‹ Dashboard

Why IoT Security

The Internet of Things (IoT) is the network of devices and components that are connected to each other or the internet. These devices serve different purposes from monitoring the heart rate of a person in the form of wearable to making a whole city “smart” in the form of various sensors. The size, cost, and complexity vary depending on the tasks they perform. With the proliferation of these devices everywhere from our offices to our homes, it is important to make sure these devices are doing only their work, and not spying on us or taking commands from anyone else. IoT security is an important field that spreads over device security, network security, and much more.

Prerequisites

- Basic knowledge of computers and the Linux OS
- Basic knowledge of computer networks

What will you learn?

You will learn about the bootloaders used in IoT devices and how to bypass login authentication to access the files on these devices. You will also learn about the communication protocols used by IoT devices and systems.

Sub-sections/topics to be covered:

Bootloader

The bootloader or boot program or bootstrap loader is a special software program that is responsible for locating and loading all the required files i.e. kernel, filesystem, and starting the operating system. Universal Boot Loader (U-Boot) is one of the most popular open-source bootloaders that is used in a lot of different architectures/platforms/devices.

In this section, we will learn about U-Boot, creating emulated IoT devices using Qemu, booting the IoT devices, and bypassing device login to access the files and resources of an IoT device.

MQTT

MQ Telemetry Transport (MQTT) is a lightweight protocol that is widely used by IoT devices to communicate with their brokers/servers situated on remote locations and clouds. The protocol is simple and consumes much less bandwidth and power than its peers, making it best for devices where network bandwidth and power are constrained. It is a two-way communication protocol. MQTT works in a subscribe-publish model. Brokers or servers play middleman for the publishers (producers e.g. sensors) and subscribers (consumers e.g. central monitoring system).

In this section, we will learn the basics of MQTT protocol, how to interact with MQTT brokers, perform enumeration and launch dictionary attacks, exploit known DoS vulnerabilities, and interact with a dummy ICS setup.

AMQP

Advanced Message Queuing Protocol (AMQP) is a standard protocol for passing messages between applications. It is mostly used in business-related applications and provides buffer capacity for incoming/outgoing messages. However, with IoT devices entering the enterprise space, the AMQP implementations like RabbitMQ are being used to send/receive/buffer the messages.