Updated 07/26/2023

Sign up

IoT and Embedded Systems Security Conversion Training

5 days (35 hours)

PRESENTATION

With the growing use of connected objects, protection of the Internet of Things (IoT) is essential. Being able to protect against attacks targeting connected objects will enable you to safeguard your customers' data and gain a definite competitive edge.

After completing this comprehensive 5-day training course, you'll be ready to become an IoT and embedded systems security professional. This course will teach you about the different types of attack and how to protect against them, embedded system architecture, hardware hacking, software access and different protection methods.

This IoT and embedded systems security retraining course will include numerous practical exercises based on attack/defense scenarios. These practical exercises will improve your ability to perform in real-life situations.

OBJECTIVES

- Know how to carry out hardware security audits
- Be able to react to an attack on IoTs or embedded systems

TARGET AUDIENCE

- IT security professionals
- People interested in hardware or embedded safety issues
- Electronics enthusiasts and professionals

Prerequisites

- Command-line proficiency in Linux is a plus
- Windows/Linux administration

PROGRAM OF OUR RETRAINING COURSE IN EMBEDDED AND IOT SYSTEMS SECURITY

Fundamentals

- The special features of embedded systems
- System architectures
- Disadvantages of using embedded systems

Cyber attacks

- Different types of attack
- Cybersecurity players
- Analysis and penetration testing

Embedded and IoT presentation

- Embedded operating systems: Win, Linux or Raspbian
- The different networks (LTE, WiFi, 4G, LoRA...)
- Presentation of the various components (chip, JTAG, UART, camera, etc.)
- Cryptography
- Architecture (ARM, MIPS, SuperH)
- Practical work: Discovering Arduino and Raspberry boards

Embedded architecture vulnerabilities

- The most important vulnerabilities
- Vulnerability scanning
- Different authentication methods
- Connectivity: network, sensor and peripheral
- Intrusion testing methodology
- Analyzers
- Debug
- Désass and Décompil
- TP: Security level of an embedded architecture

Introduction to Hardware Hacking

- Overview of attacks on connected objects
- Vulnerability overview
- Introduction to electonics

- TP: Taking information about the target (component fingerprint)

Hardware intrusion

- How to audit a product
- Audit plan and differences from software audits
- Practical work: Extracting sensitive data with Hardsploit
- TP: Acquiring electronic signals, tools and demonstration

Access the software

- Microcontroller and FPGA architecture
- I/O interfaces (I2C, JTAG / SWD, SPI...)
- Side channel attacks
- TP: Firmware access via different interfaces

Attacks on connected objects

Securing your equipment

- Cycle SDLC
- Good safety practices
- Limit JTAG access
- Embedded vulnerabilities
- Protect yourself against side-channel attacks

SDR Hacking

- Setting up an SDR audit
- Presentation of tools (GNURadio, etc.)
- Practical work: Reverse engineering a wireless protocol

Capture the Drone or the Car" exercise

- Attack-defense scenario for a mini-drone or a connected car

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.