- Filename: eccouncil-ceh31250-v10-18-2-2-iot-attacks
- Show Name: CEHv10 (312-50)
- Topic Name: IoT Hacking
- Episode Name: IoT Hacking Pt.2
- Description: In this episode, Adam and Wes discuss the vulnerabilities and attacks that can lead to IoT systems being compromised.

==========

DEFINING THE INTERNET OF THINGS (IoT) - The Internet of Things (IoT) refers to a system of interrelated, internet-connected objects able to collect and transfer data over a wireless network without human intervention.

An Internet of Things 'thing' can refer to a connected medical device, a biochip transponder (think livestock), a solar panel, a connected automobile with sensors that alert the driver to a myriad of possible issues (fuel, tire pressure, needed maintenance, and more) or any object, outfitted with sensors, that has the ability to gather and transfer data over a network.

IoT device deployments provide the data and insights needed to streamline workflows, visualize usage patterns, automate processes, and meet compliance requirements.

How does the IoT actually work?

IoT devices can either communicate with the internet directly, or access via a IoT gateway.

Devices and objects with built in sensors are connected to an Internet of Things platform, which integrates data from the different devices and applies analytics to share the most valuable information with applications built to address specific needs.

```
IoT Gateway Architecture.vsdx
```

Some vocabulary that we should understand:

ANALYTICS OF THINGS (AoT) - the analysis of IoT data, which is the data being generated by IoT sensors and devices.

CONNECTIVITY - IoT connectivity boils down to how Things connect to each other. Connections can either be wired or wireless. Some of the more popular connections: 4G LTE, Bluetooth, GPS, LoRa, mesh networking, RFID, WiFi, Zigbee and Z-wave.

EDGE COMPUTING - In a traditional IoT architecture, the data that is collected or generated by a Thing is often sent to the cloud for storage and analysis. Both edge computing and fog computing focus on pushing intelligence and processing capabilities to the network edge, closer to where the data originates and away from the cloud.

The difference between the two is that with edge computing, Things are hardwired into a smart controller. The controller then decides how to handle the data coming from the Thing, i.e., store the data locally or push it to the cloud.

Fog computing, in contrast, works with the local area network (LAN). Data is gathered, processed and stored within the network via an IoT gateway or fog node.

GEOFENCING - uses GPS and RFID technologies to create a virtual geographic boundary, like around your home property. A response is then triggered any time a mobile device enters or leaves the area. (turn the lights off when you leave and on when you get back home)

GPS - another way our Things – like our smartphones, fitness bands and connected cars – keep track of where we are and where we are going.

GRID COMPUTING - reduces costs by maximizing existing resources. This is accomplished with multiple machines working together to solve a specific problem.

INDUSTRIAL IoT (IIoT) - the use of IoT technologies in manufacturing and is part of the Industry 4.0 trend. It incorporates machine learning, big data technologies, sensor data, M2M communication and automation technologies. The philosophy behind IIoT is that smart machines are better than humans at accurately, consistently capturing and communicating data.

INTERNET OF EVERYTHING (IoE) - A term originally coined by Cisco, IoE is the intelligent connection of people, data, process and things. In essence, IoE adds network intelligence to IoT.

LORA - a long range, low power wireless platform that is being used to build IoT networks worldwide, especially by smart cities and communities. It securely transmits data and is being integrated into many Things, including connected vehicles, street lights and home appliances.

SENSOR - A sensor is a device that can detect an event or change in the environment, and send that information to a machine that can then act (or not) on the data it has received. Sensors have become ubiquitous and contribute significantly to the Things population.

SMART - Any physical entity that can exchange data with another entity through a wired/wireless connection is said to be “smart.”

ZIGBEE - A wireless mesh networking protocol popular in home automation. It provides a way for all the smart Things in your smart home to communicate with one another.

Z-WAVE - Another wireless mesh networking protocol popular in home automation.

```
IoT Devices Are Everywhere.vsdx
```

What is the multi-layer architecture of IoT?

Made up of 5 layers:

1. Application - responsible for delivering the data to users and providing a user interface to allow for control of the IoT device
2. Middleware - device and information management
3. Internet - endpoint connectivity
4. Access Gateway - protocol translation and messaging
5. Edge Technology - IoT capable devices

What are some IoT Technology & Protocols that I may want to be aware of?

Short-Range Wireless:

```
a. Bluetooth Low-Energy (BLE)
b. Light-Fidelity (Li-Fi)
c. Near Field Communication (NFC)
d. QR Codes & Barcodes
e. Radio-Frequency Identification (RFID)
f. Wi-fi / Direct
g. Z-wave
h. Zigbee
```

Medium-Range Wireless:

```
a. Ha-Low
b. LTE-Advanced
```

Long-Range Wireless:

```
a. Low-power Wide-area Networking (LPWAN)
b. LoRaWAN
c. Sigfox
d. Very Smart Aperture Terminal (VSAT)
e. Cellular
```

Wired Communications:

```
a. Ethernet
b. Power-Line Communication (PLC)
c. Multimedia over Coax Alliance (MoCA)
```

IoT Operating Systems:

```
a. RIOT OS
b. ARM mbed OS
c. RealSense OS X
d. Nucleus RTOS
e. Brillo
f. Contiki
g. Zephyr
h. Ubuntu Core
i. Integrity RTOS
j. Apache Mynewt
```

What are common IoT Communication Models? -

1. Device to Device - direct communication between two devices
2. Device to Cloud - devices communicate directly with an application server based in the cloud
3. Device to Gateway - devices communicate to a centralized gateway that gathers data and then sends it to an application server based in the cloud
4. Back-End Data Sharing - used to scale the device to cloud model to allow for multiple devices to interact with one or more application servers

What are major challenges associate with the use of IoT?

1. Vulnerable interfaces
2. Physical security risks
3. Vendor support
4. Interoperability issues
5. Difficulty upgrading/updating firmware and patching
6. Lack of a focus on C I A related protections
7. Use of weak and hard coded credentials
8. Potential for buffer overflows due to poor programming and security protections

OWASP Top 10 IoT Vulnerabilities (2014 listing)

Rank Title
I1 Insecure Web Interface
I2 Insufficient Authentication/Authorization
I3 Insecure Network Services
I4 Lack of Transport Encryption/Integrity Verification
I5 Privacy Concerns
I6 Insecure Cloud Interface
I7 Insecure Mobile Interface
I8 Insufficient Security Configurability
I9 Insecure Software/Firmware
I10 Poor Physical Security

Insecure Web Interface - A web interface is defined as a control panel to interact between a user and software running on a web server. Most house hold devices we use today to communicate with the internet have some kind of web interface.

What to look out for:

1. Never allow use of default passwords; enforce a password change upon setup of the "Thing"
2. Prevent Brute Forcing; enforce an attempt limit and lock account down after x number of failed access attempts & make sure to introduce a reset procedure that requires direct (non web) interaction with the "Thing"

3. Make sure the web application code is not susceptible to vulnerabilities such as XSS, CSRF, SQLi and others
4. Store credentials securely and do not expose them over network traffic
5. Use modern encryption techniques and do not settle for less than the latest encryption levels

Insufficient Authentication/Authorization -

What to look out for:

1. Enforce strong passwords; they should include upper and lower case characters + numeric values and maybe even a symbol & they should definitely not be shorter than six characters
2. Create user profiles and limit their permissions based on their access credentials
3. Implement two factor Authentication
4. Write secure password recovery functions and processes
5. Force password expiration dates
6. Do not allow use of default passwords

Insecure Network Services - the fact that your fridge is now using the network does not mean that the network itself has to adapt. The network stays the same and the attack vectors stay the same, therefore its important to implement the same network security measures and solutions. You want to make sure that no one can actually make your "Things" un-responsive using Denial of Service attacks or attacks such as Buffer overflow and fuzzing.

What to look out for:

1. Good static analysis security testing solutions should be able to detect such attack potentials
2. Make sure that ports not in use are not open or accessible

Lack of Transport Encryption -

What to look out for:

1. Use the latest and greatest encryption techniques for communication between "Things" and the web.

Privacy Concerns - Identity theft is on the rise and the more devices are exposed to the net the more dangerous it becomes to store data.

What to look out for:

1. Do not store data that you do not need
2. Encrypt all stored data at rest and transport
3. Anonymize data where possible

Insecure Cloud Interface - New code means new vulnerabilities which need to be validated and closed. New interface means new passwords that need to be validates and enforced.

What to look out for:

1. Validate code vulnerabilities are addressed (XSS, SQLi, CSRF and others)
2. Enforce strong passwords; they should include upper and lower case characters + numeric values and maybe even a symbol & they should definitely not be shorter than six characters
3. Force password expiration dates

4. Use two factor authentication
5. Ensure cloud systems use transport encryption

Insecure Mobile Interface - Being both a "Thing" and a handheld computer holding probably most of your sensitive data, these devices are considered to be the crown jewel for hackers.

Take a look at connected cars. These systems mostly run mobile operating systems and allow access to car controls. While these systems are very useful to provide important tools like web access, automatic crash notifications, remote system updates and other services, they also pose quite a significant risk in case the wrong user has taken control of the remote device.

What to look out for:

1. Apps should enforce high level of password security including two factor authentication, password expiration, no use of default passwords, high password complexity and account lockout mechanisms
2. Use transport encryption for any communication to avoid eavesdropping and data theft
3. Do not collect any unnecessary data and store required data encrypted and in a secure manner

Insufficient Security Configurability - When configuring a device it is critical to allow the administrator to enforce strict security regulations. Imagine an industrial engineer setting up a turbine. The turbine has its own software which allows control of the turbine speed and scheduling. These settings can be controlled via a local interface to the turbine software. Would you want to engineer to be able to modify settings without consent of management or the relevant teams?

What to look out for:

1. Enforce Application code allows password security options (two factor authentication, password expiration, no use of default passwords, high password complexity and account lockout mechanisms)
2. Validate applications are written with data encryption options (Enabling AES-256 where AES-128 is the default setting)
3. Audit logs and usage logs should be mandated as part of the application functionality
4. Security event notifications should be available to trigger and alert end users on operations which might introduce risks

Insecure Software/Firmware - Once "things" are connected to the web they will almost always have some kind of software running in the background. This software like any other might be exposed to zero day vulnerabilities, malware and other attack techniques. Therefore you will want to make sure that the software is updated on a regular basis to make sure new threats are protected against.

What to look out for:

1. Application/Software should be written to allow update capability
2. Update files should be processed in an encrypted manner
3. Updates need to be validated before implemented using signed files

Poor Physical Security - Physical access to a device is probably the easiest way to infiltrate and create some kind of damage (depending on the device).

What to look out for:

1. Utilize a minimal number of device access ports (e.g. USB and network ports)
2. Sensitive application functions should not be accessible through USB

3. Consider writing application to allow local access only (no web access)

```
OWASP IoT Top 10 - 2018.docx
```

What are the common IoT attack areas?

1. Device memory containing credentials
2. Device / Ecosystem Access control
3. Device Physical Interfaces / Firmware extraction
4. Device web interface
5. Device Firmware
6. Device network services
7. Device administrative interface(s)
8. (Unencrypted) local data storage
9. Cloud interface(s)
10. Device update mechanism(s)
11. Insecure API's (vendor & third-party)
12. Mobile applications
13. Confidentiality and Integrity issues across the ecosystem
14. Network traffic

What are the common IoT threats I should be aware of?

1. DDoS Attacks
2. HVAC System attacks
3. Rolling Code attack - used to steal cars
4. BlueBorne attack
5. Jamming attack
6. Remote access via backdoors
7. Remote access via unsecured protocols such as Telnet
8. Sybil attack - happens when an insecure computer is hijacked to claim multiple identities. Problems arise when a reputation system (such as a file-sharing reputation on a torrent network) is tricked into thinking that an attacking computer has a disproportionally large influence.
9. Exploit Kits
10. Man-in-the-Middle attack
11. Replay attack
12. Forged Malicious Device
13. Side Channel attack
14. Ransomware attack

What is the IoT Hacking Methodology?

1. Information Gathering - Shodan, Censys, Thingful
2. Vulnerability Scanning - Multi-Ping, NMAP, RIoT, Foren6
3. Launch Attack - RFCrack, Attify Zigbee Framework, HackRF
4. Gain Access
5. Maintain Access

What are common countermeasures to be taken to help secure IoT devices?

1. Firmware updates
2. Block ALL unecessary ports
3. Disable insecure access protocols such as Telnet
4. Only use encrypted communication protocols
5. Use strong passwords
6. Encrypt ALL data and communications coming into, being stored in and leaving the device
7. Use account lockout

8. Configuration management and baselining of devices along with compliance monitoring
9. Use multi-factor authentication
10. Disable UPnP

A little Shodan and tell... How do I use Shodan to find things?

A list of default webcam usernames and passwords:

ACTi: admin/123456 or Admin/123456
Axis (traditional): root/pass,
Axis (new): requires password creation during first login
Cisco: No default password, requires creation during first login
Grandstream: admin/admin
IQinVision: root/system
Mobotix: admin/meinsm
Panasonic: admin/12345
Samsung Electronics: root/root or admin/4321
Samsung Techwin (old): admin/1111111
Samsung Techwin (new): admin/4321
Sony: admin/admin
TRENDnet: admin/admin
Toshiba: root/ikwd
Vivotek: root/<blank>
WebcamXP: admin/<blank>