**Worksheet 8**

**Security in the Internet of Things**

**CPSC 3555 - Spring 2018**

Section 1: Read Chapter 10 of the textbook and answer the following questions:

1. Explain the three broad categories of threats to the Internet of Things.
   1. *Capture* threats are related to capturing the system or information.
   2. *Disrupt* threats are related to denying, destroying, and disrupting the system.
   3. *Manipulate* threats are related to manipulating the data, identity, time-series data
2. What are the 4 security requirements for IoT?
   1. Confidentiality: transmitted data con be read only by the communication endpoints
   2. Availability: the communication endpoints can always be reached and cannot be made inaccessible
   3. Integrity: received data are not tampered with during transmission
   4. Authenticity: data sender can always be verified, and data receivers cannot be spoofed and authorization
3. What are some well known routing attacks in IoT? Explain at least 2.
   1. With *selective-forwarding* attacks, it is possible to launch a DoS attacks where malicious nodes selectively forward packets.
   2. In *sinkhole* attacks, a malicious node advertises a fraudulent routing path with a seemingly favorable route metric and attracts many nearbynodes to route traffic through it.
   3. In a *hello-flood* attack, the HELLO message refers to the initial message a node sends when joining a network. By broadcasting a HELLO message, an attacker can introduce himself as a neighbor to many nodes, possibly the entire network.
   4. A *warmhole* attack is an out-of-band connection between two nodes using wired or wireless links. Wormholes can be used to forward packets fasten than via normal paths.
   5. In a *clone-ID* attack, an attacker copies the identities of a valid node onto another physical node.
4. What were some of the challenges in IoT security you recognized while reading the chapter? Authentication, confidentiality and availability are the three main challenges in computer security to this date.

Section 2: Read the following article <https://blog.malwarebytes.com/101/2017/12/internet-things-iot-security-never/> and answer the questions:

1. What are some of the hacks that have occurred in the Internet of Things?

Two years ago, a smart refrigerator was hacked and began sending pornographic spam while making ice cubes. Baby monitors have been used to eavesdrop on and even speak to sleeping children. In 2016, thousands of security cameras were hacked to create the largest-ever distributed denial of service attack against Dyn.

1. What reasons did the author give as to why defenses are so weak in IoT?

Poor security built into devices, devices in which are directly exposed to the web because of poor network segmentation. Adding on to poor security, developers sometimes leave behind code or features developed in beta that are no longer relevant and default credentials are too often hard coded.

1. What are the solution the author suggested?

Solutions suggested by the author include: government intervention to work with cybersecurity and intelligence communities to gather a series of protocols that would make IoT devices safer for consumers and businesses. Developers can also have a red team audit the devices prior to commercial release to avoid hacks.

1. What are your opinions on the solutions?

Although these solutions may sound simple and ordinary, I believe these are steps sometimes skipped over in the productions of IoT products and ay result in the leading hacks of some big historic hacks. If we can initialize efforts to create more secure products instead of focusing on the capitalism aspect of these inventions, we can certainly avoid problems in the future rather than have to recover from them.

Section 3: Take a few minutes to research IoT security flaws. Do you notice a trend in flaws, attacks, or solutions? Does the state of IoT security surprise you? Is it weaker or stronger than you thought? Cite in sources you use.

It seems like cyber attackers in the modern world of smart appliances target for these small smart “add-ons” in people’s homes. With ransomware being one of the trendiest attacks it leaves consumers defenseless when being blocked out of their house because a hacker is asking for money for them to enter their home. It seems like companies are starting to catch on to these hacking methods and are aware of the steps they must take to avoid these, but unfortunately were not capable of avoiding it to start with. The state of security surprises me that we do not hear from attacks like these more frequent for which it seems like it is simple to access some smart devices, so maybe IoT security is more advanced than I ever anticipated.

<https://www.forbes.com/sites/ciocentral/2017/05/08/security-surprises-arising-from-the-internet-of-things-iot/#17b99abf2495>

<https://www.networkworld.com/article/3164839/security/rsa-2017-the-internet-of-things-security-threat.html>