Internet of Things (IoT)

Hacking

3-Day Course

Syllabus

AppSec Labs Ltd.

info@appsec-labs.com | https://appsec-labs.com | 23 HaTa'as St., Kfar Saba 44641 Israel | T: +972-9-7485005 | F: +972-9-7730595

IoT Hacking

3-day course

Course description

The "things" are all around us, with more to come exponentially as days go by. Smart homes, connected cities, smart medical devices, industrial IoT, you name it – they all are targets for attacks that were not possible up until recent years, when they can be accessed from the cloud and controlled from your favorite mobile app.

During this course, we will cover security vulnerabilities that exists in IoT products. We'll go over each of those vulnerabilities, and witness how they can be exploited by having a demo of the tools and techniques attackers will use against our IoT product.

This training contains Hands-on labs that will give you a practical experience when testing IoT/Connected Devices.

Target audience

Members of the software development team:

- Developers
- Team Leaders
- Red Teams

Prerequisites

Before attending this course, students should be familiar with:

- Basic knowledge of in information systems
- Background knowledge in networking and the internet (WWW)

Course topics

Day 1

Introduction to IoT and Hardware Hacking

- Introduction to IoT security
- Common IoT Architectures
- Hardware security
- Scada security
- Introduction to microcontrollers & major electronic components
- Tools used in hardware hacking
- Attacks & Misconceptions

IoT Top 10 Security Attacks

- Insecure Web Interfaces
- Mobile App Attacks
- Local Memory and Storage
- Device Physical Interfaces
- Device Firmware
- Insecure Network Services
- Insecure Network Traffic
- Authentication Vulnerabilities
- Authorization Vulnerabilities
- Denial of Service (DoS) Attacks

Information gathering

- Device Unpacking
- PCB Analysis
- Google Information Gathering
- Data Sheets
- FCC
- **Hands-on Lab: PCB analysis**

Serial and Connections

- Identifying Inputs
- SPI, I2C, UART
- Using Bus Pirate
- Using GoodFET
- Getting Console/Shell
- **Hands-on Lab: Getting a shell from a UART connection**

Day 2

Debug

- Using Logic Analyzer
- Signal Monitoring
- Digital Decoding
- JTAG Overview
- Identifying JTAG Pins
- Using Jtagulator
- Using OpenOCD
- JTAG Debugging

Flash & Chip manipulations

- Using a Device Programmer
- Connecting using SPI and I2C
- In-circuit Connection
- Pulling off the Chip
- Dumping the Content of a Chip
- Patching Flash Content
- Uploading a Modified Binary to Chip
- **Hand-on Lab: Dumping the content of a flash chip**

Firmware analysis

- Getting the Device Firmware
- Using binwalk
- Reversing the Binary with IDA
- Patching Important Executables
- Bypassing Limitations
- Uploading Modified Firmware
- **Hands-on Lab – Firmware Reverse Engineering**

Day 3

Introduction to wireless security

- Frequency
- Channel width
- Modulation
- Bit rate
- Preamble
- Sync word
- CRC?
- Whitening
- Software defined Radio (SDR)

Wifi Security

- Access points interrogation
- WEP, WPA, WPA2
- SSID
- Netstumbler
- AirSnort
- Kismet
- AirCrack
- War driving
- **Lab – hacking a wireless AP**

Attacking RF based system

- Traffic analysis
- Replay attacks
- Construction of a RF message from scratch
- Transmission of specially crafted RF traffic
- Message tampering
- Avoiding CRC mismatches
- Jamming
- **Hands-on Lab: RF signal Analysis**

Bluetooth Low Energy (BLE) security

- Introduction to Bluetooth Low Energy (BLE)
- Proxy
- Man in the Middle
- Bypassing Authentication
- Breaking the Crypto
- Sniffing
- Attacking BLE devices and Mobile apps
- **Hands-on Lab: BLE Man-in-the-Middle attack**