OWASP
Open Web Application Security Project

Hacking & Securing IoT Infrastructures

Eng. Mohammad Khreesha
Twitter : @banyrock
Facebook : @khreesha

Whoami

- 13+ Years of IT & Infosec Experience
- Cybersecurity Consultant
- OWASP Amman Chapter Leader
- Youtuber, Blogger, & CTF Maker

OWASP
Open Web Application Security Project

Agenda

- Introduction to IoT
- IoT History
- IoT Applications.
- IoT Issues.
- IoT Attack Vectors
- OWASP IoT Top 10
- IoT Security Testing Scope
- IoT Security Testing Tools
- Questions

OWASP
Open Web Application Security Project

Introduction

- The Internet of Things (IoT) is the network of physical objects or "things" embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data.

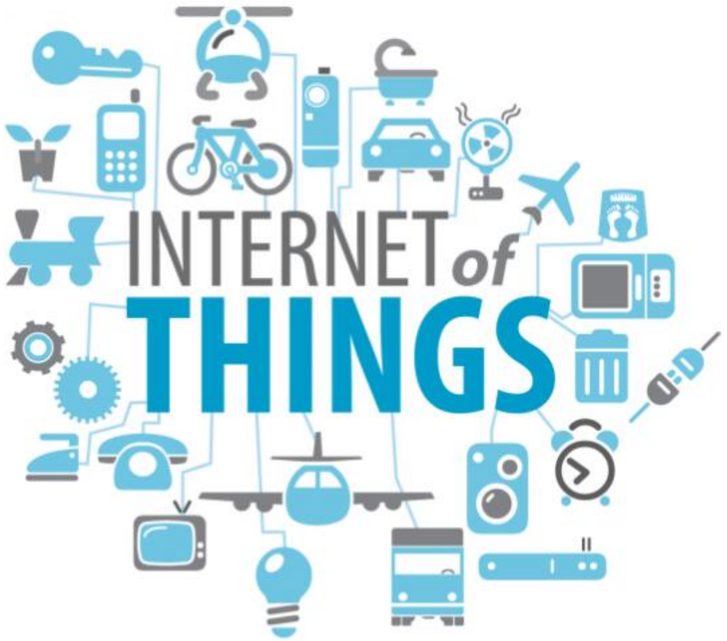
- IoT allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration between the physical world and computer-based systems

- These devices collect useful data with the help of various existing technologies and then autonomously flow the data between other devices

OWASP
Open Web Application Security Project

IoT History

- The concept of the Internet of Things first became popular in 1999, through the Auto-ID Center at MIT and related market-analysis publications.
- Radio-frequency identification (RFID) was seen as a prerequisite for the IoT at that point.
- If all objects and people in daily life were equipped with identifiers, computers could manage and inventory them.
- Besides using RFID, the tagging of things may be achieved through such technologies as near field communication, barcodes, QR codes, bluetooth, and digital watermarking.



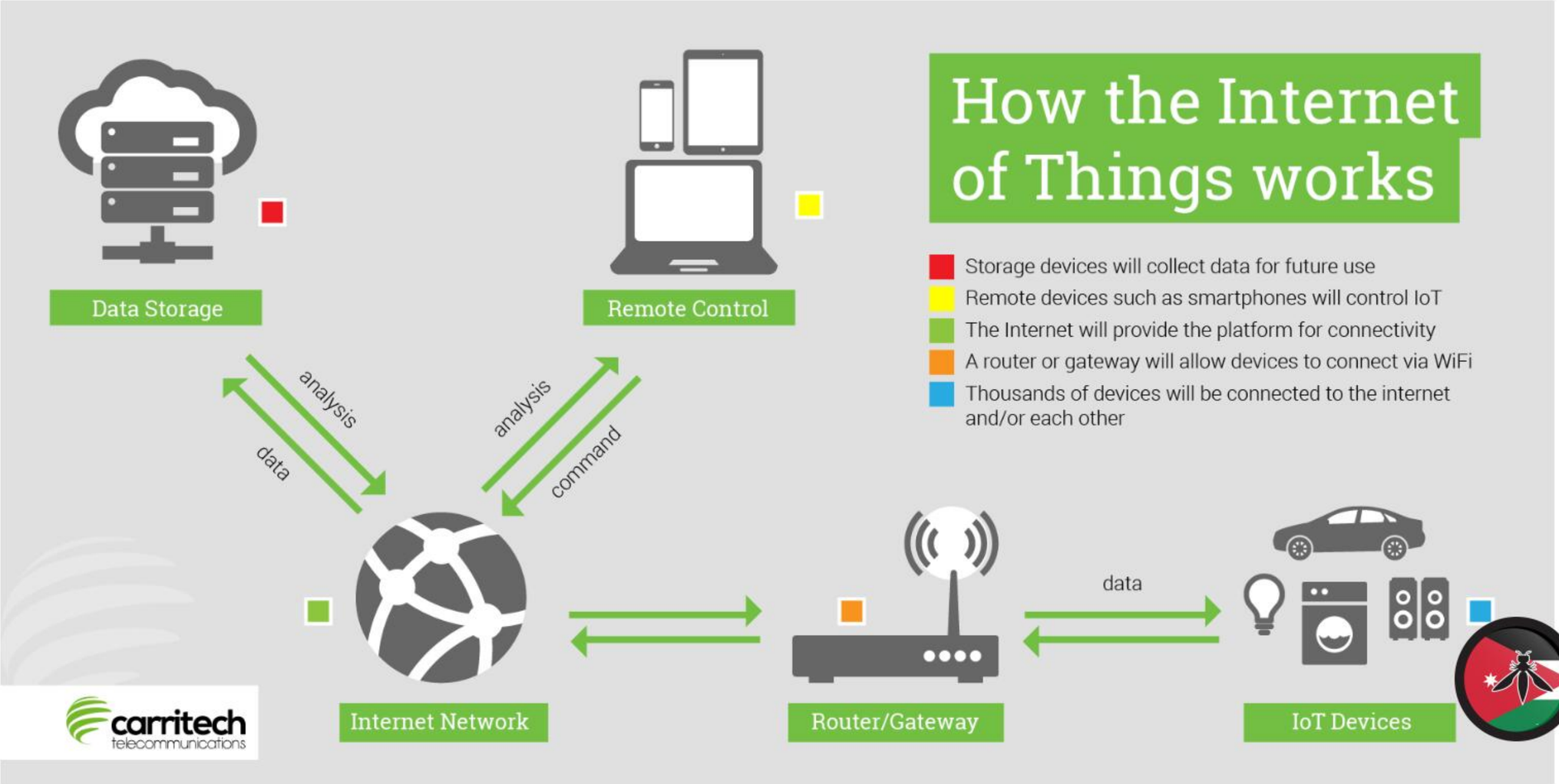
OWASP
Open Web Application Security Project

Essential Terminology

- Device-to-Device Model.
- Device-to-Cloud Model.
- Device-to-Gateway Model.
- Back-End Data-Sharing Model.

OWASP
Open Web Application Security Project

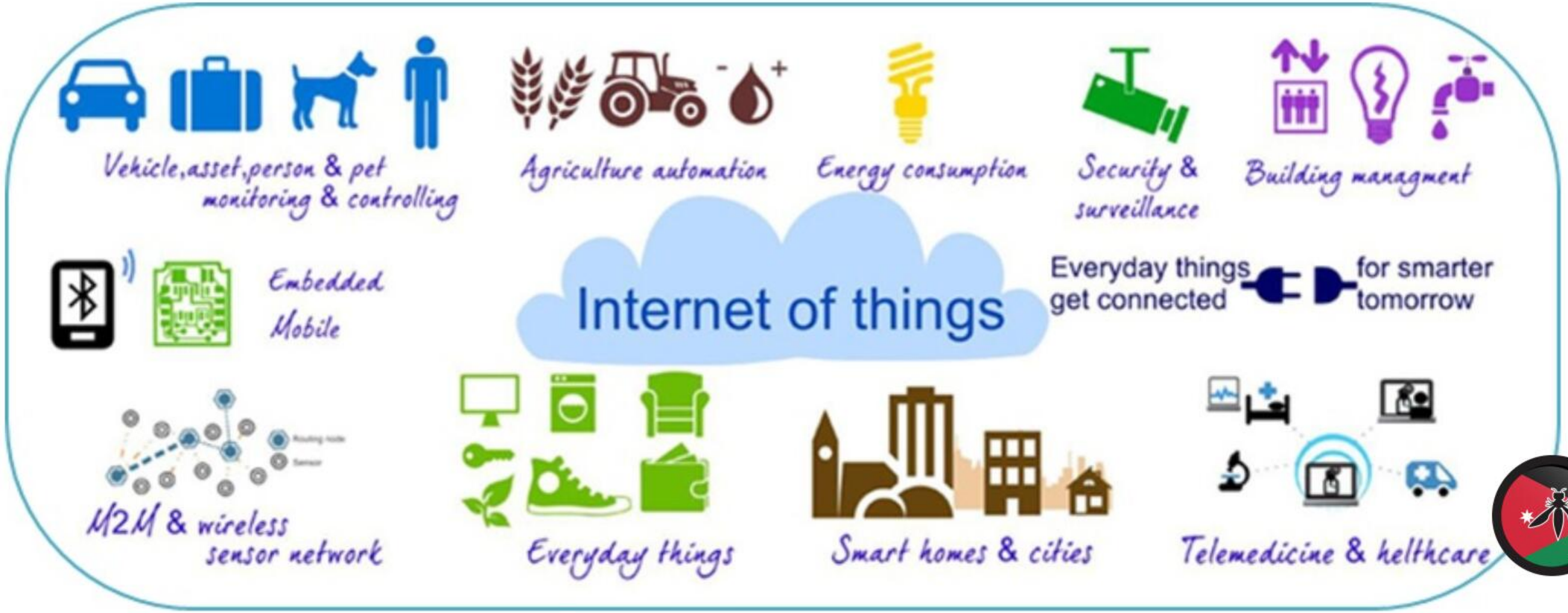
How IoT Works?



OWASP
Open Web Application Security Project

IoT Applications

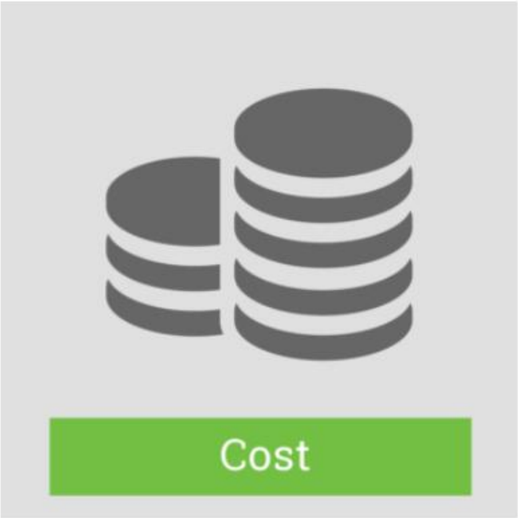
- According to Gartner Inc., there will be nearly 20.8 billion devices on the Internet of things by 2020.



OWASP
Open Web Application Security Project

IoT Issues

- There are three main issues that have arisen since manufacturers have begun to develop IoT enabled devices:



OWASP
Open Web Application Security Project

Design Flow

OWASP
Open Web Application Security Project

Problems of IoT Security

- Initial design was for private communication network then moved to IP network and later on the Internet.
- Firmware updates are hard or nearly impossible after installations.
- Started with basic security then found the security flaws and attached more complex security requirements later.
- Low security devices from early design are still out there and used in compatible fall-back mode.

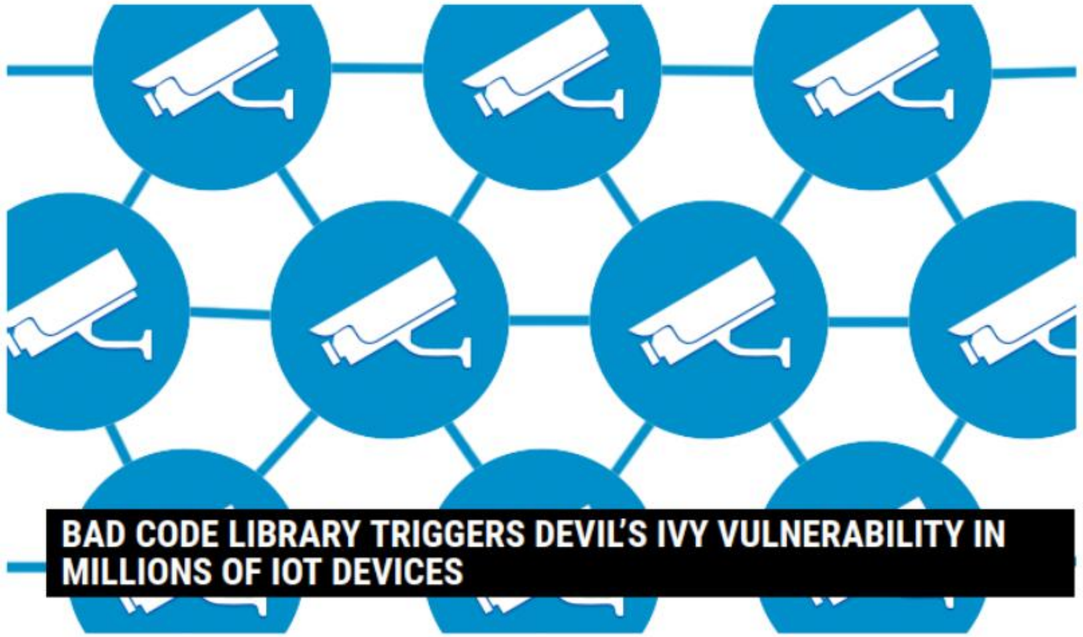
IoT = Internet of Things

IoT = Internet of threats

OWASP
Open Web Application Security Project

Library Flow

Welcome > Blog Home > Cloud Security > Bad Code Library Triggers Devil's Ivy Vulnerability in Millions of IoT Devices



by Tom Spring

July 19, 2017 , 6:00 am

Tens of millions of products ranging from airport surveillance cameras, sensors, networking equipment and IoT devices are vulnerable to a flaw that allows attackers to remotely gain control over devices or crash them.

The vulnerability, dubbed Devil's Ivy, was identified by researchers at Senrio, who singled out high-end security cameras manufactured by Axis Communications. Senrio

Top Stories

Silence Gang Borrows From Carbanak To Steal From Banks
November 1, 2017 , 12:24 pm

Flaw in Google Bug Tracker Exposed Reports About Unpatched Vulnerabilities
October 30, 2017 , 4:39 pm

Chain of 11 Bugs Takes Down Galaxy S8 at Mobile Pwn2Own
November 2, 2017 , 1:35 pm

Popular 'Circle with Disney' Parental Control System Riddled With 23 Vulnerabilities
October 31, 2017 , 5:37 pm

Rockwell Automation Patches Wireless Access Point against Krack
October 27, 2017 , 12:23 pm

Emergency Oracle Patch Closes Bug Rated 10 in Severity
October 31, 2017 , 12:48 pm

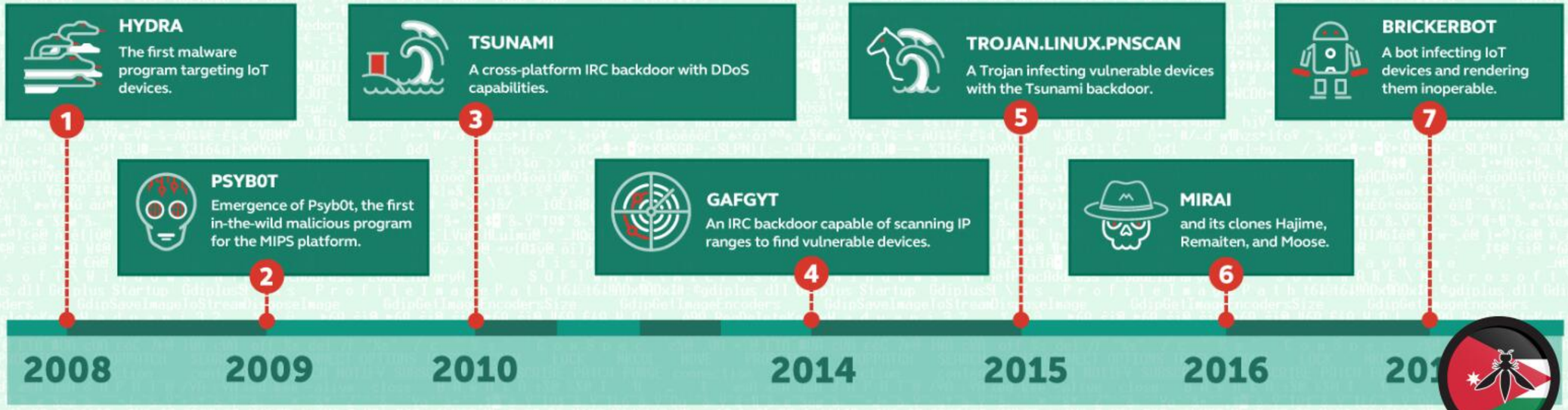
Taking HTTPS Denial to an Absurd Level
November 2, 2017 , 2:01 pm

OWASP
Open Web Application Security Project

Rises of Threats Target IoT Devices

IoT devices at risk: malicious programs target the 'Internet of Things'

Currently, over 6 billion of 'smart' devices exist globally. It was when the Mirai botnet emerged in 2016 that the whole world learned how dangerous such devices may become in the hands of cybercriminals. However, the history of malware attacking IoT devices began much earlier.



© 2017 Kaspersky Lab. All Rights Reserved.

KASPERSKY lab

OWASP
Open Web Application Security Project

Mirai Botnet

The Hacker News

Click to Subscribe

Home | Data Breaches | Cyber Attacks | Vulnerabilities | Malware | Deals | Contact

Mirai Botnet Itself is Flawed; Hacking Back IoTs Could Mitigate DDoS Attacks

October 29, 2016 Mohit Kumar

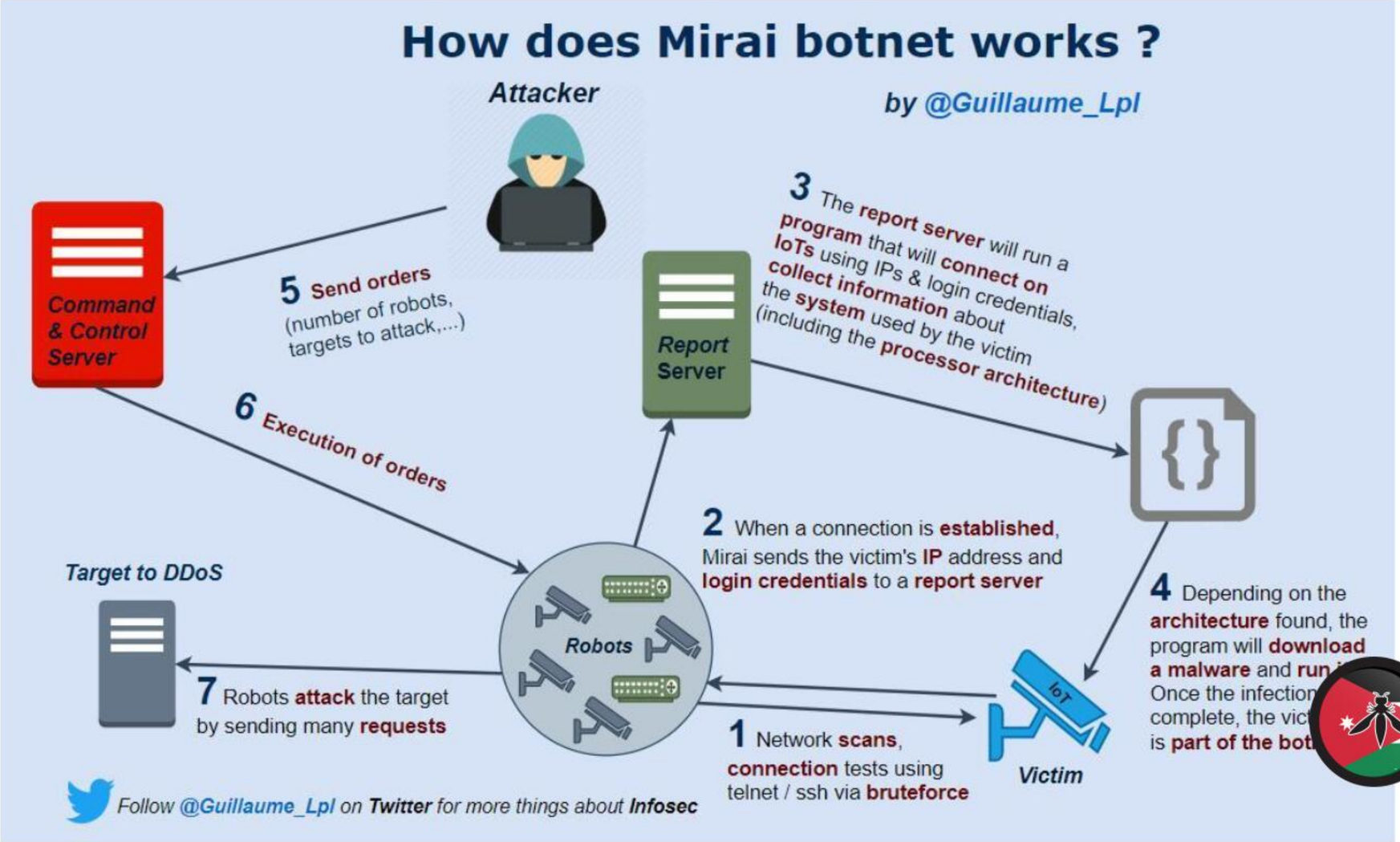
The infamous botnet that was used in the recent massive distributed denial of service (DDoS) attacks against the popular DNS provider Dyn, causing vast internet outage last Friday, itself is flawed.

Popular This Week

Sudo Flaw Lets Linux Users Run Commands As Root Even When They're Restricted

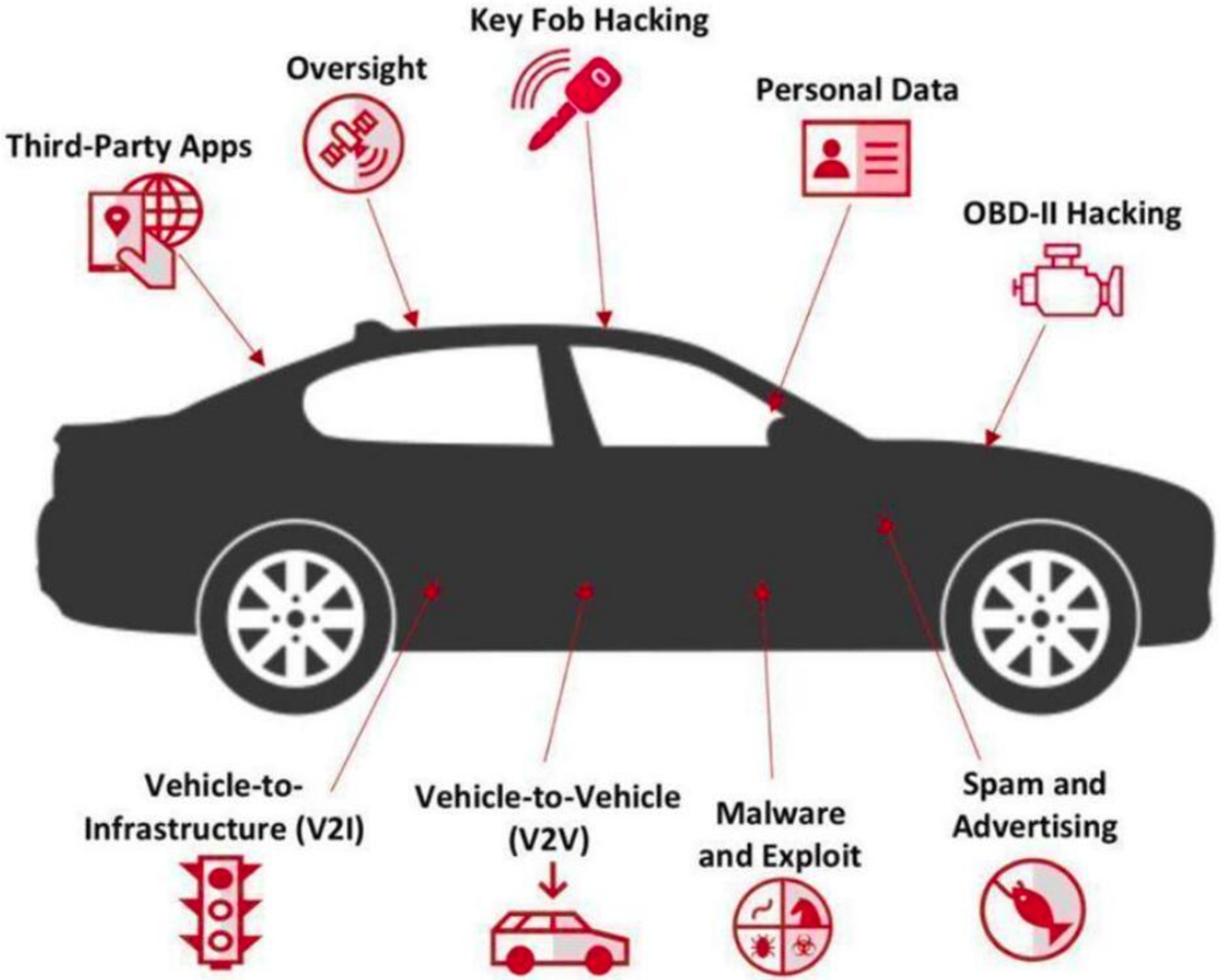
OWASP
Open Web Application Security Project

How Mirai botnet Works?



OWASP
Open Web Application Security Project

Continue..



OWASP
Open Web Application Security Project

IoT Attack Vectors

- Fake Control Server.
- Device Open Ports.
- Server Open Ports.
- Compromised Credential.
- Inject Bad Configuration or Firmware.
- Sniff Data on Private Network.
- Mobile Application
- Web Application
- Third-party Backend APIs
- Vendor Back-end APIs
- Device Firmware
- Authentication/Authorization

OWASP
Open Web Application Security Project

OWASP IoT Top 10

1 Weak, Guessable, or Hardcoded Passwords
Use of easily bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.

2 Insecure Network Services
Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control...

3 Insecure Ecosystem Interfaces
Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.

4 Lack of Secure Update Mechanism
Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.

5 Use of Insecure or Outdated Components
Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.

OWASP
Open Web Application Security Project

Continue..

6 Insufficient Privacy Protection
User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.

7 Insecure Data Transfer and Storage
Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.

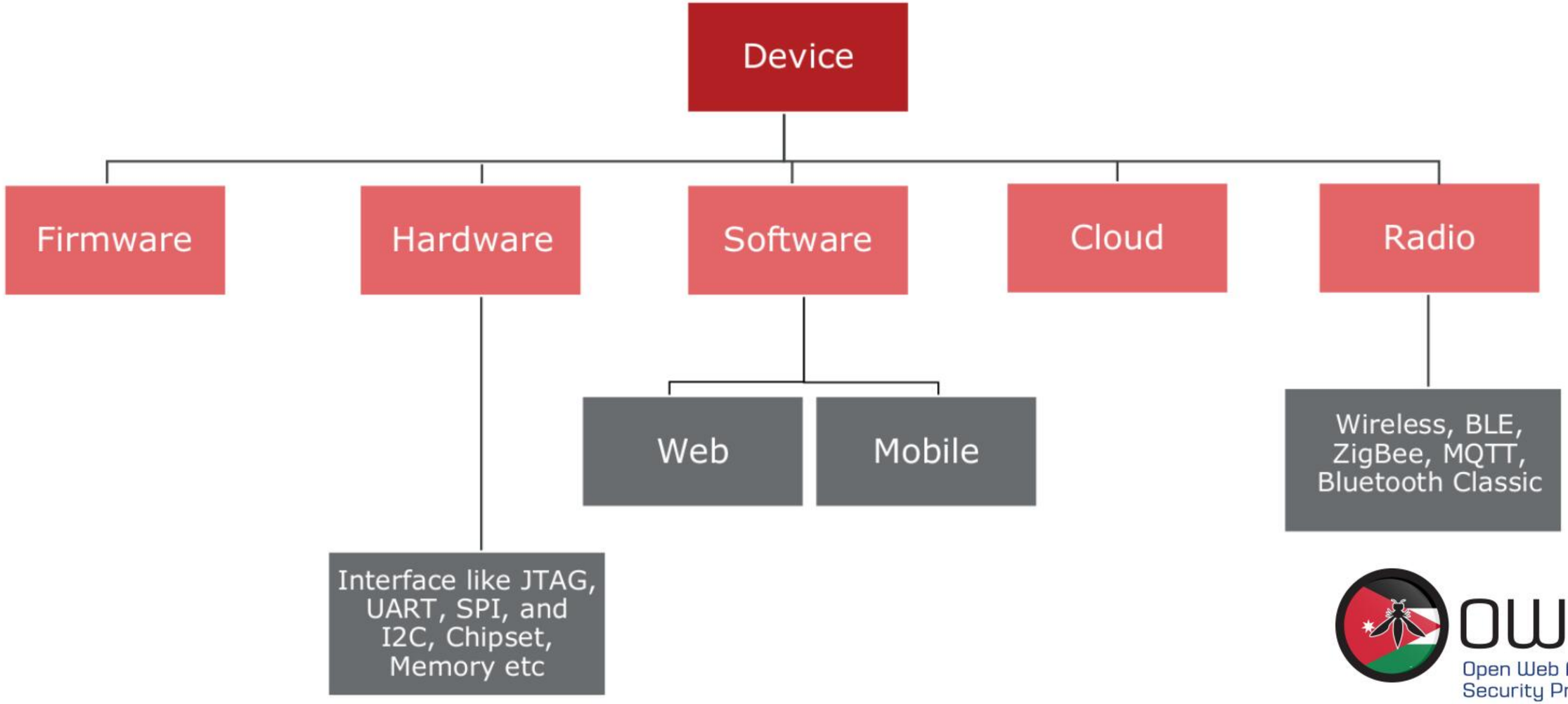
8 Lack of Device Management
Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.

9 Insecure Default Settings
Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.

10 Lack of Physical Hardening
Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.

OWASP
Open Web Application Security Project

IoT Security Testing Scope



OWASP
Open Web Application Security Project

IoT Firmware Vulnerabilities

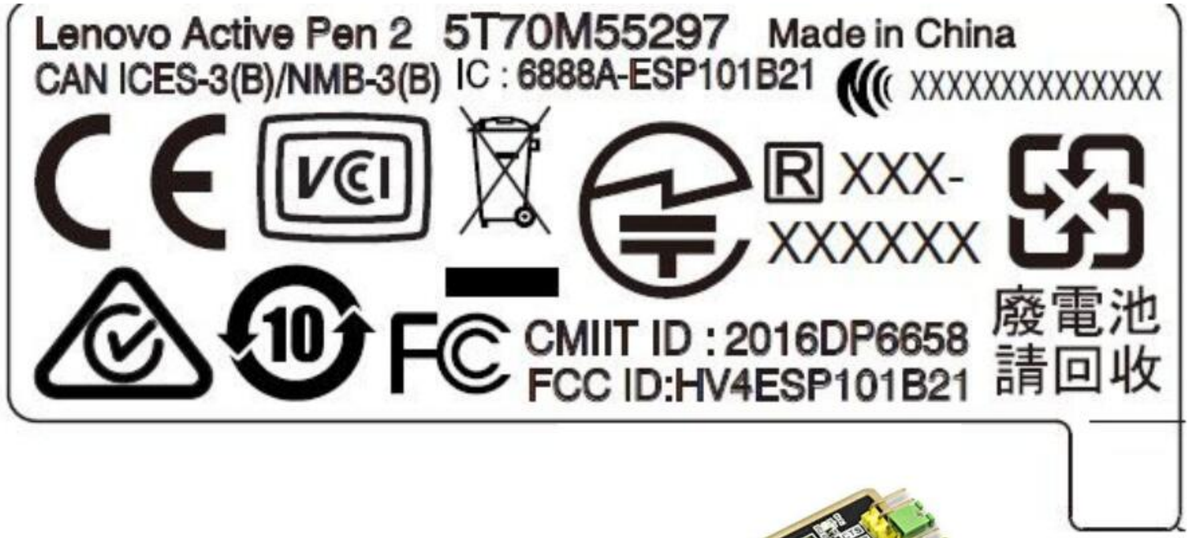
- What to do with firmware?
  - Reverse Engineering, Binary Analysis and Modification of the firmware

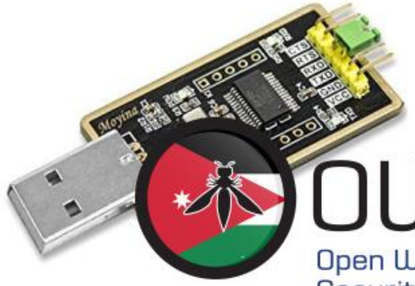
- Where to get the firmware?
  - Dumping from Device
  - Vendor’s Website
  - Support Groups & forums
  - RE Mobile Application
  - Download from vendor FTP server or search on ftp index sites
  - Capture the firmware during update, traces of DFU from wireshark

OWASP
Open Web Application Security Project

IoT Hardware Vulnerabilities

- FCC-ID database : Look up the FCC ID Identify Chips
  - CPU
  - Memory
  - Communication
- Physical ports:
  - Ethernet
  - USB
  - Serial
- Circuitry connection
  - UART - Usually 3-4 pins
  - JTAG - 6,12,13,20 pin header
  - SPI - indicates the presence of a flash chip





OWASP
Open Web Application Security Project

Continue..

- Analyze it via strings and hexdump.
- Use these tools:
  - https://github.com/craigz28/firmwalker
  - https://github.com/attify/firmware-analysis-toolkit

- Analyze configuration files and hardcoded sensitive values and certificates
- Insecure OTA update mechanism
- API keys, Encryption mechanisms, verification process, integrity checks, logins
- Watch out for Buffer overflows!
- Look for 3rd party libraries and SDKs
- look for keywords such as admin, password, remote, etc.

OWASP
Open Web Application Security Project

IoT Web App Vulnerabilities

- Look for the typical bugs like XSS, SQLi, XXE, XSRF, IDOR etc
- Use Burp Proxy to intercept, view and alter web traffic
- Check for permission level bugs user, root, admin

OWASP
Open Web Application Security Project

IoT Mobile App Vulnerabilities

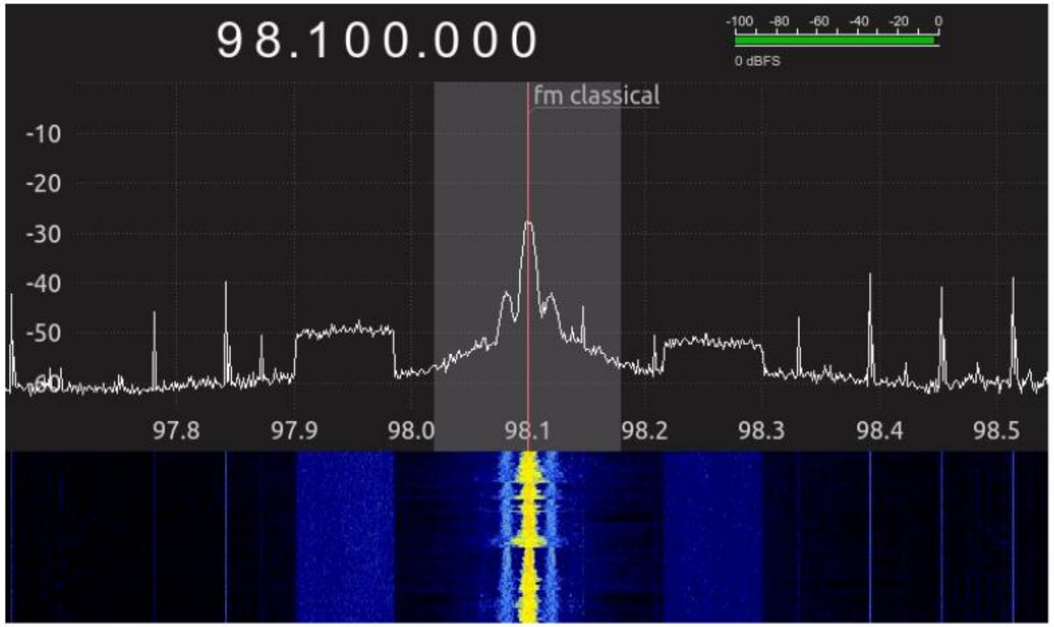
- Reverse engineer the mobile application, you may find entire logic on how device communicates with mobile app

- Common issues found in Mobile app
  - hardcoded firmware download URLs
  - Hardcoded SSIDs
  - Hardcoded encryption keys
  - Hardcoded username and password
  - API URLS, port and much more

OWASP
Open Web Application Security Project

IoT Radio Vulnerabilities

- Radio analysis requires special hardware and software
- Different protocol require different h/w and s/w
- Most commonly used are: BLE and ZigBee
- What could be done with RF signals?
  - Jamming based attacks
  - Modifying and replay attack
  - Sniffing the radio packets



OWASP
Open Web Application Security Project

Attacking Tools - Software

- Software Disassemblers
  - Ghidra
  - IDA
  - Binary Ninja
- Firmware Reverse Engineering
  - Binwalk
  - Any Extraction tools
- Fuzzing
  - QEMU
  - OpenOCD
  - Flashrom
- Minicom
- Protocol specific tools like can-utils
- Packet Inspection
  - Wireshark
- HTTP Proxy
  - Burp Suite - Yayy!!!
- Bluetooth
  - Bluehydra
  - Gattacker
  - BTLEJuice
- RF
  - Wireshark
  - GNU Radio
  - SDR
- Mobile reverse engineeri
  - Apktool
  - jadx

OWASP
Open Web Application Security Project

Attacking Tools - Hardware

- General Toolkits
  - Screwdriver ;)
  - Multimeter
  - Soldering iron
  - Connectors/Cable/Wires
- Interface Tools
  - **USB2UART**
  - Flash Dumper
- RF Tools
  - Bluetooth Sniffing
    - Ubertooth One
    - Bluefruit/Nordic Sniffer
    - Commercial Sniffers $$$
  - Software Defined Radio
    - RTL-SDR
    - HackRF
    - BladeRF
  - Zigbee
    - CC2531 Sniffer

OWASP
Open Web Application Security Project

Any Questions?