INFORISK360°™

Beyond IT Security Training. We Train Differently

With IoT,

Everything is Connected,

including CYBER ATTACKS!

Are you ready?

Join our international IoT/Embedded Device Hacking Training in Malaysia and learn from world class experts!

IoT/Embedded Device Hacking Training

Venue: Condition Zebra Professional Learning Centre
Date: 5 days
Time: 9.00am – 5.00pm

Embedded and IoT device hacking is growing concern across the globe. However, if you have never had any experience in reverse engineering or embedded system hacking, you might be afraid of getting started in. This training course is designed to help people working in the information security industry to learn basic knowledge needed to hack and reverse-engineer embedded system. The training covers embedded device hacking with UART/JTAG, dumping/parsing/extracting/analyzing firmware image, modifying firmware, detecting/analyzing embedded malware, discovering/exploiting vulnerabilities in firmware, and wireless hacking using SDR.

Who Should Attend:
Professionals who are working in information security industry and interested to expand their hacking and reverse engineering skills in IoT/embedded device.

Prerequisite Knowledge and Requirements:
1. Should be familiar with using Windows, Linux and VMWare
2. Should have an understanding of programming concepts, but programming experience is not mandatory
3. Background knowledge in reverse code engineering and vulnerability assessment will be helpful, but not required.
4. Enthusiasm is a must.

What will be offered to attendees:
- Training materials
- Lab instruction note
- Videos used in the course
- Linux virtual machine image containing necessary tools
- Various tools and devices used in hand-on practice

Course Outline:

Module 1: Hunting for UART ports
- Basics of asynchronous serial communication and UART
- How to identify UART pinout and determine the configurable parameters using logic analyzer
- How to connect to UART
- Meanings of debug and status message from the UART and what we can do with the message
- How to get into the shell through the UART and figure out the credentials that is needed to log in
- Real-world case study

Module 2: Hacking Embedded Device with JTAG
- JTAG Basics and JTAG state machine
- How to identify the test access points (TAPs) using various techniques and tools
- How to connect to JTAG
- Various techniques for hacking embedded device with JTAG including boot argument patching, kernel patching, process patching, pin/port control
- Understanding of secure JTAG
- Real-world case study

Module 3: Firmware Acquisition
- Flash Memory Basics
- SPI basics and SPI Bit banging
- How to acquire the firmware using invasive and non-invasive method

Module 4: Firmware Unpacking
- Entropy analysis and signature analysis
- How to utilize the entropy and signature analysis to analyze the layout of the firmware
- Various tools and techniques to unpack the firmware

Module 5: Basics of Reverse Engineering ARM/MIPS Code
- Basics of ARM/MIPS architecture
- ARM/MIPS instructions
- Understanding of ARM/MIPS stack
- Understanding of ARM/MIPS procedure call standard
- Code Patterns
- How to determine the base address of boot code

Module 6: Embedded Device Vulnerability Assessment
- Discovering developer backdoor in embedded system
- Discovering and exploiting command injection vulnerabilities
- Discovering and exploiting buffer overflow vulnerabilities
- Crypto attack basics

Module 7: Introduction to Side Channel Analysis Attack
- Side channel attack overview
- Software based side channel attack
- Simple power analysis
- Bypassing security mechanism using SPA

Module 8: Modifying Firmware for Fun and Profit
- Boot process of embedded Linux and the inner mechanism of secure boot
- How to modify firmware
- Various methods for bypassing secure boot

Module 9: Hacking Wireless Network
- Basics of Software Defined Radio
- Basics of GNU Radio
- Identifying Modulation
- Digital Filters
- Converting radio signal to digital data
- Basics of Bluetooth
- Hacking Bluetooth Network

Trainer Profile:

Tae-il Kim
Founder & CEO of Core Security (Korea)

Tae-il has about 20 years' extensive lecturer experience in information security industry since 1999. He is one of the most famous instructors in Korea. He has lectured about reverse engineering, penetration testing, digital forensics, exploit writing, and embedded device hacking at Korean government agencies (Korea National Police Agency, Korea Internet Security Agency, Ministry of National Defense, Cyber Command, Republic of Korea Army, and so on) and the international institute and companies (Philippine Interpol, Hyundai Motor Group, LG Electronics, Samsung Advanced Technology Training Institute, and so on).

Genie Choe
Information Security Researcher of Core Security (Korea)

She studied a wide knowledge of IT area, such as programming, mechanics, network, and computer engineering during her higher education years. Based on her great interest in electronic hardware, she started her career as a researcher in IoT security in CoreSecurity. She also has been researching in various information security field such as Malware Analysis, Network Security, and operation system vulnerability. Not only she achieved excellent performance on IoT security core but also she sincerely has been willing to share her knowledge to contribute securing industries. So she has been training IT specialist in various countries. She opened an embedded device hacking course in Mahidol University, the top university in Thailand. She delivered her knowledge successfully to participants from government agencies, national banks, militaries and police departments.