomocą podpisu cyfrowego oraz zdalnej aktualizacji parametrów układu
- W wersji dedykowanej szkolenie może być zrealizowane w oparciu moduł i tematykę warsztatów zaproponowaną przez uczestników

Dla kogo?

- Szkolenie adresowane jest do osób tworzących rozwiązania dla szeroko pojętych systemów typu IoT chcących wykorzystać układy sprzętowe do ich zabezpieczenia
- Programiści, projektanci, oraz architekci systemów zabezpieczeń

Wymagania

- Od uczestników szkolenia wymagana jest umiejętność programowania w języku C lub Java
- Zalecany jest udział w szkoleniu Praktyczne aspekty stosowania kryptografii w systemach komputerowych (CRYPT/F) lub Infrastruktura Klucza Publicznego (PKI)

- Zalecana jest ogólna znajomość problematyki programowania i komunikacji na platformach wbudowanych

Program

1. Przegląd algorytmów i protokołów kryptograficznych
   a. Funkcje skrótu: SHA-256
   b. Algorytmy symetryczne: 3DES, AES
   c. Kody uwierzytelniające wiadomość
   d. Algorytmy asymetryczne: RSA, ECDH, X25519, X448, ECDSA, EdDSA, Ed25519, Ed448
   e. Budowa kluczy kryptograficznych
   f. Generowanie liczb losowych
   g. Uzgadnianie klucza
   h. Operacje szyfrowania i podpisu elektronicznego
   i. Infrastruktura Klucza Publicznego (public key infrastructure, PKI)
   j. Protokół TLS i DTLS
   k. Protokół SCP03 i FastSCP
2. Scenariusze użycia sprzętowych modułów zabezpieczeń
   a. Personalizacja modułów
   b. Uwierzytelnienie
   c. Szyfrowanie danych
   d. Zdalna aktualizacja modułów
   e. Zabezpieczenie komunikacji z hostem
   f. Blokowanie modułów
3. Układ A71CH
   a. Architektura rozwiązania i możliwości modułu
   b. Dedykowane konfiguracje dla AWS, IBM Watson IoT Platform, and Google Cloud IoT Core
   c. Protokół SMBus
   d. Personalizacja i czyszczenie modułu deweloperskiego
   e. Praca w trybie debug
   f. Zabezpieczanie danych i transakcji
   g. Wykorzystanie liczników
   h. Rola modułu w protokole TLS
   i. Bezpieczne przechowywanie danych
   j. Zdalna aktualizacja układu
   k. Zabezpieczona komunikacja z hostem
   l. Przejście w tryb produkcyjny
   m. Blokada modułu
4. EdgeLock SE050
   a. Architektura rozwiązania i możliwości modułu w odniesieniu do A71CH
   b. Typy obiektów w module, obiekty tymczasowe i stałe
   c. Obiekt UserID
   d. Rodzaje sesji
   e. Personalizacja i czyszczenie modułu deweloperskiego
   f. PCR (Platform Configuration Register)
   g. Eksport i import obiektów
   h. Zabezpieczona komunikacja z hostem

i. Dywersyfikacja kluczy kryptograficznych
j. Uwierzytelnienie kart inteligentnych
k. Rola modułu w protokole TLS
l. Zabezpieczona komunikacja E2E (end to end)
m. Wsparcie dla WiFi
n. Komunikacja z wykorzystaniem NFC (near-field communication)

5. Alternatywne moduły bezpieczeństwa
   a. Karty inteligentne Java Card
   b. OPTIGA Trust X
   c. ATECC608A
   d. ATAES132A