Iot Forensics

- Babbu Rai

Agenda

- Introduction
- Iot Technology Includes
- Iot Forensics
- Collection of Digital Evidence from IoT
- Acquiring a Flash Memory Image
- Acquiring a memory dump using Linux dd command or netcat
- Firmware data extraction by JTAG
- Firmware data extraction by UART

Introduction

The network of devices that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information.

Sources:
NIST SP 800-172
NIST SP 800-172A

The purpose of the IoT Forensics is similar to the one of the Digital Forensics, which is to identify and extract digital information in a legal and forensically sound manner.

Iot Technology Includes

M2M: Machine to machine communications

RFID: Radio Frequency Identification

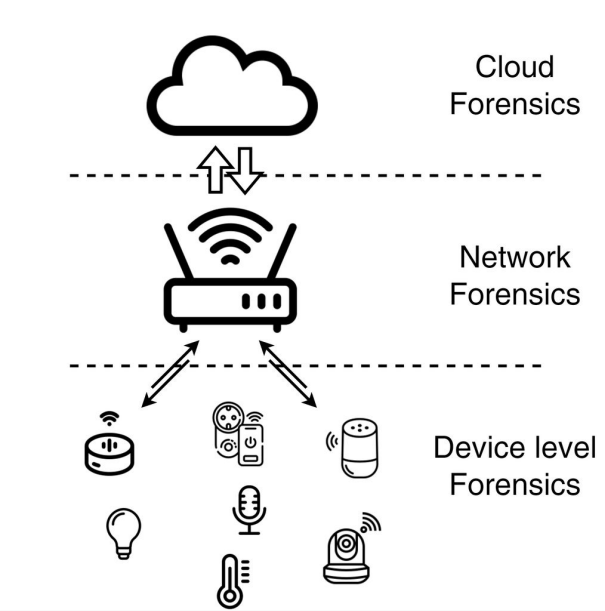
CAC: Context-aware computing

WUC: Wearable and Ubiquitous computing

Iot Forensics

Obtain data From 3 layers of IOT

1. Device Layer
2. Network Layer
3. Cloud Layer



Img

source: Wikipedia

Collection of Digital Evidence from IoT

Since IoT devices come in a variety of models, operating systems, file systems and proprietary hardware and software there is no single standard approach that can be followed in identifying and collecting data from a given IoT device. The following are some methods for collecting the data.

- Acquiring a Flash Memory Image
- Acquiring a memory dump using Linux dd command or netcat
- Extract Firmware data by using JTAG and UART techniques
- telnet
- SSH
- Bluetooth
- Wi-Fi protocols

were also used to gain access and interact with the devices.

Acquiring a Flash Memory Image

In this method, if an IoT device can be connected to a computer, the internal storage of the device can be forensically imaged using forensic imaging utilities such as

- FTK Imager
- X-ways forensics
- ENCASE

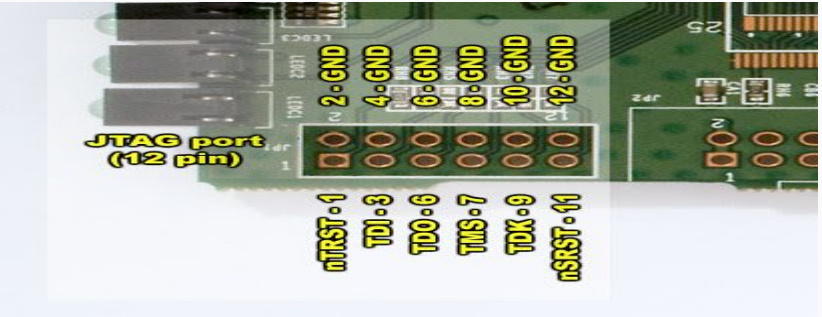
The collected forensic image can be analyzed using the majority of the digital forensic applications. Whenever possible, the flash memory storage device such as NAND/NOR Flash chips, SD/CF/MMC cards has to be imaged in a bit-stream/full physical mode.

Acquiring a memory dump using Linux dd command or netcat

- For IoT devices with operating systems such as Linux or embedded Linux, internal utilities such as Linux dd or netcat can be used to acquire a forensic image of a selected drive or the device memory.
- This requires booting into the device and a terminal access.
- The resultant forensic image can be analyzed to identify and extract information relevant to the case/ incident.

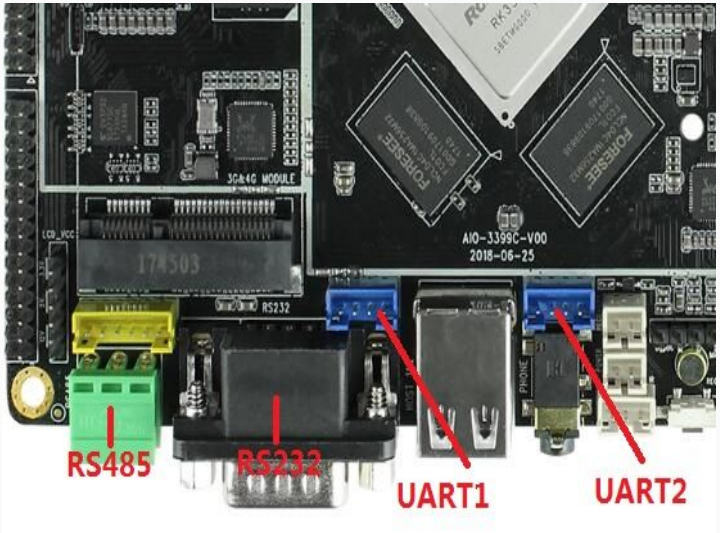
Firmware data extraction by JTAG

- JTAG stands for Joint Test Action Group which was later standardized as IEEE 1149.1 Standard Test Access Port.
- The port was initially designed for testing PCB (Printed Circuit Boards).
- JTAG Forensics involves acquiring firmware data using standard Test Access Ports (TAPS).
- The data is transferred in a raw format.



Firmware data extraction by UART

- UART is Universal Asynchronous Receiver/ Transmitter
- It is a computer hardware device which is a part of Integrated circuitry and used for serial communications over a computer or peripheral device serial port
- Accessing the firmware via UART pins and extracting the data requires specialized interfaces and it is also an invasive technique which can reset the devices to factory settings resulting in loss of data.



References:-

- https://www.slideshare.net/AbeisAb/iot-forensics-117926663
- https://www.intechopen.com/online-first/86010
- https://wiki.t-firefly.com/en/AIO-3399C/driver_uart.html
- https://sergioprado.blog/2020-02-20-extracting-firmware-from-devices-using-jtag/

Thank You

Q/A