Training Curriculum

InCTF Hardware CTF Edition

Overview

This document contains the training syllabus for students taking part in InCTF Hardware CTF. It is designed in a hands-on, step by step learning format that makes it easy for people of different skill levels, grasp concepts easily while still being interesting and challenging.

Modules

Each module comprises of an introduction to the field, including the detailing on the submodules to be focused on. The modules are crafted to incorporate exploitation techniques and mitigation methodologies against common vulnerabilities.

The modules are meticulously planned and are designed in a manner geared toward the maximization of efficiency. Our goal is to best prepare the students while taking up the least amount of their time possible. We believe that the more time they dedicate to the cause, the faster they climb the ladder.

The modules are categorised into 5 main categories:

● IOT 101	Internet of Things device security.
● SDR 101	Introduction to software defined radio.
● FWA 101	Firmware analysis.
● ATO 101	Automotive security.
● RFID 101	RFID and smart card hacking.

IOT 101: Internet of Things device Security.

Overview

Physical attacks target the hardware of an IoT system and include breaches at the sensor layer. They typically require physical proximity to the system but can also involve actions that limit the efficacy of IoT hardware. Attackers can tamper with nodes to gain control over sensor nodes or devices in an IoT environment and use that control to extract materials, data and code. With malicious node injection, attackers can physically deploy malicious nodes between legitimate nodes in an IoT network. Also known as a man-in-the-middle (MitM) attack, the malicious nodes can then control operations and the data flowing between linked nodes.

Set 1: Reckon or Background check on hardware.

Performing an external visual inspection of the device ID and other certifications, Internal pictures, exposed interfaces, Frequency which is being used, Markings of compliances and protocols used, External ports and interfaces, USB, Ethernet, SD Card slot, Voltage and Power consumption.

Set 2: Analyzing and Exploiting the device

Identify the various components on the board, datasheets, Identify the pinouts for the Serial interface, Multimeter, Logic analyzer, JTAGulator, connect to the Serial interface using a USB-TTL

Identify the baud rate, Shell, Dump the firmware, modify values on the device, Control the device components via the shell, Bootloader manipulation attacks JTAG, Dump firmware, write new firmware, perform run-time manipulation of the binaries, Flash, Dump data from the flash, Modify and write data back to the device, Glitching based attacks.

Set 3: Hacking Communications (Mobile and Web)

Reverse engineer the mobile application, reveal any information on how the device communicates with the mobile app and vice-versa, ports which are being used, hardcoded firmware download URLs, Command messaging format, Hardcoded SSIDs, Hardcoded encryption keys, Intercept the traffic using a proxy tool, MQTT, COAP.

PREREQUISITES

- Basic Electronics and embedded systems.
- Embedded architectures and coding.
- Basic knowledge about android and web applications.

TAKEAWAYS

- Deep understanding about embedded devices.
- Embedded device security.
- Android and web security.
- Basic firmware analysis.

SDR 101: Introduction to Software Defined Radio.

Overview

Software-defined radio (SDR) is a radio communication system where components that have been traditionally implemented in hardware (e.g. mixers, filters, amplifiers, modulators/demodulators, detectors, etc.) are instead implemented by means of software on a personal computer or embedded system. While the concept of SDR is not new, the rapidly evolving capabilities of digital electronics render practical many processes which were once only theoretically possible.

SET - 1 [Radio IoT Protocols Overview]

Understanding Radio, Signal Processing, Software Defined Radio, GNU Radio, creating a Flow Graph, recording specific radio signal, analyzing radio signals, Replay Attacks.

SET - 2 [BLE]

Bluetooth vs BLE Basics, Understanding and Exploiting, Identify the device information, understand the difference between Bluetooth Classic & BLE Security, Check the services in BLE and check for Read/Write data, Overwrite or change the value of service, MiTM (Man in The Middle) Attack, GATTacking Bluetooth Smart Devices – Introducing a New BLE Proxy Tool.

PREREQUISITES

- Basic knowledge of Python language.
- Laptop with Linux Environment with windows VM (or vice versa).

TAKEAWAYS

- Basic skill set of a RF reverse engineering workflow that applies to all systems.
- Familiarity with RFTools.

FWA 101:Firmware analysis.

Overview

Firmware is a software program programmed on a hardware device. It provides the necessary instructions on how the device communicates with the other computer hardware.

Set 1: Dumping from the device, analyzing firmware, analyze it via strings and hex dump, firmware encrypted, to figure out the entropy, extracting components from the firmware.

Set 2: Extract the file system, API keys, Private certificates, Backdoors, Sensitive URLs, Config files revealing useful information, Emulating the firmware, Identify the architecture, Perform analysis and exploitation via emulation.

Set 3: Reverse engineering firmware binaries, Decompiling and emulating binaries. Identifying Buffer overflows and other software binary specific vulns and exploitation, Bypassing the security protections.

PREREQUISITES

- Assembly(x86) and Embedded C.
- File Systems and Linux Architecture

TAKEAWAYS

- Device firmware analysis.
- Dumping firmware.
- Firmware encryptions.
- Backdoors.

ATO 101: Automotive security.

Overview

The approachability of a vehicle from outside also significantly raises the risk of hacker attacks. Outside attacks (e.g. via mobile phone, Bluetooth or Wi-Fi). Automakers, therefore, need to ensure that information is concocted securely and protected against external access and manipulation. Computer attacks are now a clear and present threat for car drivers, owners, dealers, manufacturers, and even suppliers. Increased automation, vehicle-to-vehicle, and vehicle-to-infrastructure communications and advancements in autonomous driving will fire up computer security and data privacy to authenticity and safety as foundations for consumer reliance and advancing in the automotive industry.

Set 1: Introduction to Vehicle network and bindings of the Communication protocol and Mechanical components of the Vehicle.

Set 2: Understanding of Vehicle protocols like CAN, CAN-FD, MOST, LIN & other protocols. A more in-depth explanation of the CAN protocol and its structure & function.

Set 3: Simulating a vehicle network and understanding the flow of the vehicle network, Evaluate the flow disturbance in the simulation by sending cloned commands.

Set 4: Reversing a vehicle network to understand its function in the field of data it produces in the bus.

PREREQUISITES

- Basic understanding of Linux.
- Basic programming knowledge in Python.
- Knowledge of wire-shark will be an advantage.

TAKE AWAY

- Knowledge of Security in vehicles.
- Basic testing skills to evaluate a network/ECU.

RFID 101: RFID and smart card hacking.

Overview

This module will help students learn about Smart Cards and RFID Technology. This module will help students understand various types and classes of smart cards used focusing especially on HF band. Examples (iClass, Mifare, Mifare Classic, Desfire, NFC). It would enable to understand the basic functionalities of the RFID. And then allow them to learn about existing vulnerabilities and drawbacks existing in the system.

Set 1: Introduction to RFID Tech; Demonstration of Basic Configuration and usage of RFID Cards (Mifare, iClass, Usage of RFID Card Reader and Writers, Android App)

Set 2: Understanding vulnerabilities on iClass (Wiegand Protocol, FSK Modulation & decoding, Replication and cloning attacks)

Set 3: Understanding vulnerabilities on Mifare Classic (Exploiting the weak crypto implementations)

Set 4: Existing tools for breaking security (Proxmark RDV4, Hydra NFC)

PREREQUISITES

- Knowledge of basic electronics

- Basic Python scripting

TAKEAWAYS

- Students after completion of this module are expected to have:

- Basic skills of exploiting vulnerabilities in Smart Cards

- Familiarity with RFID Tools (Proxmark and Hydra NFC)

- Exclusive access to challenges created for through understanding of smart card security.