Lab – Learning the Details of Attacks

Objectives

Research and analyze IoT application vulnerabilities

Background / Scenario

The Internet of Things (IoT) consists of digitally connected devices that are connecting every aspect of our lives, including our homes, offices, cars, and even our bodies to the Internet. With the accelerating adoption of IPv6 and the near universal deployment of Wi-Fi networks, the IoT is growing at an exponential pace. Industry experts estimate that by 2020, the number of active IoT devices will approach 50 billion. IoT devices are particularly vulnerable to security threats because security has not always been considered in IoT product design. Also, IoT devices are often sold with old and unpatched embedded operating systems and software.

Required Resources

- PC or mobile device with Internet access

Conduct a Search of IoT Application Vulnerabilities

Using your favorite search engine, conduct a search for Internet of Things (IoT) vulnerabilities. During your search, find an example of an IoT vulnerability for each of the IoT verticals: industry, energy systems, healthcare, and government. Be prepared to discuss who might exploit the vulnerability and why, what caused the vulnerability, and what could be done to limit the vulnerability? Some suggested resources to get started on your search are listed below:

Cisco IoT Resources

IoT Security Foundation

Business Insider IoT security threats

Note: You can use the web browser in the virtual machine installed in a previous lab to research security issues. By using the virtual machine, you may prevent malware from being installed on your computer.

From your research, choose an IoT vulnerability and answer the following questions:\

a. What is the vulnerability?

Vulnerability is a weakness in system software, hardware, IoT devices or networks which may cause to exploited by attackers to gather unauthorized data access where hackers steal data causes the damage to network or devices. It can relate to a person's weakness to cause damage such as a physical vulnerability.

There are some vulnerabilities which are related to IoT security include:

- IoT devices are physically accessible to everyone if device got stolen. It is easy for the attacker to steal the sensitive data from the device.
- IoT device does not encrypt the data when it connected to network that can be collect and read by anyone.
- The default passwords used by many IoT devices are simple to guess, making them vulnerable to illegal access.
- Many IoT devices are not made to auto download updates, they are exposed to newly found threats.

b. Who might exploit it? Explain.

It may exploit in many ways in IoT devices. In IoT security there are different types of attackers who might exploit vulnerabilities. There are attackers who creates unauthorized software to access our device's. When we install such packages to our devices then it was accessible by many attackers. In such a way attacker gains our privacy information and confidential files. Attackers tries in unusual way to gain our personal data. In order to prevent such exploits should not click on unknown links where in spam mails, unknown messages.

c. Why does the vulnerability exist?

IoT devices commonly have complicated in both hardware and software models that could be complex to secure. IoT devices has a specific of memory, battery life. Where amount of IoT devices is limited, it is difficult to implement security system in IoT devices. Many of the IoT devices have simple protocols and there are no communication protocols which has no encryption of data exists in devices. This can make attacker easier to intercept and manipulate data from the device. Where the attackers exploit, and vulnerability exists.

d. What could be done to limit the vulnerability?

- Try to avoid saving of passwords.
- When we increase the size of memory in IoT device we can make it secured by adding few new protocols such as communication protocol.
- By adding encryption algorithms in memory.
- Avoid surfing of fake sites and avoid clicking on unknown links.
- Try to update the device up to date.