Cybersecurity

& Internet of Things

"By 2016 Gartner predicts 6.4 billion devices will be connected to the internet" (Barker, 2015)

Arko Dewri (704301345)

Arvin Nguyen (304300135)

Frank Chen (204256656)

Matthew Lin (904281426)

Shitij Gupta (104310164)

TA: Roger Blum

ENGR 183EW Winter 2017 – DIS 1D

Monday, March 20, 2017

Table of Contents

1 Executive Summary

Nowadays, the Internet has become the ultimate medium for connecting people all over the world. Technical innovations have pushed the boundaries of what devices could be connected: transportation, assistance, healthcare, and home devices. Despite the rapid rise of these Internet of Things (IoT) devices, cybersecurity remains an ever present threat to today's consumers. The paradox in our never-ending cycle of technological advancement is that as our infrastructure gets more advanced, there will be an increased opportunity for hackers to take advantage of.

We analyze the issue of cybersecurity and IoT through four areas of interest: smart transportation, smart assistance, healthcare devices, and smart home automation. Furthermore, we motivate our issue with a case study on the massive distributed denial of service (DDoS) attack that happened in October 2016 via exploited IoT devices.

Smart Transportation. The field of smart transportation presents a huge vulnerability that attackers will try to exploit because humans rely on transportation to get anywhere. Every transportation device or system is at risk once they connect to the Internet; therefore, people must be educated about the risks involved when purchasing smart vehicles or using public transportation systems that are connected to IoT. The three major technical issues within the realm of transportation deal with hacking software, preventing accidents, and disrupting traffic systems. Hacking software can either incapacitate or seize a person's smart vehicle. Accidents can occur as a result of flawed software used by smart vehicles. Traffic systems in public places such as airports can be disrupted by smart attackers. There are also major ethical concerns including allocating the right proportion of IoT connected devices, adding a failure option once a hacker breaks in, and deciding whether to open source or close source the smart transportation device's source code. The general population is greatly affected by all of these issues and must be cognizant of computer security. Using common sense and erring on the side of caution when in doubt are good tips to add to one's ethical framework to stay safe from malicious attackers.

Smart Assistance. As technology is expanding to make lives easy and efficient, consumers need to be aware of the capability and incapability of the products they are using. In terms of smart assistance devices, it is highly important for customers to be acquainted with the shortcomings of the devices so that they could better protect themselves from threats. While manufacturers have been making an effort to enhance the hardware, algorithm, and security of these devices, hackers are constantly evolving to bring new threats in the society. Consumers could best protect themselves by establishing custom password, updating the firmware

from time-to-time, and checking up on their devices for any unusual activity. In regards to privacy threats, both the manufacturers and the customers should work together to ensure that the information collected by these devices are kept secured, and thus privacy rights are protected. However, during critical situations, such as incidents that require law enforcement to obtain the data recorded, it would be ideal for both parties to inquire the depth of the situation before revealing any information; perhaps the data could be utilized to help find a murderer but not to assist in a divorce case. If properly employed, these smart assistance devices could become one of the most significant technological assets in the society.

Healthcare Devices. There are a huge array of applications for IoT devices in the healthcare industry. Many of our medical applications and devices are already linked wirelessly to a central server or another IoT device such as the smartphone. We will be analyzing two types of healthcare devices: wearables and implanted devices. However, there are key cybersecurity issues within healthcare devices such as privacy and integrity of data. Our personal health data is important for hospitals to diagnose and treat us properly, so maliciously modifying or taking away that data can be detrimental to the safety and well-being of our society. Some of the ethical issues that we analyze include whether the loss of autonomy for patients using IoT healthcare devices is justified, and how much transparency is needed from manufacturers of healthcare IoT devices on the functioning of their product. We approached these issues with potential solutions that called for minimizing loss of information during a security breach, as well as enforcing transparency so that patients can make an informed decision on whether to allow a device to capture their data.

Smart Home. The IoT is on track to change people's daily lives with its growing prevalence in the home. Household appliances communicating with one another and connected to the internet has the ability to automate common tasks increasing energy efficiency and improving time management. However, there is a downside to these supercharged thermostats, refrigerators, security cameras, and electronic door locks. Sensors are ubiquitous in an IoT connected home and they are constantly monitoring and collecting data. This leads to serious security concerns about the possibility for hackers to take control and the damages that would result. The large amounts of data generated also spur ethical discussion about the privacy rights of the consumers. Society needs to consider what information companies are allowed to collect about their customers and what can that information be used for. We approach these problems with solutions by arguing for government regulation enforcing higher standards through and transparency from IoT companies.

[Case Study] DDoS Attack using IoT Devices. On October 21, 2016, the DNS provider Dyn was shut down for the majority of the day, causing many web services such as Spotify, Reddit, and Twitter to be unavailable to users. This DDoS attack was made possible by hackers exploiting the vulnerabilities in IoT devices to be used to simultaneously send thousands of requests to the Dyn servers. This incident was a major

wake up call for the manufacturers of IoT devices, as they realized that many of their commercialized products are not secured and are susceptible to exploits. For the Dyn DDoS attack, hackers used an open-source software called MIRAI to scan for vulnerable IoT devices around the world and use them to their advantage. Some of the ethical issues we explored in this case study include whether it is ethically sound for companies to sell vulnerable IoT devices, and the trade-offs between companies and consumers to create a safe future with IoT devices. Some of the solutions we propose to tackle this issue is to enforce strict security testing of IoT devices before they are commercialized, as well as implementing mandatory reset of default password in avoid vulnerability from factory-set username and password that could be easily cracked.

2 Introduction

	Frank	Matthew	Arko	Shitij	Arvin
Front Matter	P		R		
Introduction	D, I	D, I, P	D, I	D, I	D, I
Topic 1 - Smart Transportation	R	P			
Topic 2 - Smart Assistance		R	P		
Topic 3 - Healthcare Devices				P	R
Topic 4 - Home Automation			R		P
Topic 5 - DDOS attack using IoT Devices [case study]	P			R	
Ethical Discussion*	P, R	P, R	P, R	P, R	P, R
Recommendations*	P, R	P, R	P, R	P, R	P, R
Conclusion	D, I	D, I, P	D, I	D, I	D, I
Reference Cited	P, R	P, R	P, R	P, R	P, R
Final Proofreading	P, R	P, R	P, R	P, R	P, R
P = Primary					
R = Review for content, form, and grammar					
D = Discuss					
I = Input					
*we're each writing our own recommendations and ethical discussions					

Figure 1: Our group's RAM chart showing individual contributions from each team member.

As shown in Figure 1, we used the RAM chart created in class to organize our workload for the paper. We decided to divide our paper into three sections: Technological Issues, Ethical/Societal Issues, and Recommendation, with each section containing the 5 different sub-topics that we were respectively responsible for: Smart Transportation, Smart Assistance, Healthcare Devices, Smart Home, and the case study on the DDoS attack.

We each worked on the technological issue, ethical/societal analysis, and recommendation for the sub-topic that we were assigned to. Our sub-topics were divides as the following:

Smart Transportation - Matthew Lin

Smart Assistance - Arko Dewri

Healthcare Devices - Shitij Gupta

Home Automation - Arvin Nguyen

[Case Study] DDoS Attack using IoT Devices - Frank Chen

3 Problem Statement & Background

3.1 Problem Statements

3.1.1 Smart Transportation.

Smart transportation is a rapidly evolving field that has seen major advancements in the last decade. While the progress of these smart vehicles has been quite promising, a lot of ethical issues will inevitably arise such as hacking vehicle software, preventing accidents from occurring, and disrupting traffic control systems in major areas of transportation. Because smart transportation has the potential to become a massive part of our everyday lives, it is important to remain educated on the dangers that smart transportation can present and learn how to protect ourselves and our smart vehicles. The current solutions for the three ethical issues are outsmarting the hackers with stronger authentication, choosing situations that will cause the least harm out of all possible scenarios, and maintaining backups of all traffic control systems in the event of an attack.

3.2.2 Smart Assistance.

Smart assistance devices have demonstrated their significance in people's lives by saving valuable time and bringing ease in daily activities; as a result, they quickly gained popularity in the society. Although their development have been quite remarkable, these devices reveal issues in the areas of connectivity, security, and voice analysis. These areas contain vulnerabilities that could be easily exploited by hackers; if left unresolved, the vulnerabilities could potentially lead to bigger problems for consumers. In order to solve these issues, manufacturers could introduce stricter security methods, enhance the listening algorithm, and adopt better hardware for these devices. In addition, ethical concerns emerged due to the information recorded by these devices. Revealing the data would violate consumer privacy, however, in criminal investigate these data could be utilized to help solve a case. Hence, the debate unfolded: should data be completely concealed or could data be disclosed during critical situations?

3.2.3 Healthcare Devices

An important area of application of Internet of Things is the medical sphere. Today we have devices, both on top and inside our bodies that help us stay more connected with our personal well-being. Smart medical

devices such pulse monitors, fitness tracker bands and brain sensors help provide constant round-the-clock monitoring of vital levels and wirelessly connect to the internet for storing and managing the collected medical information. However, these devices are plagued by security and privacy risks. Moreover, the use of such devices raises ethical questions related to reliability, transparency, harmful analytics and sustainability. These issues can be resolved through proper legal regulations, use of centralized control devices and in-depth testing before release to market. Moreover, a culture of strong ethics needs to harbor among the professionals developing these smart medical devices.

3.2.4 Smart Home.

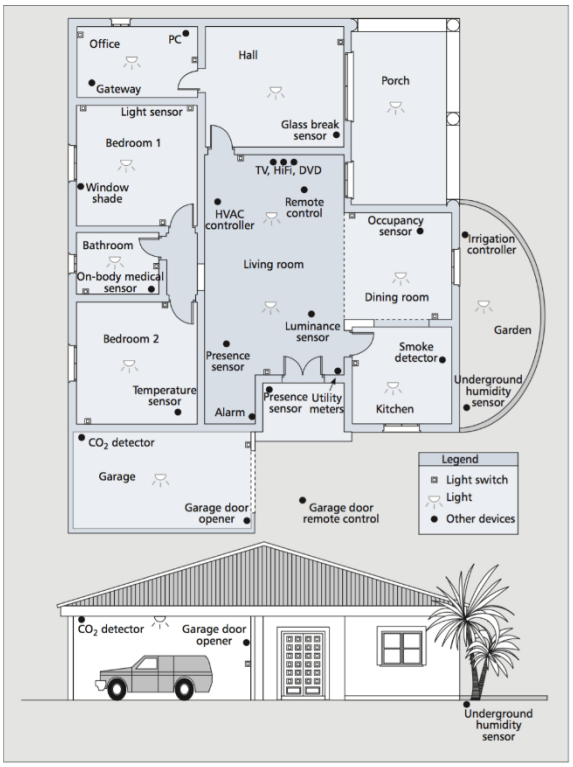

Figure 2: An example wireless home automation network (Gomez, 2010)

The Internet of Things has promising potential in the realm of home automation - the networked connection of home appliances and sensors to form a cohesive system. Home automation has the potential to disrupt how people live their daily lives by offering extreme convenience. With a mobile smart phone a tenant can operate the lights in a different room, feed the fish while he is on vacation, or turn on the air conditioning on a hot summer day before he returns home from work. Sensory devices can detect if the pantry is getting empty, the refrigerator contains spoiling food, or an intruder is present. Energy conservation is another possible benefit. Houses can collect data about the activity patterns of the occupants with smart thermostats that regulates the temperature at an optimal schedule, lights can automatically turn off in unoccupied rooms, and faucets can send alerts when they detect leaks. As shown in Figure 2, there is opportunity for nearly every aspect of a modern house. Home automation can also empower the elderly and disabled by delivering "electronically coordinated assistance", such as by prompting patients with dementia reminders of their current task and environment (Davis 2003).

3.2.5 [Case Study]: DDoS Attack using IoT Devices.

IoT is an increasingly popular phenomenon describing everyday devices having the capability of communicating with each other through Internet. While IoT devices promise exciting potential for big data, home automation, and various other revolutionary technological advances, there will be ethical issues that arise due to the vulnerability of these systems. As a result of an increasing number of unprotected IoT devices,

Distributed Denial of Service (DDoS) attacks are becoming more common. DDoS attacks takes advantage of IoT devices to send massive requests to servers and DNS providers. IoT devices will soon become a part of every one of our lives, so it is crucial that we take an early step to protect these devices and prevent DDoS and various other cyber-attacks from happening.

3.2 Background

3.2.1 Smart Transportation.

Cybersecurity is a critical concern for transportation mobility and safety (Transportation Systems Security, 2008). Smart transportation encompasses numerous vehicles including airplanes, trains, and cars; many of these vehicles are equipped with electronic features that make them vulnerable to cyber security threats. Technologies such as radio frequency, Wi-Fi connection, and cellular networks enable features such as vehicle controls, real-time travel planning, and automated dispatching that are such a large part of our lives that cyber-attacks can cripple our way of life.

Technical issues are multiform with regards to smart transportation and include threats from the user end (incorrect settings and virus infection) as well as from that of the attacker, such as unauthorized usage and settings, information leakage, sniffing, Distributed Denial of Service (DDoS) attacks, and tampering with message logs (Hong, 2016). The direct effects that these technical issues will have on vehicles include limited vehicle external connectivity and computational performance as well as hampered real time operation capabilities. This situation is so frightening that even "isolated" legacy systems are risky; a 14 year old boy exploited a weakness in Polish trams in January 2008, which led to 4 light rail trains getting derailed and 12 people injured (Transportation Systems Security, 2008). He modified a TV remote control so he could change the track points, and he obtained information needed to build the device by studying the tram depots and the tracks (The Register). Although this boy did not have any malicious intent, his actions created an unsettling precedent because he was able to transform a simple household device into a weapon that could possibly have killed people. No smart transportation system is safe as long as it can be connected to the Internet, and this is where we must learn from past cyber-attacks to avoid these dangerous scenarios in the near future.

3.2.2 Smart Assistance.

Smart assistance devices have become well-known among Americans with the rise of "Internet of Things". They not only reduce the time needed to accomplish a certain task, but also attempt to understand an individual's needs through constant listening. They have the potential enhance communication and operation in different aspects of everyday lives. Currently the smart assistance devices that are in the market are Google Home and Amazon Echo; the artificial intelligence in Amazon Echo is referred to as Alexa.

Figure 3: Google Home (left) and Amazon Echo (right), two competitors in Smart Assistance (Torres, 2016).

They are able to help accomplish daily tasks, such as calling an Uber or ordering Starbucks, in seconds, which might otherwise cost more time and effort for an individual. However, these smart assistance devices also introduce technical and ethical issues, including problems with safety, security, and protection of privacy. As a result, people are unsure about the limits of these devices and hesitant about their trust on these devices. If there is sudden connection loss, these devices could contribute to hazardous situations. While these devices are constantly listening to the people to better understand their needs, hackers could be eavesdropping or performing "denial of service attacks". In fact, there comes the ethical concern whether the data obtained by these devices should never be revealed or used in specific instances, such as criminal cases. Some of the solutions for the technical issues include introduction of better hardware, adoption of better algorithm, and restriction of open-sourcing software. The solution for the ethical dilemma is highly dependent on individual situations, and need to be analyzed on case by case basis. Perhaps, the best solution is to educate the public about the advantages and shortcomings of these devices so they can better protect themselves.

3.2.3 Healthcare Devices.

In the modern world, applications of Internet-of-Things (IoT) in the healthcare industry are widespread. Today, we have a vast variety of medical applications and devices that are linked wirelessly to a central data server or other IoT enabled devices like smartphones. According to Business Insider's premium research service, Business Intelligence, the installed base of healthcare IoT devices is estimated to grow from about 95 million in 2015 to 646 million in 2016 (as shown in Figure 4) (Meola, 2016). And this number doesn't even include the most popular category of healthcare IoT devices i.e. wearable devices like fitness trackers.

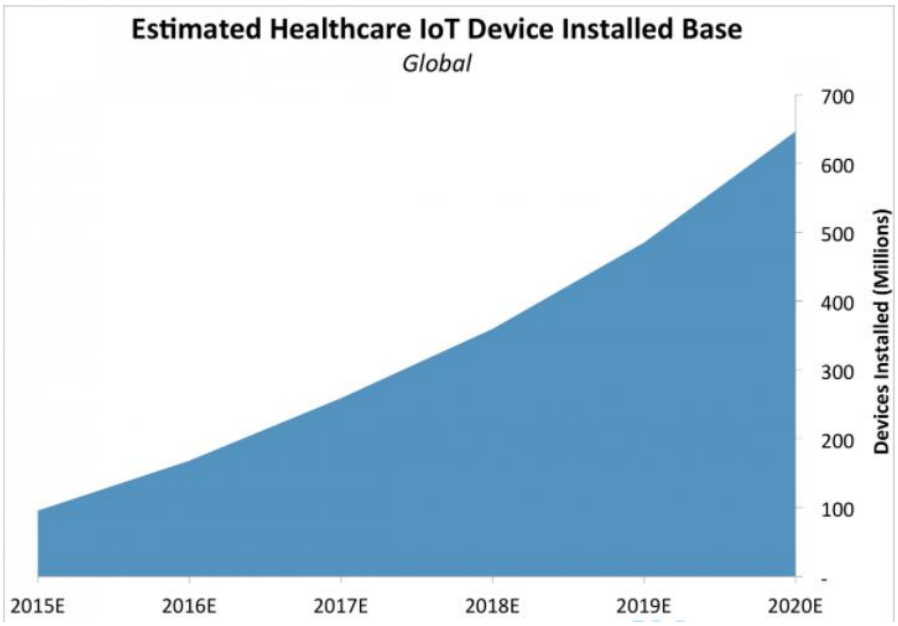

Figure 4: Estimated healthcare IoT devices installed base (Meola, 2016)

Broadly, we can classify smart medical devices into two primary categories: wearables, worn or used on the surface of the human body, and implanted, those that are inserted inside human body (Ameen, 2012). Wearable healthcare devices include blood pressure monitors, heart rate monitors, glucose sensors, fitness bands while cardiac arrhythmia recorders, brain liquid pressure sensors, and endoscope capsules are examples of implanted devices (Ameen, 2012). These devices, besides providing remote monitoring features, play a significant role in designing personalized fitness programs, providing improved connectivity, and scheduling limited-available resources for better access across patients and ultimately decreasing costs and increasing the quality of life (Islam, 2015). Moreover, disease management and drugs management is improved through the constant monitoring and errors are reduced significantly. However, as is the scenario for most IoT applications, smart healthcare devices too are plagued by cybersecurity issues.

3.2.4 Smart Home.

Figure 5: Nest, the home automated thermostat (Nest, 2011)

Home automation has been trending with the explosion with mobile cell phone. The professional services firm PricewaterhouseCoopers estimates that the "connected home market could be worth nearly $150 billion globally" by 2020 (Hsu 2016). Corporate titans are recognizing the growing space in home automation and are investing appropriately. In 2014 Google acquired Nest (shown in Figure 5), a smart thermostat producer, for 3.2 billion dollars and Dropcam, a home-security camera producer, for 550 million dollars (The Economist 2016). Samsung is selling internet-connected refrigerators and pushing SmartThings as their smart home brand. Apple created HomeKit as a software framework for developers to connect iPhones with house appliances.

3.2.5 [Case Study] DDoS Attack using IoT Devices.

On October 21, 2016, Twitter, SoundCloud, Spotify, Reddit, and other websites have been inaccessible to many users in the East Coast and Southern parts of the United States throughout the day. After investigations, the DNS provider Dyn stated that the outages are the result of several distributed denial of service (DDoS) from IoT devices that attacked Dyn (Gallagher, 2016).

A DDoS attack is a method of attacking a server or network by sending more requests to it than it can respond to (Vowell, 2016). All DDoS attacks have a common goal of disrupting network activity and denying users access to resources. As shown in Figure 6, a malicious attacker can perform a DDoS attack by utilizing a botnet, which is a collection of compromised devices (zombies or 'bots') that they can force to participate in the attack. The DDoS attack model contains a botmaster, which oversees and instructs the devices in the botnet, sending instruction on when and how to implement the attack. Their victim target is usually a DNS service

provider like Dyn, whose primary purpose is to provide the mapping between the hostname users type into their browsers and the IP address of the actual resource. Without DNS providers such as Dyn, the Internet would cease to exist. How a DNS provider (or any server, for that matter) works is by taking incoming requests from users and process them. For example, a user who wants to access google.com will be routed to google.com by Dyn. However, when there are simultaneously millions of requests coming in to the server, it becomes increasingly more difficult for that server to process all the requests in a timely manner without crashing. Once a server crashes, they can no longer provide the mapping functionality that is needed to give users the websites they want to visit, therefore "shutting down the Internet".

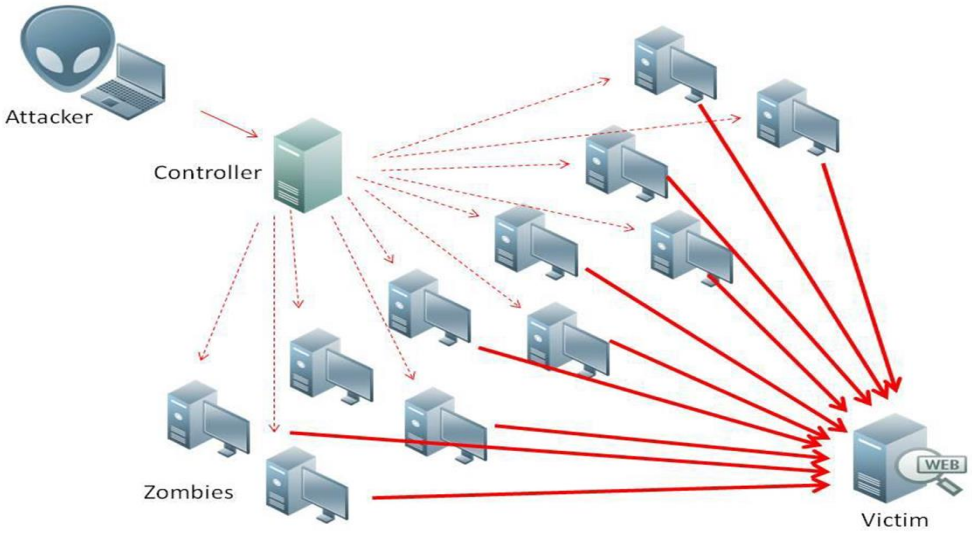

Figure 6: How a DDoS attack sequence work (Bisson, 2016)

4 Technological Issues

4.1 Smart Transportation

A major technical issue regarding cybersecurity and IoT is with regards to hacking vehicle software. In July 2015, hackers seized control of a Jeep via a laptop and mobile phone from 10 miles away and crashed it into a ditch (Curtis, 2015). There are two particularly scary factors to this attack. The first is that the attackers used two common devices that nearly everyone owns rather than sophisticated technological equipment, indicating that the potential for increased amounts of hacking is extremely high. The second concern is that more than 470,000 cars made by Fiat Chrysler have vulnerabilities to similar attacks, and this suggests that everyone who owns a car is at risk from a cyber-attack. These vulnerabilities are not just limited to our personal vehicles; a hacker named Chris Roberts exposed serious weaknesses while flying on United Airlines by hacking the in-flight entertainment system and overwriting the code on the plane's Thrust Management Computer to cause the plane engines to climb in a lateral motion (Foster, 2015). Because passengers do not control these methods of transportation, they are especially at the mercy of hackers if they take over the electronic systems of smart vehicles.

Figure 7: Tesla's Model S, a fully electric car with IoT components (Tesla, 2013)

Tesla's Model S earned a recent claim to infamy when its self-driving "Autopilot" system led to the death of the driver Joshua Brown. His Model S's "Autopilot" system failed to distinguish the white side of a turning tractor-trailer from the bright sky and failed to activate the brakes (The Associated Press, 2016). The implications about this incident are significant because it shows that even the most cutting-edge pieces of

technology are not immune to failure (nothing is immune to failure), and this could have huge ethical ramifications for the companies developing these technologies. A lot of problems currently stem from the trend that technology tends to be released to the market prematurely before all the safety patches have been implemented. Since accidents are always a major risk to consider, a more serious design consideration is deciding who to sacrifice in the case of an unavoidable accident. The classic example of killing 10 innocent people versus killing 1 innocent person (yourself). This dilemma ties in well with the Utilitarianism ethical framework, which states we should strive to maximize one's welfare without harming others. Additionally, it has a very important effect on the company's design decisions because people will not want to purchase a vehicle that sacrifices its owner, but paradoxically, people will be in favor of cars that sacrifice the occupant to save others as long as they are not driving that car (ArXiv, 2015). This dilemma will continue to drive the decision making process of elite autonomous vehicle manufacturers as they strive to keep refining their algorithms to make morally correct decisions in the future.

Vehicles themselves are not the only victims of cyber-attacks. Traffic control systems also have massive vulnerabilities that have been exposed in the recent past. On June 22, 2015, hackers breached Warsaw's Chopin airport's computer systems and prevented the airline LOT Polish Airways from creating flight plans (CNN). The cause of this problem was the flight plan-delivery protocol used by these airlines; this protocol does not require authentication, so hackers were able to send bogus flight plans to the flight crew that seem valid (Zetter, 2015). This caused 20 flight cancellations and several delays that impacted air travel in Poland. The scariest thing about this incident was that all airlines currently follow this protocol, so malicious hackers can send fake plans and completely disrupt air travel (Zetter, 2015). This attack could be a catalyst for future attacks because of the potential havoc that attackers could wreak upon airlines in order to extort potential demands such as money. For passengers and flight crew, this type of hack could hinder air travel by delaying flights as well as diminishing the trust that fliers have in air travel. Other forms of transportation such as sea travel also have similar weaknesses and attacks on these traffic control systems can result in huge economic losses for these industries with regards to trade as well as consumer recreation.

4.2 Smart Assistance

Setup problems are common among the customers of Google Home. A customer explained that he could not get Google Home connected to his 5-GHz network, even when he positioned Google Home within five feet of his dual-band router. In fact, multiple attempts and rebooting had to be done before the product connected to the 2.4-GHz network. Google Home also lacked consistency in connection when he connected with it to his speaker set. During the process, the customer explained that he changed the router settings and disabled VPNs; however, Google Home kept disconnecting at random times (Martin, 2016). This sort of situation could potentially reduce customer trust on Google Home. If a customer schedules Google Home to perform a specific task at a specific time, there is no guarantee that the device would not disconnect without prior notice before accomplishing the task. Similar disconnection problem were found among Amazon Echo speakers as well. These products sometimes struggle to stay connected to wireless networks. After some investigation, it was determined that household devices, such as microwave and radio antennae, cause interference issue on the 2.4GHz network. While 5GHz signal works much better for Amazon Echo, connectivity is obstructed if the device is a little too far from the router (Lagace, 2017). Despite, hardware compatibility is still an issue among these smart assistant devices. Furthermore, these devices are programmed to look for nearby network services on their own and connect to a router automatically; however, after a disconnection, the devices fail to work properly until the owner manually reboots appliances. So, during a hypothetical scenario where an Amazon Echo or a Google Home is used to schedule turning off an oven, it would become a potential fire hazard if the product erratically disconnects before finishing its scheduled task. Thus, technical problems among these smart assistance devices could produce some serious safety threats.

Security had been a major concern among smart assistance devices, as well. In an infographic analysis from Cisco it was revealed that today "more products are connected to the Internet than people". It has been predicted that 50 billion devices would be connected through the internet by 2020. With evolving internet, the attack surfaces for hackers are exponentially expanding (Barajas, 2014). A well-known path for hackers to perform attacks is the open source web interfaces. Currently Google and Amazon had made some of the software functionalities open source so other people could contribute to the codebase. This could be a potential threat because it allows hackers to access the software structures of the devices. In addition, customers could be victims of phishing attacks if Google Home or Amazon Echo is navigated to insecure network services or web interfaces during any search process; hackers accessing the open source could modify code that opens the door to such possibility. Furthermore, these smart assistance devices require manual update of firmware to ensure continued security; new updates are introduced from time to time to keep up with evolving threats. However, if a user fails to update the device at proper time, the device could experience attacks such as denial-of service or improper access to private information; unfortunately these devices cannot update themselves without the customer's involvement. One such scenario persisted when phrases from TV commercials

confused an outdated Google Home device, causing it to go "haywire", as explained by a customer named Scott Foster (Woodyard, 2017). If hackers exploit such a situation, they could potentially cause the Google Home device to freeze and deny the user of any service. Moreover, Amazon Echo operates by relying on a large amount of data. In order to acquire the data, Amazon Echo constantly listens, even when not prompted with a question, in order to prepare itself for the intelligence that the consumer desires. As a result, these devices track sensitive information about an individual's fitness, finances, and other critical parts of everyday life. But during the constant listening period a hacker could potentially eavesdrop upon the device, violating user privacy and obtaining sensitive information. (Baca, 2017). Currently, there is no strict approach that exists, which ensures that hackers or harmful individuals will not be able to access data from any of these smart assistance devices. Therefore, lack of security is certain a concern as the issue is putting user privacy at risk.

4.3 Healthcare Devices

Data communication and monitoring is done using wireless sensors in smart healthcare devices. This means that they are affected by the same security and privacy concerns that undermine wireless networks. Owing to the extensive use of wireless sensors for collection and sharing of data regarding the human body, a whole new class of networks called wireless body area networks (WBANs) has emerged (shown in Figure 8). The WBAN interacts with the cloud servers that are used to store health data, or with the Internet IP network which relays data to the health experts' workstations or user smartphones (Islam, 2015). It is also possible that the recorded medical data could be stored on the device itself in its memory. Thus attacks on the device or on the communication channel between the device and other connected devices or servers could lead to serious loss of sensitive information. A number of different attacks are employed by malicious individuals or organizations, which can compromise the security and privacy of a user of such health devices and applications.

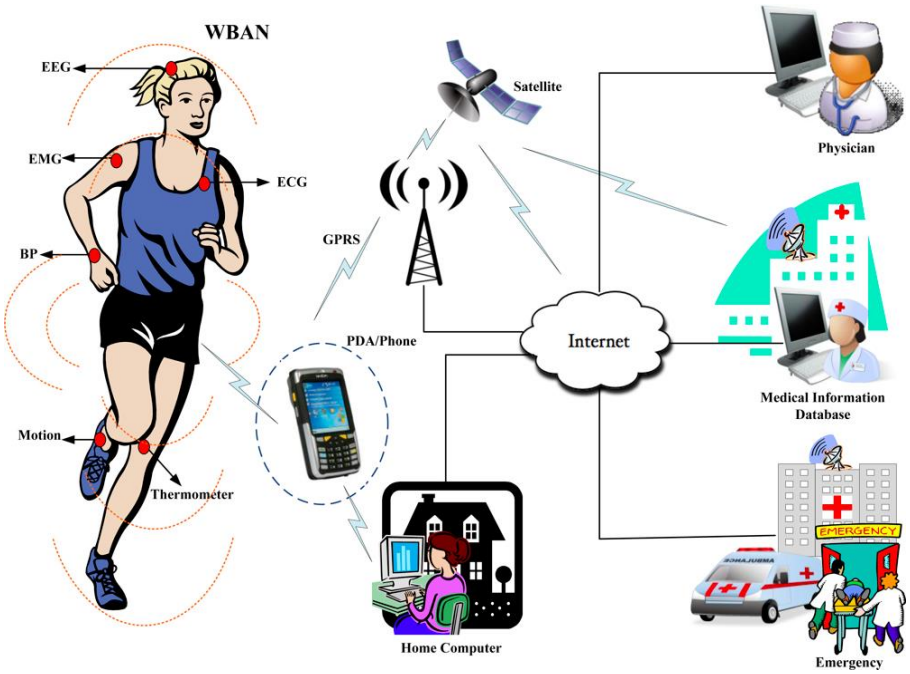

Figure 8: WBAN architecture for medical applications (Saleem, Ullah and Kwak, 2011)

Security. A major concern with the use of IoT devices, specifically healthcare devices, is the increased vulnerability to security lapses. It is hard to ensure necessary security requirements like confidentiality (content encryption and protection), integrity (non-alteration of data in transit and storage), availability (access to information at all times) and authentication (access for only authorized user) when communication takes place across wireless sensors and over large geographical distances (Islam, 2015). It becomes even harder when attackers come up with new modes and types of attacks every day. These attacks on health data and devices can be broadly classified under the following (Islam, 2015):

- **Attacks on disruption of information.** In-transit or stored health data can be susceptible to interruption attacks like Denial-of-Service attacks wherein the authorized user can't access his/her's or the patient's medical information. Similarly, attacks can be carried out to read or modify relevant medical information being transferred wirelessly. Even worse, false medical data could be injected by such attacks.
- **Attacks on Host properties.** Attacks can also be based on host properties. User devices can be compromised when attackers steal users' passcodes. Similarly hardware of health devices can come under attack and can be reprogrammed with malicious code (a big safety issue as well).
- **Attacks based on network properties**. Due to the use of multi layer networking protocol stack for communication across sensors, attackers can base attacks off the vulnerabilities between different layers. The networking protocol stack for health sensors and servers comprises of layers such as Application, Transport (for packet transmission), Network (IP address handling), MAC (router level layer) and security can be compromised if any of the layers are not secured (Islam, 2015).

Privacy. Another major area of concern that accompanies the use of IoT healthcare devices is the loss of privacy under attack. Privacy issues regarding the guarding of health data have come under attack in recent years. Where the medical records and data collected by sensors should be stored (remote health data servers or personal servers) and who should have the authority to look and examine medical data of an individual (access for sensor manufacturers or not) are some of the questions that have been raised and still remain unanswered (Ameen, 2012). Eavesdropping is another major technical issue that compromises the privacy of the user of healthcare IoT device. Attackers can monitor the information exchange across connected healthcare devices or can even introduce their own device into the network of connected devices and steal private medical data. Things get even worse when the information being shared is unencrypted. Another challenge accompanying healthcare IoT devices in particular is that they need to account for the mobility of the person using the device. As people move outside their relatively safe home wireless network to public wireless networks with lower security mechanisms, privacy of the individuals must be protected.

These attacks on healthcare IoT services have already been witnessed and are costing a lot of money to the U.S. healthcare system. According to a Bloomberg report in 2015, $6 billion a year was the loss from cyberattacks on hospitals and doctors (Pettypiece, 2015). Even wearable devices like Fitbit, a fitness tracker for personal health analysis, aren't safe from these attacks. In 2015, few researchers demonstrated that a Fitbit device could be hacked through a laptop in the vicinity of the device by exploiting the bluetooth connection. They were able to upload a small piece of non harmful code into the device hardware and had showcased concern that this vulnerability could be exploited to distribute malware (malicious program) across network or spy on someone by monitoring their location, thus compromising privacy (Weise, 2015).

4.4 Smart Home

One of the technological issues that is preventing home automation's adoption is the cost. PricewaterhouseCoopers reports that "72% of people have no plans to adopt smart-home technology in the next two to five years and that they are unwilling to pay for it" (The Economist 2016). Currently the added conveniences are just not significant enough for the common household to see internet connected house objects as anything but a luxury. Large appliances such as refrigerators have a long lifecycle and replaced slowly. Augmented lights and thermostats have a high initial cost and take years before they pay for themselves with their energy saving properties. Installation is another monetary barrier.

Home automation's main appeal is added convenience, but the technology is currently inflexible. Different manufacturers are all producing their products that communicate with their own network protocols. It is often difficult for different appliances to communicate and operate with each other in an easy manner: phone-controlled devices all need their own independent application. The best solution for a well-integrated home system is to use one company's platform. However this would lock the homeowner into one vendor that is incompatible with others and depends on the vendor's success. Homeowners are further reluctant to incorporate novel technology into their homes because they fear that it will make their estate to be more difficult to sell (Brush 2011).

The primary criticism against Internet of Things and home automation is the security concerns. Because household Internet of Thing devices is still full of immature technology, it is a prime target for hackers to exploit. The rapid iteration in products leave many vulnerabilities that criminals discover. Kamin Whitehouse, a smart building researcher and an associate professor at the University of Virginia states, "Once the house starts becoming fully connected, there's no reason to think that it won't become a target." (Metz, 2013). For example, in 2014, a hacker gained control over a networked camera setup and used the baby monitors "to scream obscenities into a baby nursery" (Wood 2015). The shared network between devices makes hackers especially dangerous as they can affect items throughout the house after gaining control of just one device. Finding a weakness in a single home appliance means the attacker can harm thousands of other people too.

With the many sensors in an automated home, a strong concern is for another person to secretly monitor a household. Malicious agents could remotely control video cameras and watch a family without them knowing, or access microphones and listen to conversations. Besides invading privacy, the invader could steal confidential information such as passwords, credit card numbers, and data that could lead to identity theft. Kamin Whitehouse explains that network traffic patterns can be used in conjunction with a "few assumptions about human behavior to get an idea of what's going on inside the house" (Metz, 2013). With this knowledge a burglary can be planned for when the house is unoccupied.

Ironically, even home security systems connected to the Internet meant to protect the tenants may actually introduce more vulnerabilities and make the house even more insecure than it would have otherwise

been. In a field study, researchers at HP Fortify examined 10 new home Internet of Things security system and all of them had failures. The researchers were able to gain access to the video cameras (Storm, 2015).

David Bryan and Daniel Crowley, security researchers at Trustwave Holdings demonstrated that hackers can inflect monetary damage. Crowley and Bryan exposed how easily one, Satis, Android smartphone app controlled music-playing toilet, could be set to flush repeatedly to waste water and play music continuously to waste electricity. Heating bills are another source that hackers manipulate (Metz, 2013). Attackers can also use online methods to impose physical harm. Electronically locking doors might be unlocked remotely allowing for an intruder to break in.

4.5 [Case Study] DDoS Attack using IoT Devices

What was especially insidious about this particular DDoS attack was that there were several waves that happened throughout the day. Service was temporarily restored after the initial attack around 9:30 AM, but a second attack began around noon, taking multiple websites down again. The third wave began around 4:30 PM before Dyn resolved the issue two hours later.

DNS providers such as Dyn operate as a link between the URLs typed in the browser and the corresponding IP addresses. DDoS attacks are frequently used to censor specific websites by overwhelming them with junk traffic and knocking them offline. However, by attacking Dyn, it's possible to overwhelm that directory function and cause outages and loading problems across a large swath of the internet (Etherington, 2016). The hackers behind the Dyn DDoS attack utilized massive botnet, assembled via open source code called MIRAI that took control of tens of thousands of IoT devices, such as routers, web cameras, and printers (Ducklin, 2016). The MIRAI botnet codebase is relevant in our discussion because it takes advantage of vulnerable IoT devices, and uses these devices as "bots" to initiate DDOS attacks. These devices sent enough requests to overwhelm Dyn's network resources, resulting in a huge DDoS attack. Since most of Dyn's service runs in the East Coast and the South, those were the major areas that were affected, as shown in Figure 9.

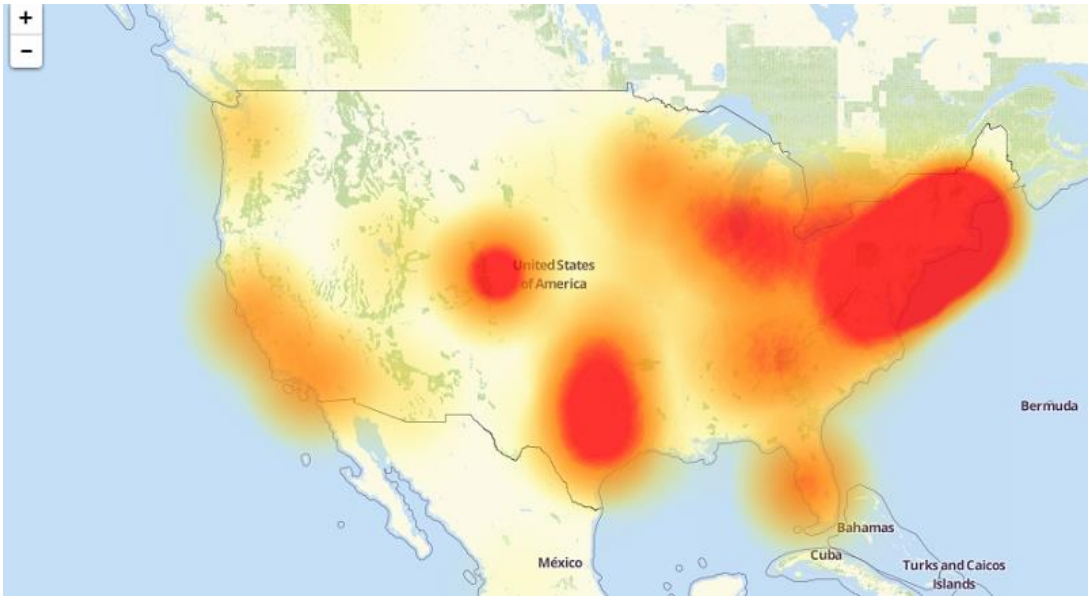

Figure 9: Area in red and orange indicate affected areas by the MIRAI DDoS attack (Krebs, 2016).

Botnet refers to a set of malware-infected devices built to perform tasks over the command of botmasters. A basic attack is composed of a single or multiple botmasters, botnets, the command and control (C&C) architecture and its communication protocol. MIRAI has three main components:

- A call-home system that is downloaded to a central IoT compromised device and acts as a server, downloading information on potential victims. MIRAI uses default, factory-set usernames and password as a dictionary to perform brute-force password cracking to compromise IoT devices.

- A set of attack routines that generates random legitimate-looking network traffics to overflow the victim's network capacity. The attacks append random strings of text to the front of domain names, transforming them into new requests that can be repeatedly sent in to attack the network.
- A network scanner that searches randomly across the internet, building a list of insecure IoT devices for the next wave of attacks. This allows MIRAI to continue the attacks wave after wave.

root	xc3511
root	vizxv
root	admin
admin	admin
root	888888
root	xmhdipc
root	default
root	juantech
root	123456
root	54321
support	support

Figure 10: a sample list of default usernames and passwords that MIRAI uses in its dictionary attack (Herzberg, 2016).

Another characteristic that makes MIRAI DDoS attacks unique is their ability to send GRE (Generic Routing Encapsulation) floods. GRE is a tunneling protocol that can encapsulate a wide variety of network layer protocols over an IP network. This is a very powerful method of DDoS attack because most public routers will let GRE requests go through, since GRE requests are widely used for generating VPN connections. According to Incapsula's technical report, hackers used a hit-and-run tactic with the MIRAI virus and initiated a GRE flood on the website; the attack peaked at 280 Gbps and 130 Mpps, which indicates that the MIRAI virus is very powerful botnet. The graph of the attack is shown in Figure 11.

Figure 11: Incapsula mitigating a slew of MIRAI-powered GRE floods (Herzberg, 2016)

Furthermore, MIRAI is extremely robust; both the attack bot and the control server can be built to run on regular computers as well as many commonly-used hardware devices due to MIRAI's cross-platform support. As can be seen from Figure 12, these compromised devices can be found all over the world.

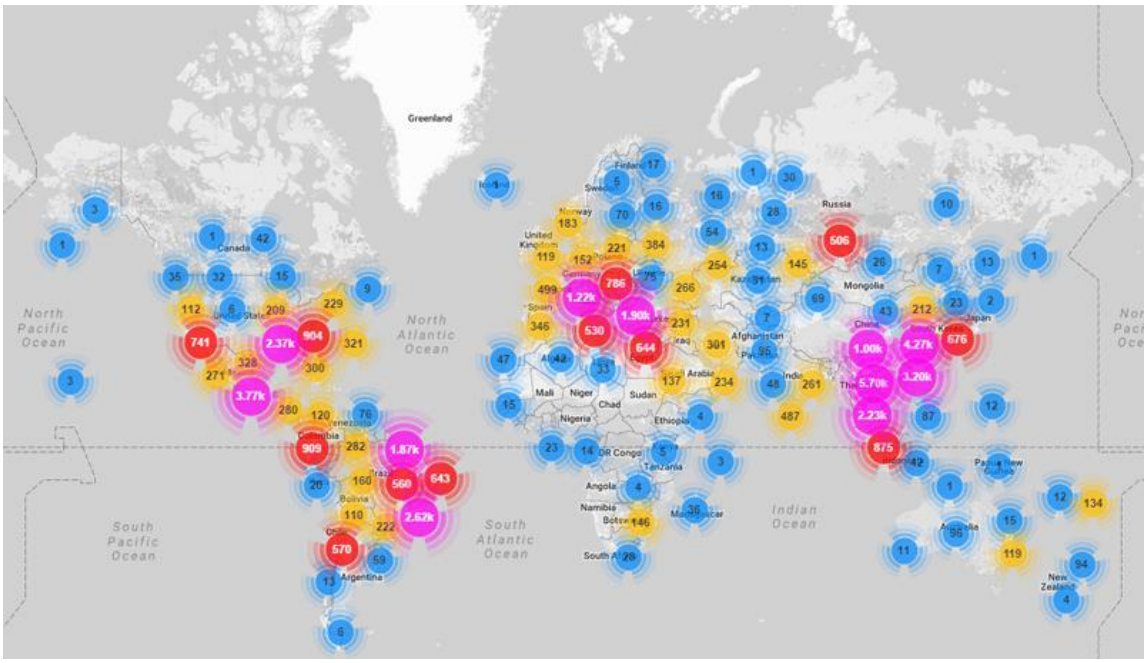

Figure 12: geo-locations of all MIRAI-infected devices uncovered so far across the world (Herzberg, 2016).

5 Ethical/Societal Analysis

5.1 Smart Transportation

In addition to the serious technical issues that smart transportation faces in the areas of cybersecurity and Internet of Things, there are a plethora of ethical considerations to keep in mind. While both technical and ethical problems can be improved upon and resolved by the engineers, ethical issues differ from technical issues in that engineers have more control over their ethical design decisions and "good" ethics can be taught. The five major ethical questions arising from smart transportation are as follows:

1. Who should be sacrificed in the case of an unavoidable accident?
2. Who should take the blame whenever a system gets compromised?
3. What percentage of autonomous transportation infrastructure should use IoT software given the risks of cyber-attacks?
4. In the case of an attack, should there be a failure option that causes the vehicle/system to stop working to prevent further damage?
5. Should IoT source code be distributed openly or removed from the public domain?

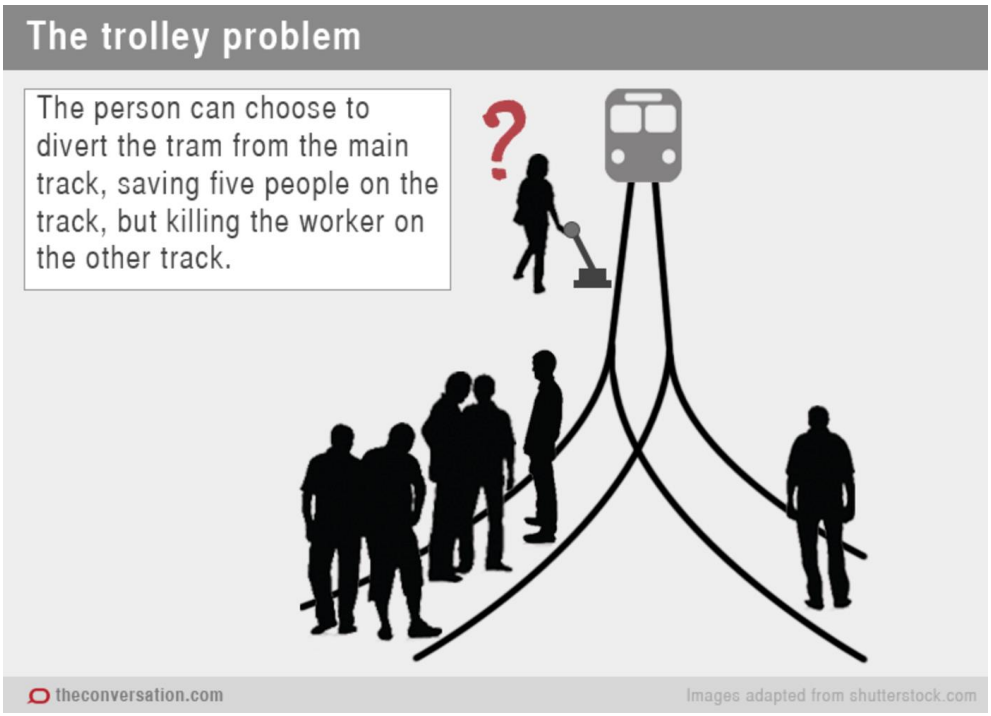

Figure 13: The infamous trolley problem visualized (D'Olimpio, 2017)

As mentioned earlier, it is always a difficult ethical decision on who to sacrifice whenever death is inevitable. The dilemma of killing others on the road versus killing yourself if it minimizes the death toll is incredibly difficult for automobile manufacturers because there are many different scenarios for the artificial intelligence system to consider when deciding who to sacrifice. This ethical issue is similar to the ethical question raised by the trolley problem (visualized in Figure 13). Since the system must consider heuristics such as the other vehicle's size and design, the speed at which the vehicle is moving relative to other cars, and the size and age of the passengers, it is very difficult to decide what is ethically "correct" since there are so many cases to code for (ArXiv, 2015).

System programmers and designers play a huge role in ensuring that an autonomous vehicle or traffic system is safe by trying to write safe code that cannot be compromised. Unfortunately, this lofty goal is impossible since there is always going to be some weaknesses that malicious attackers can exploit. Thus, we have a major ethical problem that arises whenever a system gets compromised. Should we blame the system programmer/designer for writing code with poor security standards?

As our society grows more and more technologically advanced, an important design decision to keep in mind is the proportion of smart transportation infrastructure that use IoT software. Although it is true that having a car that knows when to speed up, slow down, and stop completely can potentially change lives for the better, it is also true that increased usage of IoT software increases the risk of cyber-attacks. Criminals realize that they can take advantage of multiple IoT components in cars and lack of attention to detail in regards to security from automakers in order to obtain valuable information from victims (Kiss, 2016).

The previous question dealt with preventing cyber security breaches; another major ethical decision would be how to perform error handling as soon as the system has been compromised. One possible remedy would be to have a failure option that causes the vehicle/system to stop working to prevent future damage. It seems like the simple solution would be to always have a failure option to handle errors gracefully, but the problem with this is that crashing the system can cause data loss or corruption (IBM Knowledge Center).

The final ethical question has parallels with computer security debates in traditional software engineering. The debate over open source vs closed source platforms has been widely debated for decades with advocates on both sides. Proponents of open source platforms claim that they experience fewer exploits and patches are received more quickly (Veracode, 2015). Meanwhile, fans of closed source platforms will claim that their code bases are secure since no one hacker will know how the system runs, so the software is less likely to be exploited (Veracode, 2015).

5.2 Smart Assistance

Americans have become accustomed to the idea that "computers are always listening". But the data or record stored during the listening procedure had been generating legal concerns during recent years. The recorded information could be useful when investigating crime or analyzing a divorce proceeding, but it could be an infringement on an individual's right to privacy. Privacy experts have been debating whether it would be ethical to perform such kind of voice tracking. According to the director the Center of Law and Information Policy, Joel Reidenberg, at Fordham Law School in New York, no privacy exists when people install such listening devices that transmit data to third parties. He further argued that under the Fourth Amendment and based on the Electronics Communications Privacy Act, people are waiving their privacy rights when they knowingly set up these devices. On the contrary, the executive director of Electronic Privacy Information Center in Washington, Marc Rotenberg, argues that people who are not the direct owners of such devices did not agree to waive in their rights. Yet, they might find themselves in a room where the devices are listening to their voices and recording information; this is a violation to privacy rights (Weise, 2016). A real life example of such a problem was displayed during a murder case in Arkansas, as it raised legal concerns regarding data recorded by an Amazon Echo device. The prosecutors demanded that Amazon turn in the recording taken by the device found at the home where the murder occurred, believing that the information could provide clues regarding the murder. However, both Amazon and some privacy rights activists argued against such practice based on the constitutional limits granted to the public. Hence, data regulation could be one of the biggest battles that technology industries will face due to smart assistance devices. In reality, it is difficult to find the ethical balance on what information should be revealed and what information should be concealed (Baca, 2017).

Immanuel Kant's first categorical imperative of universality principle instructs people to "act only on that maxim which you can at the same time will that it should become a universal law" (Poel, 2011). The maxim that technology industries should follow is to protect consumer privacy at all times. Based on this maxim, manufacturers cannot reveal the information acquired by the smart assistance devices. Currently, both Amazon and Google have taken the preventive measure to secure the data by audio zipping them and encrypting the information as they are stored in the device. So, even if the network is compromised in any way, the devices would help in protecting the privacy of the owners. But if someone gets hold of the password for these devices, they could potentially see the log of any online interaction (Moynihan, 2016). Often people disregard setting their own custom passwords to these devices and just keep the factory default passwords, which certainly puts them at risk. Many hackers look for factory default passwords and utilize them to perform attacks on the devices. Hence privacy is a serious concern in regards to the smart assistance devices. Amazon had been highly determined to ensure that customer's privacy rights are protected, as they refused to provide the recorded information during the procedure of the Arkansas murder case. However, some law enforcement individuals were more interested in finding the culprit and bringing them to justice. Amazon was working under the maxim

of "protecting the privacy rights of all customers" and this maxim could be applied universally because right to privacy is a universal right of all individuals. Hence, Amazon was completely adhering to Kant's universality principle.

Jeremy Bentham's ethical framework of utilitarianism takes a different approach to the privacy issue. His principle attempts to focus on "the greatest happiness for the greatest number" (Poel, 2011). While Amazon was attempting to protect the privacy of the customers, they were probably not determined to provide "the greatest happiness for the greatest number". More people would certainly like to see the murderer being caught and punished, as a murderer on the loose puts the lives of many to danger. Furthermore, it would be unfair if the murderer is not punished and the victim's family does not receive proper justice for their loss. Certainly, it would put more people at ease if the information reveals clues to get to the murderer. During the course of investigation with the Arkansas murder case, Amazon proclaimed in the form of a statement that they will not release information regarding a customer without a "valid and legal" binding demand. Although it was not revealed what "valid and legal" binding demand the police acquired, it was revealed that the police received some form of extracted audio recording or transcribed recording of the Echo device from Amazon. In the aftermath, a man named James Andrew Bates was found guilty of the first-degree murder of another man named Victor Collins. Many civilians and law enforcement individuals stated that the takeaway from this incident was that connected technology devices were becoming essential police investigations (Carman, 2016). Even though the incident gave rise to some privacy concerns, the end result pointed that information from technology devices helped resolve a critical situation. If Amazon concealed the data, the resolution might not have been easily reached. Solving the murder case gave satisfaction to greater number of individuals and thus resulted in "the greatest happiness for the greatest individual" (Poel, 2011). Bentham's utilitarian principle proves to be the more appropriate solution during this specific ethical dilemma.

Another ethical issue that arose with the smart assistance devices is trustworthiness. While both Google Home and Amazon Echo attempts to advance themselves by listening to others, it is sometimes difficult for them to discern what is the right action to take in a particular scenario. For an example, in San Diego, California, a local TV station presented a six year-old girl who ordered a dollhouse that worth $160 using Amazon Echo without the knowledge of her parents. When the TV stations quoted the little girl saying, "Alexa, order me a dollhouse", a bunch of people experienced their Amazon Echo proceeding to order a dollhouse based on what they have heard from the TV station. As a result, people started calling the TV station with complaints that their Echo device have responded to the TV station's request. While the device consists of streamlined 1-click ordering capability, it is hard to discern for them what a serious command is and what is an unimportant alternative. While Alexa can hear within 20-30 feet of the device, the content of what is being listened highly depends on the circumstance. In another scenario, when a customer made an error while processing an order using Amazon Echo, it was impossible for him to ask Alexa that he has changed this mind; when the customer would say "Alexa, stop!" the device would proceed to order an alternative item of the same category. In order

to actually cancel the order, the customer had to use the Alexa app or go on the Amazon website to manually perform the cancellation (Cobb, 2017). This issue gives rise to the concern of how much people can actually trust these devices during critical situations. When these devices would be used to monitor sensitive elements such as oven or water supply, they could simply fail and generate a massive disaster. Only an individual would be able to decide how much trust they can put on these smart assistance devices and to what extent.

5.3 Healthcare Devices

Along with technical issues that plague healthcare IoT devices, there are a number of ethical issues as well. One such ethical issue is that of loss of autonomy for patients choosing to use these smart medical devices. Usage of these devices involves sharing a large amount of private data such as personal health and medical records and being under constant monitoring of doctors. This can be viewed as an invasion of privacy by most people while on the other hand they may be conflicted with the benefits that come from using these devices that are not limited to better personalized patient care and constant remote observation for chronic diseases. German philosopher Immanuel Kant stated that autonomy is essential in making moral judgements. If using healthcare IoT devices robs an individual of his/her autonomy then how can we truly expect them to make moral decisions?

Not only do ethical issues arise for patients using smart healthcare devices but also for the doctors. Ashfaq Gilkar, head of IT operations at West Middlesex Hospital, said that new technologies (connected medical devices) weren't being supported because clinicians had been showing resistance either because they were too old to cope or didn't understand the technologies. And this was despite showing to them proven benefits of using such technologies (Bennett, 2014). Hence, the ethical dilemma of adopting a new healthcare IoT technology that shall benefit patients and bring costs down but at the same time may lead to lower business for older generation of doctors has restricted certain clinicians from supporting healthcare IoT devices.

Another major ethical issue that underlies use of healthcare IoT devices is the possible plan of action in the event of a malfunction or loss of information. Figuring out the responsible party when an IoT healthcare device is compromised or damaged is an ongoing debate. For example, if an IoT enabled pacemaker installed in a human body were to be hacked and sensitive personal information were to be stolen, would the company that manufactured the pacemaker be also held accountable for launching a device that lacked proper security mechanisms or would the hacker be considered the sole culprit. This ethical issue can escalate if the actual physical safety of the person wearing the pacemaker, or any other healthcare IoT device, were compromised. In today's world, it is extremely unlikely that a product has 100% reliability and even if it does, it's nearly impossible to prove that, no matter how many tests are performed. And how can a company sell a product, whose 100% reliability can't be ensured, to a customer, especially when the life of the buyer may depend on the device working reliably, as in the case of an IoT enabled pacemaker.

Similarly, while we can limit the number of users in the network who actually have access to the sensor collected medical data, it can become an issue in the case of an emergency. During an emergency, we would want the personnel responding to a distress call to have complete access to the collected medical information of the patient by the healthcare IoT device as it might contain evidence of the last known medical activity and can help determine the right treatment (Ameen, 2012). However, therein also lies the ethical dilemma of

whether such a personnel can be trusted with patient's sensitive information and guarantee the privacy of the patient without compromising medical care.

There is another ethical issue that is faced by manufacturers of healthcare IoT devices. That is the issue of how transparent they need to be as regards to the functioning of their product and handling of collected personal information from patients. The Health Insurance Portability and Accountability Act of 1996 protects sensitive medical information such as medical diagnoses, names of medications and health conditions. However, this is done only for certain entities like doctor's office or insurance companies. Healthcare IoT devices now collect the same information through wireless sensors, to which HIPAA protections do not apply (FTC, 2015). According to the U.S. Department of Health and Human Services, the HIPAA breach notification rule requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Since healthcare IoT devices aren't included under HIPAA, it may be possible that breaches of sensitive medical information collected by these devices would not be informed to the public and more importantly, to the users of these devices. On the other hand, if the manufacturers disclose such breaches then it may be possible that nobody might want to buy the product in the first place, thus causing an ethical dilemma. Similar is the case when risks associated with the smart medical devices aren't told to the public beforehand (FTC, 2015).

Yet another ethical issue that can arise due to the use of healthcare IoT devices is the unethical analysis of the medical information collected by these devices. This involves use of the medical data to price health or life insurance or to infer user's suitability for credit or employment (FTC, 2015). This type of decision making can lead to bias or discriminatory practices against certain classes of society. The Fair Credit Reporting Act (FCRA) imposes limits on the use of consumer data to make determinations about credit, insurance, employment etc. However, it doesn't cover IoT device manufacturers that do their own in-house analytics (FTC, 2015). Nor does it include companies that collect data from these connected smart medical devices. This can lead to a situation where an insurance company may offer people the option to submit the personal health data collected by their smart medical devices in exchange for lower health premiums (FTC, 2015). Thus, unethical marketing would be promoted and privacy violations can occur.

As the race for obtaining the largest market share of the growing healthcare IoT industry gets intense, companies would be faced with a hard decision of balancing efficiency against security. Due to power, memory and computation constraints, companies would need to distribute resource consumption wisely in order to make sure security is not compromised to achieve greater efficiency (Islam, 2015). Similarly, as companies produce a greater number of healthcare IoT devices, the ecological impact of producing these devices would need to be analyzed and monitored. Smart healthcare devices rely heavily on body sensors embedded in semiconductor rich devices for deployment, collection and sharing of data. These sensors and devices are made from rare earth metals and toxic chemical compounds (Islam, 2015). If the production and disposal of these

vast number of healthcare IoT devices is unchecked, then it can lead to an enormous negative impact on the environment.

5.4 Smart Home

Product quality. An ethical issue is what level of quality companies need to ensure in their products - as companies eagerly attempt to capitalize on the exploding Internet of Things house market, they often sacrifice security. Bryan and Crowley observe that companies aren't concerned with security practices as they try to push to market. Product development time is prioritized instead. Crowley remarks that "a lot of these devices is they don't require any authentication at all" to use, even if they are capable of a lot of harm when used by the wrong people (Metz, 2013). Even when consumers purchase a brand new device, the software installed on it might be outdated. In one survey, it was found that common the software in home routers "were four to five years older than the device" (Schneier, 2014). Despite the embedded computers having many security flaws, manufacturers aren't providing any easy methods to patch them. Some system components are designated as outdated and updates are no longer being made at all. This brings up the issue of how long manufacturers must support their products and what happens if the company is no longer operating. A stagnant system becomes an increased risk because vulnerabilities become more discoverable. Roya Ensafi, Princeton researchers, states that manufacturers are designing their devices "without any way to close software loopholes", leaving them insecure. Security camera maker TRENDNet had to settle a case with the Federal Trade Commision because it did not adequately represent their security flaws (Hiltzik 2016).

Companies are also manufacturing their devices under the assumption of lifelong ownership, which has serious implications when consumers are reselling devices. The products are not properly dissociated with the original owners. Lance James, Chief Scientist at the business risk intelligence company Flashpoint, "considers this to be a major vulnerability that is not being properly addressed." David Bryan, a security professional at IBM, bought a home automation hub and attempted a factory reset to clear any data and settings lingering on the device. However, it was not effective and another phone number was still listed as an administrator. In another instance, Heather Petrone-Shook, president of the Greater Philadelphia Association of Realtors, reports a client purchased a house and found that the seller still had the ability to control their Nest thermostat. She voices the importance of the issue, remarking "It can be really creepy if the seller still has access to those security cameras around your house and can see what you're doing." (Weisbaum, 2017).

Pursuing their own best interest, companies are creating proprietary designs and creating an ecosystem of devices that do not work together. Consumers are forced to be locked into one vendor if they want an integrated system.

Privacy. The numerous sensors in an Internet of Things connected home generates a lot of data and a lot of ethical discussion concerns who owns the data: the service providers or the consumers. The New York Times warns that "data can be shared in ways we don't anticipate or can be revealed as part of larger breaches" (Wood 2015). A fully connected home enables full surveillance of its tenants. The companies can record the

family's habits and gain insight on their behavioral patterns. That information can be used to create targeted advertising, creating insurance policies, rent prices, or employee hiring. Consumers are left unaware about what is being collected about them and how that data will be used.

Liability. The complex interconnection of IoT devices makes them prone to failures, and an issue is to what extent is the manufacturer held liable. Sensors might malfunction and send inaccurate measurements. This can cause waste, such as sprinklers turning on unnecessarily or lights failing to turn off automatically. Homes might not be able to be unlocked or garage doors might not be opened when the owner needs it the most.

What if one device causes a second device to malfunction, which one is responsible for the resulting damage? In 2009, Raul Rojas, a computer science professor at the Free University of Berlin, experienced this scenario when a light fixture repeatedly emitted notifications that it needed to be changed. The network was overloaded and the smart home hub froze, rendering all other smart devices to be inaccessible as well (Hill, 2015).

5.5 [Case Study] DDoS Attack using IoT Devices

One of the most important parts of a post-mortem analysis is the analyzing the ethics behind the incident. A key question in this MIRAI DDoS attack is establishing who is responsible for protecting ourselves against the attacks, as that will become the basis for organizing a series of actions that can ensure our online safety from DDoS attacks. There are both ethical and technical issues that need to be addressed in this incident. Some ethical problems that we need to address are the following:

1. Should IoT devices undergo sufficient software testing before being commercialized?
2. Was Dyn, the DNS provider, at fault for not protecting their service against DDoS?
3. What kind of trade-offs need to be established to mitigate the effects of these attacks?

We will be applying Kantianism to analyze the ethical lapses of IoT devices. To apply Kant's first categorical imperative, the Universality Principle, to this DDoS case, we first examine whether the maxim: "Business will market IoT devices knowing that the software for these devices are vulnerable to potential malicious attacks." can be universalized. We determine if this maxim can become a universal law, and can be willed without contradiction. The universal law would indicate that the selling of these devices is allowable. However, this is improbable, as no rational patient would willingly receive treatment for a device that can potentially be compromised and turned into a bot. It is clear then, that this maxim cannot be universalized, and should, therefore, not be followed by any company selling IoT devices. In addition, the second categorical imperative, Reciprocity Principle, will also not be met because companies are knowingly selling vulnerable IoT devices to consumers; they are using people's ignorance as a means to their end, which is making a revenue at the cost of these devices being used maliciously by hackers.

Many commercial devices today are Internet connected, but they are not necessarily categorized as IoT devices. A simple home printer that is enabled through WiFi has been around for decades, but it was only recently that their vulnerabilities as unsecured IoT devices had been exposed through various botnet viruses, such as MIRAI (Meyer, 2016). This raises the question of whether IoT devices should undergo sufficient security testing before being commercialized, and whether already-commercialized products should be recalled so that they can be made safe again by companies and manufactures. The ethical dilemma here can be analyzed by Kantian ethics in the Categorical Imperative. First, we apply the Universality Principle, and we want to define our maxim, which is the following: "manufacturers should sell products that should be well tested to prevent vulnerabilities made by the MIRAI or other botnet virus". This is a valid maxim because no moral customers will buy any of these products if they know these devices can be vulnerable to being taken advantage of in a DDoS attack or a hacking attack. Therefore, in order to follow through with this maxim, companies and manufacturers have a responsibility to build products that are safeguarded against cyber-attacks.

Similarly, we can analyze the responsibility that Dyn holds in making sure that their service is protected against MIRAI and other viruses. In recent years, DDoS attacks are very difficult to protect against. This can be mainly attributed to the fact that it's possible to rent a botnet of tens or even hundreds of thousands of infected or "zombie" machines relatively cheaply and use these zombies to launch an attack (Rubens, 2016). Additional techniques can only partially mitigate the situation, such as implementing rate limit on routers to prevent overwhelmed web servers, and dropping spoofed or malformed packages (Nogueira, 2016). Unfortunately, DDoS attacks nowadays are usually too large for these measures to have any significant effect. In this particular incident, Dyn could not carry out its job of acting as a switchboard for the internet, and consumers could no longer reach popular websites that relied on Dyn. However, it is important to realize that the real culprit here is not Dyn, but the various IoT devices that allows themselves to be compromised. According to a detailed report by cybersecurity expert Brian Krebs, there were a total of 68 username and password pairs in the botnet source code (Krebs, 2016). What was especially sinister about these informations is that these passwords could have been reused in many devices, including routers, security cameras, printers and digital video recorder (DVRs).

In this case, the tradeoff that needs to be established is finding a middle ground between companies that manufacture IoT devices and the threshold of security testing that can allow these devices to be commercialized. It is clear that the key vulnerability that MIRAI was taking advantage of was building botnets off of devices that did not prompt users for strong authentication, sometimes even using the default authentication. This is a very problematic pattern because these devices will continue to be used as botnet "zombies" to perform more DDoS attacks.

6 Recommendation

6.1 Smart Transportation

We can clearly see that despite the enormous potential use cases of smart transportation, there are numerous technical and ethical issues that this area faces with regards to cyber security and Internet of Things (IoT). Many of these challenges do not have a simple solution and security engineers need to constantly be up to date with new trends in cyber security and vulnerable areas within a system.

Technical Problems:

1. Hacking vehicle software
2. Preventing accidents from occurring
3. Disrupting traffic control systems in major areas of transportation.

Ethical Problems:

1. Who should be sacrificed in the case of an unavoidable accident?
2. Who should take the blame whenever a system gets compromised?
3. What percentage of autonomous transportation infrastructure should use IoT software given the risks of cyber-attacks?
4. In the case of an attack, should there be a failure option that causes the vehicle/system to stop working to prevent further damage?
5. Should IoT source code be distributed openly or removed from the public domain?

To prevent hacking of vehicle software, we would first try to make sure that the source code was written by someone well-trained in good security practices. Additionally, unit and integration testing can be used to check for any possible exploits and help minimize the weaknesses of a system. Other methods of authentication such as strong passwords and two-factor authentication will also aid in defending against hacking attempts.

When trying to prevent accidents, software should be able to consistently and reliably determine distances of one's vehicle relative to other objects on the road and in its surroundings. The technical way to improve this is to develop better object classification (and therefore computer vision) algorithms. The other thing that can also be refined over time are heuristics in each possible driving scenario and to try to develop better ways to optimize the Freedom (No Harm) Principle.

For the third technical problem, a similar idea to preventing hacking of vehicle software applies to preventing complete shutdowns of traffic control systems. Good security practices is the first step to protecting a system against attacks. Error checking, test-driven development, and strong authentication methods will help to ensure safety. Also, having multiple copies of backups on several servers or data storage centers would help to alleviate this issue.

The ethical solutions that we came up to the five previously discussed ethical problems were as follows:

From the perspective of a potential buyer of these smart vehicles, we would prefer the vehicle to ensure the driver's safety over that of others even if it is selfish, but of course, we would prefer to minimize the amount of deaths from the other affected group. The emphasis on saving the driver is derived from a phenomenon mentioned in Garrett Hardin's Tragedy of the Commons, which states that people will act in their own self-interest in order to preserve their own lives (Hardin, 1968).

We would personally argue that security engineers need to be held accountable to a certain extent. Security engineers need to be well-versed in current safety standards of the day in order to work in these fields. However, there are limits to knowledge in security since that field is rapidly evolving, and if a system gets hit with a completely new attack that has not been seen before, it would be unreasonable to punish the engineers since they could not have thought of this situation.

For this subject, we would want to weigh the advantages that additional IoT software adds to the driving experience and only incorporate those in if the strengths outweigh the security weaknesses. Otherwise, we add unnecessary vulnerabilities to our system.

We would always err on the side of caution even if we do lose data because the hacker has a lot more power if he or she gains control of our system than if we allow the system to crash and lock out the hacker.

In terms of security, we favor closed source platforms because attackers will not know exactly how the system runs internally, so they will not know of all the possible backdoors. Closed source software will usually have better bug fixes that are released more consistently with better support since one could more easily track down the original programmer on a closed source project rather than a contributor on an open source project (Veracode, 2015).

6.2 Smart Assistance

As recommendation, introducing a better algorithm is certainly a priority. Proper recognition algorithm with voice is not always easy to implement, and maybe it would be better to eliminate specific functionalities from these devices altogether to allow more trust. Perhaps, adding order cancelling functionalities would be beneficial. It would also be helpful to introduce the service of owners saving their voice to these devices, so that the devices would only listen to the specified owner and ignore any command from all other voices. As a result, during autonomous listening process, these devices would ignore information received from other individuals, protecting their privacy. Furthermore, more security needs to be introduced to these devices. One way to accomplish this would be to avoid making the software an open source platform, concealing important programming clues from hackers; any hackers could find the weakness of these devices by researching the open source codes. Eliminating open source code could potentially reduce the amount of denial-of service attacks and eavesdropping attacks as the vulnerabilities would more likely be concealed. Both Amazon and Google need to utilize better hardware in these smart assistance devices.

The connectivity issue could potentially be a product of poor hardware quality, causing the device to have compatibility issue. In addition, the speakers used in Google Home are not the best quality; Google should definitely introduce better speaker quality so that the device could better understand the speech of the user. It would also be substantial to limit these devices from performing certain tasks. While the consumers could avoid using these devices in critical situations, manufacturer could limit some of the functionalities to ensure that no unanticipated circumstances are produced. This would certainly increase the safety and privacy issues associated with smart assistance devices.

6.3 Healthcare Devices

To tackle the technical and ethical issues with healthcare IoT devices, a mixture of technical as well as non-technical solutions is needed. To handle the issue of authentication ad impersonation, a centralized control device can be used between body sensors measuring health data and the remote servers. This centralized device can simply be a smartphone that allows the user of healthcare IoT device to determine the validity of incoming and outgoing connections (Ameen, 2012). Similarly, Cyclic Redundancy Checksum (CRC), which is used to protect random errors during transmission of information, should be used to ensure integrity (Moosavi, 2016).

To ensure and promote a transparent relationship between clinicians, patients and smart medical device manufacturers, informed consent i.e. obtaining patient's permission before any medical procedures/interventions, must be taken and HIPAA should extend its jurisdiction to include healthcare IoT devices. That way any breaches would have to be reported to the public who can then make an informed decision on whether to give their consent in using a smart medical device. Also, if security breaches were to happen, then loss of information has to be minimized. One way to do that is to remove personally identifying information such as date-of-birth or five-digit zip code from medical and personal health records. It's been concluded through a study in 2009 that appropriately de-identified data sets are more secure and reduce privacy risks (FTC, 2015). Similarly, storing the data in encrypted form would help ensure that stolen data can't be useful to malicious hackers. This would provide for safer wireless transmission of data across connected devices.

Figure 14: iStan (Glisson, 2015)

Moreover, the FCRA should be expanded to cover healthcare IoT devices to prevent unethical marketing by insurance companies and impose restrictions on data analysis carried out by healthcare IoT device manufacturers. Appropriate tests need to be carried out before releasing a device into the market. Medical mannequins like iStan can prove to be very useful in this regard. iStan (shown in Figure 14) is a medical mannequin that simulates respiratory, neurological and cardiovascular systems (Glisson, 2015). Recently, an iStan was compromised by students at University of South Alabama through exploitation of its software. They even hacked a smart pacemaker installed in the medical mannequin. They performed penetration testing and explored multiple vulnerabilities through the whole testing procedure. Such testing for all healthcare IoT devices would definitely help release more secure and reliable products in future.

An end-to-end security model needs to be developed to ensure that the data communication end points are strongly protected and would help facilitate secure communication across wireless body sensors. To improve reliability, distributed storage of medical information should take place as opposed to a centralized

storage space. This would improve fault tolerance by making sure the data is always accessible - an important requirement for healthcare IoT devices.

6.4 Smart Home

Standards and Regulations. Manufacturers should be required to adhere to using the best security practices in their devices. This includes enforcing their devices to require authentication so that only the intended user can operate it. This includes using strong password that are not easily guessable. The importance of strong passwords is exemplified by the website Insecam, a site that allows people to view live feeds from thousands of security cameras that have been accessed without permission because they are using a default password (Augenbraun, 2014). Other ways to mitigate unauthorized access is to use two-factor authentication. This prevents losing one "key" to compromise the entire household. Companies should be audited by independent security professionals to ensure that companies are actually complying.

All automated devices need to have the ability to be manually overridden and operate like a normal device. This would prevent cases such as a failure in the home's automation hub from disabling the whole house and its door locks.

Standards for interfaces between IoT devices should be established by reputable engineering societies such as The Institute of Electrical and Electronics Engineers. This would solve the problem of compatibility among devices and allow a freer market where users have a choice of choosing among more options in a healthy ecosystem where product differentiation is more representative.

Data. Companies have a responsibility to protect their customers and their data. All data sent to service providers must be encrypted to prevent the harm that can be done by data breaches. HP states "configured transport encryption is especially important" for home security devices (Storm, 2015). However, Whitehouse also claims encrypted data can be analyzed by observing network traffic patterns (Metz 2013). Users should also be able to opt out of sending data completely when possible.

The data contained in a device needs to be able to completely erased so reselling it won't reveal any private information of the original owner. James wants all IoT devices to have "a mandatory self-destruct button" that resets them to the original factory setting. Such a button would need to "prove that it works before the product is sold", he elaborated (Weisbaum, 2017).

Awareness and Transparency. The security concerns are understated by companies that try to hype the products. Instead, companies must offer full disclosure of the risks. Even at the risk of hurting company stock prices, companies need to also reveal all vulnerabilities as soon as they are discovered. Educating consumers is the best way to prevent any unintended consequences. Consumers need to know what they are getting into before purchasing these internet-connected devices. Most people are unaware of any risks because disclaimers are buried under pages of legal jargon in a user manual where someone is unlikely to actually read any privacy policies. When consumers are aware of the risks, they can take better action to mitigate them. For

example, the company Bitdefender, created Bitdefender Box, "a physical device that plugs into your Internet router and constantly scans your network and the websites you visit for potentially harmful software or viruses" (Wood, 2015). Symantec similarly is marketing "a mobile-enabled WiFi router that touts machine learning and Symantec's threat intelligence smarts to defend your home network" (Lee, 2017).

Corporations would need to publish their service level agreement and inform consumers of how long they will provide updates to the software for. The updates would ideally be automatic so consumers will always have the latest and safest software.

Real estate professionals are already adapting to the world of connected homes. Keys are not the only item being transferred, but all the IoT devices too. NBC reports that "the National Association of Realtors is teaching its agents how to spot IoT devices and how to deal with them at closing", such as informing the buyers of all the devices (Weisbaum, 2017).

6.5 [Case Study] DDoS Attack using IoT Devices

As mentioned before, the source of DDoS attacks is the compromised devices that act as botnets. DDoS works so well because it takes advantage of these machines that it can use to repeatedly send requests to a DNS provider to crash their service. Taking away what fuels DDoS attacks will discourage this type of cyberattack from happening. In our case, this means we need to secure our IoT devices so that they do not become botnets. One way we can achieve this is to pass a strict set of laws and regulations on the various cybersecurity features of IoT devices. First and foremost, a strict rule on password strength and resetting passwords should be enforced. Many of the hacked IoT devices from the MIRAI virus was due to default usernames and password set forth by the companies who made them. If companies required users to make strong passwords as soon as they turned on the device, that would prevent viruses like MIRAI from penetrating the system. A simple factory-default password like 'password' will take less than an hour to crack when using John the Ripper, a state of the art open-source password cracking software. However, a password with both upper and lowercase letters will take hundreds of years to crack, even with the strongest password cracker that exists today.

In addition, the software testing process for IoT devices can be significantly improved. In fact, there should be a standardized testing procedure for all IoT devices to ensure that they all meet a universally agreed upon set of security rules. This includes an initiative to secure legacy devices that are out in the market, uses Internet connectivity, but have poor security, as they are the most susceptible to being compromised. While it was okay for the first IoT devices introduced in the market to lack in security testing, it does not make sense for current day IoT devices to follow the same pattern. As technology has advanced in the past decade, so has the sophistication of cyber-attacks, and IoT devices must follow up with that.

Lastly, all companies should follow Kantian ethics when making decisions about their products. The Universality Principle provides strong grounding for ensuring that companies think about what a moral customer would be satisfied with when looking at buying a commercial IoT product. In addition, the second categorical imperative, Reciprocity Principle, should also be met if companies initiate strong security screening of their IoT devices. Reciprocity Principle states that we should not use people as means to an end, and if companies are transparent with how secure their IoT devices are, this will allow consumers to make the rational decision of whether to buy the product or not.

The MIRAI DDoS attack is making history as one of the largest DDoS attacks. This incident was a wakeup call for both the cybersecurity field as well as the IoT industry, providing a stark reflection of the current security state in our IoT safety testing and design. It is important to learn from mistakes and reinforce for future preparation, and this case illustrated the importance of considering security as the need for IoT devices continues to grow.

7 Conclusion

An increasing amount of devices and products are falling under the category of IoT, which is connecting people across the world in an unprecedented fashion. However, the downside of having more IoT devices is that there are more vulnerabilities that malicious hackers can exploit. We can see these threats most clearly in the realms of smart transportation, smart assistance, healthcare devices, and smart homes.

Strengthening the protective mechanisms for smart transportation would require better integration testing as well as more secure methods of authentication such as stronger passwords and two-factor authentication. Also, accident prevention would need better algorithms to determine relative distances and more heuristics to track each possible driving scenario.

For smart assistance, improvements could be made in terms of security by handling misinformation or false data better, implementing more sophisticated listening algorithms, incorporating better hardware connectivity, avoiding open source software, restricting potentially dangerous devices, and educating the public about the weaknesses of these devices. Like smart transportation, improving the software only goes so far; the public needs to be more careful when using smart assistance devices and understand the shortcomings that these devices present.

In the realm of health care, some recommendations would be to encrypt stored data, centralize a control device, and limit personal information with regards to stored and transferred data. This is because hospitals are major targets of ransomware attacks since lives are at stake. These practices will help keep the healthcare devices up and running with backed up data even if one of the device channels is attacked.

With regards to smart homes, it is vital for the seller to maintain a lot of transparency with the customer, especially when it comes to data usage and liability. Ideally, the smart home product sellers should provide compatible interfaces to give consumers more options to choose from, but they should also let the customer know exactly what risks are entailed when using smart home devices like Nest. Much like the previous examples, education is paramount to ensuring the integrity of customer data.

Lastly, with respect to the DDoS attack case study, this builds on the previous recommendations and reaffirms three major recommendations that are important in any cybersecurity scenario. The first is enforcing a strong password reset; passwords should have a mix of alphanumeric characters along with punctuation marks, capital letters, and assorted symbols to make it more difficult for hackers to crack. Secondly, a standardized testing procedure would help to ensure the security quality of an IoT device is safe enough to be released to the market. The third and final recommendation is to follow the Universality Principle when making design decisions for IoT devices. This is because the product seller must avoid bias towards certain demographics since this will tend to compromise the security quality of IoT devices.

8 References

Ameen, M. A., Liu, J., and Kwak, K., 2012, Security and privacy issues in wireless sensor networks for healthcare applications: *Journal of medical systems*, v. 36, pp. 93-101.

ArXiv, 26 Oct. 2015, Emerging Technology from the. "Why Self-Driving Cars Must Be Programmed to Kill." *MIT Technology Review. MIT Technology* Review, Web. 17 Feb. 2017.

Augenbraun, Eliene, 11 Nov. 2014, "Site Exposes Security Weakness in Thousands of Webcams." *CBS News*. CBS Interactive, Web. 20 Mar. 2017.

Baca, Joshua. January 17, 2017. "Overheard: Debate Over Alexa and Data Regulation." *Federal News Radio*.

Barajas, Omner. April 24, 2016. "How Internet of Things (IoT) Is Changing the Cyber Security Landscape." *Security Intelligence*.

Barker, Colin. 11 Nov. 2015. "Six Billion Connected Devices by next Year: The Internet of Things Takes Shape." *ZDNet*, Web. 20 Mar. 2017.

Bennett, M., August 28, 2014, Doctors and nurses need to take their Internet of Things pills: *The Inquirer*.

Bisson, David. April 15, 2016. "DDoSCoin - An Incentive to Launch DDoS Attacks?" *Bleeping Computer*. N.p., n.d. Web. 17 Mar. 2017.

Blumenthal, Eli. October 22, 2016. "Hacked Home Devices Caused Massive Internet Outage." *USA Today*. Gannett Satellite Information Network.

Brush, A. J., 2011, "Home automation in the wild: challenges and opportunities." *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM.

Carman, Ashley. December 27, 2016. "Police Want an Echo's Data to Prove a Murder Case, but How Much Does It Really Know?" *The Verge*.

Cobb, Stephen. January 10, 2017. "Amazon Echo and the Alexa Dollhouses: Security Tips and Takeaways." *We Live Security*.

Curtis, Sophie, 21 July 2015, "Hacker Remotely Crashes Jeep from 10 Miles Away." *The Telegraph*. Telegraph Media Group, Web. 17 Feb. 2017.

"Cyber Security and Resilience of Intelligent Public Transport. Good Practices and Recommendations." *Cyber Security and Resilience of Intelligent Public Transport. Good Practices and Recommendations* ENISA. N.p., n.d. Web. 02 Feb. 2017.

"Cybersecurity and the Future of Smart Cars." *IBM Big Data & Analytics Hub*. N.p., n.d. Web. 02 Feb. 2017.

Davis, Christopher, 19 Nov. 2003, "UF "Smart Home" Demonstrates Concept Of Automated Elderly Help And Care." UF. *University of Florida News*, Web. 17 Feb. 2017.

D'Olimpio Laura. 17 Mar. 2017. Senior Lecturer in Philosophy, University of Notre Dame Australia. "The Trolley Dilemma: Would You Kill One Person to save Five?" *The Conversation*. Web. 20 Mar. 2017.

Ducklin, Paul, 24 Oct. 2016, "Mirai "internet of Things" Malware from Krebs DDoS Attack Goes Open Source." *Naked Security*. Sophos. Web. 27 Jan. 2017.

Etherington, Darrell, and Kate Conger, 21 Oct. 2016. "Large DDoS Attacks Cause Outages at Twitter, Spotify, and Other sites." *TechCrunch*. Web. 03 Feb. 2017.

Federal Trade Commision, 2015, Internet of Things: Privacy and security in a connected world: Federal Trade Commision, 71 p.

Foster, Peter, 17 May 2015. "Hacker 'made Plane Climb' after Taking Control through In-flight Entertainment System." *The Telegraph*. Telegraph Media Group, Web. 17 Feb. 2017.

Gallagher, Sean, 21 Oct. 2016. "Double-dip Internet-of-Things Botnet Attack Felt across the Internet." *Ars Technica*, Web. 03 Feb. 2017.

Glisson, W. B. et al, 2015, Compromising a medical mannequin: Mobile, Alabama: Cornell University Library, arXiv:1509.00065, 11 p.

Gomez, Carles, and Josep Paradells, 2010, "Wireless home automation networks: A survey of architectures and technologies." *IEEE Communications Magazine* 48.6.

"Hackers Successfully Ground 1,400 Passengers." *CNN*. Cable News Network, n.d. Web. 17 Feb. 2017.

Hardin, Garrett. "The Tragedy of the Commons," 13 Dec. 1968, Vol 162, No. 3859.

Herzberg, Ben, 26 Oct. 2016, "Breaking Down Mirai: An IoT DDoS Botnet Analysis." Incapsula.com. *Imperva Incapsula,* Web. 18 Mar. 2017.

Hill, Kashmir, Mar. 2015, "This Guy's Light Bulb Performed a DoS Attack on His Entire Smart House." This Guy's Light Bulb Performed a DoS Attack on His Entire Smart House. *Fusion*, Web. 20 Mar. 2017.

Hiltzik, Michael, 1 Mar. 2016, "Apple, the FBI, and the Internet of Things: Your Whole House Is Open to Attack." *Los Angeles Times*. Los Angeles Times, Web. 17 Feb. 2017.

Hong, Jinkeun. "Cyber Security Issues in Connected Vehicle of Intelligent Transport System." *Indian Journal of Science and Technology* 9.24 (2016): n. pag. Web. 2 Feb. 2017.

Hsu, Tiffany, 7 Oct. 2016, "Smart Owners Leave the House to Its Own Devices." *Los Angeles Times*. Los Angeles Times, Web. 17 Feb. 2017.

"IBM Knowledge Center." *IBM Knowledge Center*. N.p., n.d. Web. 03 Mar. 2017.

"Introduction To Transportation Systems." *Transportation Systems Security* (2008): 1-10. Web. 2 Feb. 2017.

Islam, S.M.R. et al, 2015, The Internet of Things for health care: A comprehensive survey: *Institute of Electrical and Electronics Engineers*, v. 3, pp. 678-708.

Kiss, Jemima, 13 Mar. 2016, "Your next Car Will Be Hacked. Will Autonomous Vehicles Be worth It?" *The Guardian*. Guardian News and Media, Web. 03 Mar. 2017.

Krebs, Brian, 21 Oct. 2016, "Krebs on Security." *Krebs on Security*. N.p., Web. 17 Mar. 2017.

Lagace, Marc. January 16, 2017. "Common Amazon Echo Problems and How to Fix Them." *AndroidCentral.*

Lee, Nicole, 03 Jan. 2017, "Symantec's Norton Core Router Aims to Protect the Connected Home." *Engadget*. Engadget, Web. 20 Mar. 2017.

Martin, James A. November 7, 2016. "Why You Might Want to Hold off Buying Google Home." *CIO.*

Meola, A., December 19, 2016, Internet of Things in healthcare: Information technology in health: *Business Insider.*

Metz, Rachel, 19 Sept. 2014, "You Should Be Wary of." *MIT Technology Review*. MIT Technology Review, Web. 20 Mar. 2017.

Meyer, Robinson. 21 Oct. 2016, "How a Bunch of Hacked DVR Machines Took Down Twitter and Reddit." *The Atlantic.* Atlantic Media Company, Web. 03 Feb. 2017.

Moosavi, S. R. et al, 2016, End-to-end security scheme for mobility enabled healthcare Internet of Things: *Future Generation Computer Systems*, v. 64, pp. 108-124.

Moynihan, Tim. December 5, 2016. "Alexa and Google Home Record What You Say. But What Happens to That Data?" *Wired.* Conde Nast.

Nest. 21 Oct. 2011. "Hand Adjusting a Blue Nest Learning Thermostat." Flickr. Yahoo! Web. 20 Mar. 2017.

Nogueira, Michele, December 1 2016, "Anticipating Moves to Prevent Botnet Generated DDoS Flooding Attacks*". CoRR*. Volume 1611.09983.

Pettypiece, S., May 7, 2015, Rising cyber attacks costing health system $6 billion annually: *Bloomberg Technology*.

Press, The Associated, 03 July 2016, "Authorities Investigate First Driver Death in Self-driving Car Accident." *NOLA.com*. N.p., Web. 17 Feb. 2017.

"Polish Teen Derails Tram after Hacking Train Network." *The Register® - Biting the Hand That Feeds IT*. N.p., n.d. Web. 18 Mar. 2017.

Rubens, Paul. 2016. "6 Tips for Fighting DDoS Attacks." *ESecurityPlanet* N.p., Web. 03 Mar. 2017.

Saleem, S., Ullah S., and Kwak, K. S., 2011, A Study of IEEE 802.15.4 Security Framework for Wireless Body Area Networks: Sensors, v. 11, pp. 1383-1395.

Schneier, Bruce, 06 Jan. 2014, "The Internet of Things Is Wildly Insecure — And Often Unpatchable." *Wired.* Conde Nast, Web. 20 Mar. 2017.

"Security of Autonomous Vehicles." *Security of Autonomous Vehicles*. N.p., n.d. Web. 02 Feb. 2017.

"Security Showdown: The Open Source vs. Closed Source Debate." *Veracode*, 22 Jan. 2015, N.p., Web. 03 Mar. 2017.

Storm, Darlene, 11 Feb. 2015, "IoT-connected Home Security Systems." *Computerworld.* Computerworld, Web. 20 Mar. 2017.

The Economist, 11 June 2016, "Where the Smart Is." *The Economist*. The Economist Newspaper, Web. 17 Feb. 2017

"The Merits of Open Source vs Closed Source (Proprietary) Software." 06 Nov. 2014, *Java PDF Blog*. N.p., Web. 20 Mar. 2017.

Torres, Timothy. 06 Oct. 2016. "Google Home vs. Amazon Echo: Which One Should Rule Your Smart Home?" *PCMAG*. PCMAG.COM, Web. 20 Mar. 2017.

Vowell, Peter, Web. 17 Feb. 2017. "What Is DDoS?" *Announcements and Resources for Developers*.

Weise, Elizabeth. October 22, 2015, Fitbit hacked from 10 feet away, security firm says: *USA Today*.

Weise, Elizabeth. March 2, 2016. "Hey, Siri and Alexa: Let's Talk Privacy Practices." *USA Today*. Gannett Satellite Information Network.

Weisbaum, Herb, 28 Feb. 2017, "Secret spies: Smart homes aren't smart enough to know you moved out." *NBCNews.com*. NBCUniversal News Group, Web. 20 Mar. 2017.

Wood, Molly, 07 Jan. 2015, "CES: Security Risks From the Smart Home." The New York Times. *The New York Times*, Web. 20 Mar. 2017.

Woodyard, Chris. February 6, 2017. "Google's Super Bowl Ad Makes Google Home Systems Go Crazy." *CNBC*.

Yu, Howard. November 28, 2016. "Google Home, And What Amazon Gets About Innovation That Google Doesn't." *Forbes*.

Zetter, Kim, 22 June 2015, "All Airlines Have the Security Hole That Grounded Polish Planes." *Wired*. Conde Nast, Web. 18 Mar. 2017.