CIS 4367.01 **Brandon Thompson**
Prof. Elibol Due Date: 4/25/2020

Homework 17

The internet of things is an architecture of devices that communicate between each other and other services. This results in the generation of enormous amounts of data which has to be stored, processed and presented in a seamless, efficient, and easily interpreted form. [3] A simple IoT architecture is composed of sensors that collect data and send it to a database, the database retrieves and compiles necessary information and the user interface and displays this information to the user in as close to real time as possible.

In 2016 Ronen et al [4] classified attacks on IoT architectures into four groups, ignoring functionality, reducing functionality, misusing functionality and extending functionality. The main focus of the paper was to show an extended functionality attack on smart lights to leak data from secure locations or cause epileptic people to have seizures. This assumes that there is already an infected computer and the attacker is using the lights to retrieve the compromised data. This attack is a major breach in integrity and availability because the attacker can turn the light on or off, removing the availability of the light(s) or it could have a larger impact on the system by providing an channel for compromised data to escape from the would be extremely difficult to trace.

Williams et al [5] conducted a large scale Nessus vulnerability scan on 156,680 consumer IoT devices and found that 12% of these devices contained a vulnerability of 'critical', 'high', 'medium' or 'low' risk. The devices scanned were webcams, smart TV's and printers that were considered part of an IoT infrastructure. This means that 12% of consumer IoT devices could be susceptible to attacks. Considering the number of devices is expected to grow by 21 percent annually, rising to 18 billion between 2016 and 2022 [2] this percentage is not acceptable and could cause major security issues or data breaches in the future if companies do not improve the security of their IoT devices.

In general, IoT is still fairly new as a technology, and its benefits are still being developed, but as people are developing new methods to utilize the IoT, they are not considering the confidentiality, integrity, or availability flaws of their system. Cisco released a video on their Youtube channel [1] about the anatomy of an IoT attack and how attackers could use an unsecure device to gain access to more critical systems.

References

[1] Cisco. Anatomy of an iot attack.

[2] Ericson. Ericson mobility report: Read the latest report.

[3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 2013.

[4] E. Ronen and A. Shamir. Extended functionality attacks on iot devices: The case of smart lights. *2016 IEEE European Symposium on Security and Privacy (EuroSP)*, 2016.

[5] R. Williams, E. McMahon, S. Samtani, M. Patton, and H. Chen. Identifying vulnerabilities of consumer internet of things (iot) devices: A scalable approach. *2017 IEEE Interantional Conference on Intelligence and Security Informatics (ISI)*, 2017.