securITum

CERTYFIKAT

UCZESTNICTWA W SZKOLENIU

PRAKTYCZNE WPROWADZENIE DO HACKOWANIA SPRZĘTU

DLA:

Robert Diak

DATY: 7, 14 i 21.11.2024 r. | **TRENER:** Piotr Rzeszut | **CZAS TRWANIA:** 8 godzin

AGENDA

Interfejsy międzyukładowe i pamięci w systemach wbudowanych:

- Czym są systemy wbudowane?
- Gdzie szukać zagrożeń bezpieczeństwa systemu?
- Interfejsy komunikacji międzyukładowej – I2C, SPI.
- Obserwacja interfejsów za pomocą analizatora stanów logicznych.
- Identyfikacja układu scalonego i podłączenie programatora.
- Analiza i modyfikacja zawartości pamięci w celu przeprowadzenia ataku.

Interfejsy komunikacyjne:

- Przegląd najpopularniejszych interfejsów komunikacyjnych (RS232, RS485, CAN).
- Obserwacja każdego z interfejsów za pomocą oscyloskopu i analizatora stanów logicznych.
- Metody analizy przesyłanych danych.
- Ataki różnych typów – *capture*, *repeat*, *brute-force* (RS232, RS485).
- Metody zabezpieczania danych – sumy kontrolne, proste algorytmy szyfrujące.

Zagadnienia zaawansowane i sesja Q&A:

- Kompleksowa analiza systemu – interfejsy, pamięci, szyfrowanie i zabezpieczenia.
- Wstrzykiwanie danych do interfejsu CAN.
- Proste błędy w oprogramowaniu – *stack overflow*.
- Demonstracja wykorzystania w praktyce podatności *stack overflow* – wstęp do Return Oriented Programming.
- Ghidra – czyli co można wywnioskować z deasemblacji kodu?
- Sesja Q&A.

PUNKTY CPE/ECE: 8

SZKOLENIA.SECURITUM.PL