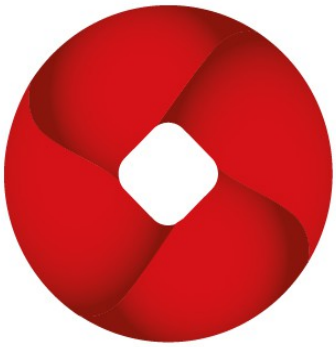

Payatu

Practical IoT Hacking Training

Duration : 3 Days

Payatu Technologies Pvt. Ltd
502, Tej House, M.G Road,
Camp, Pune – 411001
Maharashtra, India.
www.payatu.com

Duration

Three days training

Overview

"The great power of Internet Of Things comes with the great responsibility of security". Being the hottest technology, the developments and innovations are happening at a stellar speed, but the security of IoT is yet to catch up. Since the safety and security repercussions are serious and at times life threatening, there is no way you can afford to neglect the security of IoT products.

"Practical Internet of Things (IoT) Hacking" is a research backed and unique course which offers security professionals, a comprehensive understanding of the complete IoT Technology suite including, IoT protocols, sensors, client side, mobile, cloud and their underlying weaknesses. The extensive hands-on labs enable attendees to master the art, tools and techniques to find-n-exploit or find-n-fix the vulnerabilities in IoT, not just on emulators but on real smart devices as well.

The course focuses on the attack surface on current and evolving IoT technologies in various domains such as home, enterprise Automation. It covers grounds-up on various IoT protocols including internals, specific attack scenarios for individual protocols and open source software/hardware tools one needs to have in their IoT penetration testing arsenal. We also discuss in detail how to attack the underlying hardware of the sensors using various practical techniques. In addition to the protocols and hardware we will extensively focus on reverse engineering mobile apps and native ARM/MIPS code to find weaknesses.

Throughout the course, We will use DRONA, a VM created by us specifically for IoT penetration testing. DRONA is the result of our R&D and has most of the required tools for IoT security analysis. We will also distribute DIVA – IoT, a vulnerable IoT sensor made in-house for hands-on exercises.

The "Practical Internet of Things (IoT) Hacking" course is aimed at security professionals who want to enhance their skills and move to/specialise in IoT security. The course is structured for beginner to intermediate level attendees who do not have any experience in IoT, reversing or hardware.

Course outline

* Introduction to IOT
* IOT Architecture
* IoT attack surface

* IoT Protocols Overview

* MQTT
  - Introduction
  - Protocol Internals
  - Reconnaisance
  - Information leakage
  - DOS attack
  - Hands-on with open source tools

* CoAP
  - Introduction
  - Protocol Internals
  - Reconnaissance
  - Cross-protocol attacks
  - Hands-on with open source tools

* CanBus
  - Introduction and protocol Overview
  - Reconnaissance (Active and Passive)
  - Sniffing and Eavesdropping
  - Replay Attack

* Understanding Radio
  - Signal Processing
  - Software Defined Radio
  - Gnuradio
    - Introduction to gnuradio concepts
    - Creating a flow graph
    - Analysing radio signals
    - Recording specific radio signal
    - Replay Attacks

* Radio IoT Protocols Overview

* Zigbee
  - Introduction and protocol Overview
  - Reconnaissance (Active and Passive)
  - Sniffing and Eavesdropping
  - Replay attacks
  - Hands-on with RZUSBstick and open source tools

* BLE
  - Introduction and protocol Overview
  - Reconnaissance (Active and Passive) with HCI tools
  - GATT service Enumeration
  - Sniffing GATT protocol communication
  - Reversing GATT protocol communication
  - Read and writing on GATT protocol
  - L2cap smashing
  - Cracking encryption
  - Hands-on with open source tools

* Expliot – IoT exploitation framework
  - Intorduction
  - Architecture
  - Test Cases

* Mobile security (Android)
  - Introduction to Android
  - App architecture
  - Security architecture
  - App reversing and Analysis

* ARM
  - Architecture
  - Instruction Set
  - Procedure call convention
  - System call convention
  - Reversing
  - Hands-on Labs

* MIPS (If time permits)
  - Architecture
  - Instruction Set
  - Procedure call convention
  - System call convention
  - Reversing
  - Hands-on Labs

* Device Reconnaissance
* Conventional Attacks

* Firmware
  - Types
  - Firmware updates
  - Firmware analysis and reversing
  - Firmware modification
  - Firmware encryption
  - Simulating device environments

* External Storage Attacks
  - Symlink files
  - Compressed files

* IoT hardware Overview
* Introduction to hardware
  - Components
  - Memory
  - Packages

* Hardware Tools
  - Bus Pirate
  - EEPROM readers
  - Jtagulator/Jtagenum
  - Logic Analyzer

* Attacking Hardware Interfaces
  - Hardware Reconnaissance
    - Analyzing the board
    - Datasheets
  - I2C
    - Introduction
    - I2C Protocol
    - Interfacing with I2C
    - Manipulating Data via I2C
    - Sniffing run-time I2C communication
  - SPI
    - Introduction

  - SPI Protocol
  - Interfacing with SPI
  - Manipulating data via SPI
  - Sniffing run-time SPI communication
- UART
  - What is UART
  - Identifying UART interface
    - Method 1
    - Method 2
  - Accessing sensor via UART
- JTAG
  - Introduction
  - Identifying JTAG interface
    - Method 1
    - Method 2

Who should take this course

- Penetration testers tasked with auditing IoT
- Bug hunters who want to find new bugs in IoT products
- Government officials from defensive or offensive units
- Red team members tasked with compromising the IoT infrastructure
- Security professionals who want to build IoT security skills
- Embedded security enthusiasts
- IoT Developers and testers
- Anyone interested in IoT security

Pre-requisites

- Basic knowledge of web and mobile security
- Basic knowledge of Linux OS
- Basic knowledge of programming (C, python) would be a plus

What attendees should bring

- Laptop with at least 50 GB free space
- 8+ GB minimum RAM (4+GB for the VM)
- External USB access
- Administrative privileges on the system

- Virtualization software – VirtualBox 5.X (including Virtualbox extension pack)
- Linux machines should have exfat-utils and exfat-fuse installed (ex: sudo apt-get install exfat-utils exfat-fuse).
- Virtualization (Vx-t) option enabled in the BIOS settings for virtualbox to work
- Latest OS on the host machines (For ex. Windows 7 is known to cause issues)

What attendees will be provided With

- Commercial IoT Devices for hands-on during the class
- DIVA - IoT: custom vulnerable IoT sensor Testbed
- Hardware tools for sensor analysis
- Drona VM - Platform for IoT Penetration testing
- DIVA - ICS: Custom Vulnerable ICS Testbed VM
- Training material/slides (500+ pages) PDFs
- Practical IoT hacking Lab manual (100+ pages) PDF

What to expect

- Hands-on Labs
- Reversing fun
- Getting familiar with the IoT security
- This course will give you a direction to start performing pentests on IoT products

What not to expect

- Becoming a hardware/IoT hacker overnight. Use the knowledge gained in the training to start pentesting IoT devices and sharpen your skills.

About Trainer

Aseem Jakhar is the Director, research at Payatu payatu.com a boutique security testing company specializing in IoT, embedded, mobile and cloud security assessments. He is well known in the hacking and security community as the founder of null - The open security community, registered not-for-profit organization http://null.co.in and also the founder of nullcon security conference nullcon.net and hardwear.io security conference http://hardwear.io He has worked on various security software including UTM appliances, messaging/security appliances, anti-spam engine, anti-virus software, Transparent HTTPS proxy with captive portal, bayesian spam filter to name a few. He currently spends his time researching on IoT security and hacking things. He is an active speaker and trainer at security conferences like AusCERT, Black Hat, Brucon, Defcon, Hack In The Box, Hack.lu, Hack in Paris, PHDays and many more. He is the author of various open source security tools including:

1. ExplIoT – An open source Internet Of Things Security Testing and Exploitation framework - https://bitbucket.org/aseemjakhar/expliot_framework
2. Linux thread injection kit - Jugaad and Indroid which demonstrate a stealthy in- memory malware infection technique. Indroid - https://bitbucket.org/aseemjakhar/indroid Jugaad - https://bitbucket.org/aseemjakhar/jugaad
3. DIVA (Damn Insecure and Vulnerable App) for Android which gamifies Android App vulnerabilities and is used for learning Android Security issues. https://github.com/payatu/diva-android
4. Dexfuzzer – Dex file format Fuzzer. https://bitbucket.org/aseemjakhar/dexfuzzer/src