Industrial Cybersecurity Training programs

kaspersky

IoT vulnerability research and exploitation

Nowadays, most companies and individuals own one or more smart devices. Internet of Things (IoT), essentially includes such embedded devices and their ecosystem. For security professional, new skillsets such as firmware reverse engineering, hardware communications and radio frequency analysis are now essential to fully encompass the whole attack surface during a security assessment.

Learning objectives

We will guide you through systematic analyses of IoT devices to identify vulnerabilities.

You will interact directly with hardware interfaces, and become comfortable with using hardware and software tools to evaluate IoT devices and their firmware.

After having experimented with different devices, you will have a chance to apply your newly acquired skills by conducting a penetration test against a simulated environment.

After the training, you will be able to analyze and exploit the hardware and software attack surfaces of IoT devices to secure them.

Going forward you will tackle most situations confidently, including when the firmware is not publicly available. You will also develop an instinct for approaching uncommon targets.

Course topics

- Vulnerability research methodologies
- Hardware reconnaissance and PCB reverse engineering
- Hardware interfaces security (UART, SPI, I2C, JTAG)
- Firmware extraction, analysis and emulation
- Reverse engineering custom of binaries and protocols
- Wireless protocols security
- Automation of static binary analysis tools
- Fuzzing embedded targets executables and libraries

Training prerequisites

- Experience with C/C++, Python or any other programing language
- Familiarity with basic Linux commands
- Basic reverse engineering skills
- Knowledge of the most common network protocols
- Experience using a disassembly tool would be helpful, but not necessary

Course format

Onsite instructor led lessons, workshop, hands-on sessions. A hybrid or online format is possible

Duration

3 days

Group

Up to 10 people

Who can benefit:

- Security researchers
- Penetration testers
- Product security teams
- Software and security architects
- Technical product managers

Resources

- Course materials
- Target IoT devices and firmware
- Hardware toolbox for device analysis
- Lab manuals