ECE 531
Introduction to Internet of Things

Nitin Bhandari

Assignment 2

Harden your Code (Attack Surfaces)

1) Introduction

Here in this assignment, we aim to reduce the security vulnerabilities of our IoT deamon. An IoT client device is prone to attacks through its hardware, network, devices attached to it, applications, etc. For examples, if we are using a kernel version which is having security vulnerabilities is prone to attack even though you have maintained a very tight secure code and software for the security of your device. Therefore before deployment of the device, it is necessary to go through all the number of exploitable vulnerabilities in a system whether it is caused by system programs, or the open network ports or the hardware devices attached to it. Usually, the attack is caused due to the loophole on the system which might not be the developer's fault but if the system is not analyzed for the vulnerabilities it is a fault of the team.

2) Attack Surfaces

a. Physical cyber-attacks
These attacks result from breaches to the IoT device's sensors. With an IoT physical cyber-attack, the hacker most often accesses the system through close proximity, like inserting a USB drive.

b. Network cyber-attacks

These attackers infiltrate your network devices to see what's flowing. They can insert themselves between you and your devices (known as "Man in the Middle" or "MitM"), creating fake identities, stealing information, and redirecting packets to their desired location, away from your network (also referred to as a "sinkhole" attack).

c. Software attacks

Software attacks occur when malware is installed into your network's program. This malicious software sends a virus, corrupts or steals data, and can both interrupt and spy on the activities.

d. Encryption attacks

Hackers analyze and deduce your encryption keys, to figure out how you create those algorithms. Once the encryption keys are unlocked, cyber-assailants can install their own algorithms and take control of your system.

A possible attack surface of a lot(Cellphone) Device

3) Securing our daemon process

In order to secure our daemon process, we have to make some changes.

- Instead of returning the error codes and allowing the system to be used we are replacing them with exit functions to exit once the process has encountered an error.
- We can give access to the user and the trusted group the ability to read or write that particular application. These permissions can be set using chmod command. Permission is an area where attackers are most actively seeking the vulnerabilities.
- We are removing any kind of acceptance of input during the runtime.
- We already had “unmask” which is a type of file mode creation mask. The umask acts as a set of permissions that applications cannot set on files.

- **There are no external dependencies in the program other than loading of header files which does not contain any of the libraries like curl to make a connection to the client.**
- **Also it neither uses any environmental variables nor it uses any external files**

4) Steps were taken by the secure bootloader process to have a secure system

- Verify the integrity of software by passing through a secure boot process.
- The software which is getting loaded is verified using the private key given by the authority and the public key present in the hardware to verify the signature of the loaded software and thus verifying the bootloader
- The process itself can be repeated through a series of signature verifications.

5)Measures for an overall attack on an Application

- Check for the encryption of data comprising of keys, passwords, etc
- Always try to have proofread of the code and the software by others as is easy for others to have a check on the security faults made by you
- The sum up of all paths for data and commands into and out of the application.

6) References

- https://www.sciencedirect.com/topics/computer-science/attack-surface
- https://www.lastline.com/blog/iot-devices-earn-a-fail-for-security-the-rise-of-automated-attacks-and-large-scale-infections/
- https://www.channelpartnersonline.com/blog/iot-insecurity-6-common-attacks-and-how-to-protect-customers/
- https://www.l-tron.com/iot-security-risks-4-types-of-cyber-attacks/