Jorie Fernandez

Moe Abdipour

TCSS 431 A

Final research paper

**The Internet of Things, the New Unavoidable Challenge**

We live in a world where nearly all aspects of our lives are being connected and managed online. This phenomenon is known as The Internet of Things (IoT). The connection to the web of everything with everything. On the face of it, this technological achievement is a powerful tool that has the potential to make our lives easier and more productive, but there is a dark side as well. Every device we connect to the web, from our car navigation systems to the locks on our front doors and the thermostats in our homes, becomes a potential entry point to our networks for malicious hackers to exploit. “It seems the unending chess match between hackers and security experts has found a new field of play.” (Greenemeier, 2011, p. 18). Traditionally, as a nation of daily internet users, we have been most concerned with securing our private data and personal information, but what if there were more at stake? For every hacktivist and financial cybercriminal there is a shutdown of the power grid or a triggering of a defense system. The world has grown extremely sophisticated and so we must grow with it if not beyond it. How else can we hope to defend and maintain dominance as a nation in a world where the balance of power is ever changing? The question then becomes can technology be made to harm us?

**Background**

British tech entrepreneur Kevin Ashton is generally credited with coining the term “Internet of Things” back in 1999 while working as an assistant brand manager for Proctor & Gamble where he had become interested in using RFID technology to manage the company’s supply chain. He envisioned a future where RFID tags would be attached to everything allowing computers to track, inventory and manage our lives. The concept, though, of interconnected devices sharing data across a vast network was first discussed as far back as 1982. At Carnegie Mellon University, a modified soda machine became the first internet connected appliance. It was able to track and give updates as to its current inventory as well as report on whether or not the drinks it held were cold.

Fast forward nearly four decades to the present day where there are estimated to be about 6 to 10 billion devices connected to the internet world wide. That number is estimated to double by the year 2020. From the cars we drive to the homes we live in, so much of our lives have become connected that we don’t really give much thought to the security protocols that are required to maintain stability and safety. We have always been concerned with safeguarding our personal data, but what about our personal safety? Every new device connected to the internet brings with it convenience and vulnerability. Every new connection is a possible point of entry for those looking to cause mischief or real harm.

Until very recently the focus of security when it comes to computers and the internet has been on personal information. We encrypt our wireless connections, create complex passwords we can’t remember, and even use our fingerprints to restrict access to things like our banking information or our personal correspondence. We are all aware of identity theft, but we have never given much thought to how hackers could infiltrate our lives and cause us actual physical harm. With so many new devices being created with internet connectivity it is guaranteed that there will be security failures somewhere amongst them. According to Huansheng, Hong, and Yang (2013), attacks can be classified into four categories; gathering attacks, imitation attacks, blocking attacks, and privacy attacks. Gathering attacks involve the skimming of transmitted messages for useful data, the collection of entire messages for later analysis, and the monitoring of network traffic in the hopes of finding an exploitable pattern. Imitation attacks allow hackers to gain unauthorized access to a system by tricking the authentication process into thinking they are the authorized user. Blocking attacks interfere with communications and prevent authorized use much like a directed denial of service (DDoS) attack. Privacy attacks seek to directly harm an individual or group by disclosing sensitive information collected on them. Any of these techniques have the potential to cause lasting damage, but when it comes to the security of our connected vehicles it is the imitation attacks and blocking attacks that we should be most concerned with.

Live updates to your vehicle’s in dash navigation system. Targeted ads about services available at the next off-ramp. Remote starting of your car from your smart phone. These are just a few of the technologies that are already here or are on the near horizon. They are all very exciting, but what if your vehicle's connection to the internet were accessed by an unauthorized party? They may simply cause mischief like changing your radio station or adjusting your climate controls, but what if they were a bit more sadistic? What if you were driving down the highway with your family on a Saturday afternoon when suddenly your car begins to accelerate wildly and the brakes do not respond? These scenarios are not science fiction. They have already been proven to exist in some vehicle manufacturers most popular models. Connected vehicles are quickly becoming smartphones on wheels and so are susceptible to all the same dangers that any other of our personal devices and computers are. Unlike our phones though, “cars are big hunks of metal and, when not in control, can do a lot of damage. BMW recently admitted that its ConnectedDrive platform had been hacked by researchers, who took control of the air conditioning and door locks” (Kirk, 2015, p. 17). Ford’s Sync system along with GM’s OnStar has also proven to be currently vulnerable by researchers working at the University of Washington. These systems, equipped with cellular connections, are typically used to perform safety functions (Milo, 2011). “Researchers found that they could take control of this system by breaking through its authentication system. The relative ease of access the researchers were able to achieve points out the vulnerability of many of the electronic systems in today’s cars” (Milo, 2011, p. 6). In 2015 it was widely reported that researchers had identified and then utilized a technique known as a zero-day exploit to remotely hack Jeep’s in dash entertainment unit. This allowed the researchers to take control of several systems within the vehicle such as the climate controls, the radio, and the windshield wipers. As with the previous Ford and BMW examples these are relatively harmless examples of wireless vehicle hacking, but the Jeep example is different in that the researchers involved were also able to gain access to critical parts of the vehicle like the transmission, engine acceleration, and braking (Greenberg, 2015). This was all done from a laptop in a home nearly 10 miles away from the test vehicle. Vulnerabilities like these must be identified early by manufacturer testing and corrected before the vehicle in question ever becomes available to the public. “When you lose faith that a car will do what you tell it to do it really changes your whole view of how the thing works” (Greenberg, 2015).

**Security in IoT**

IoT projects security risks as it is considered an evolutionary form of the Internet. According to Furfaro and others, “IoT scenarios data come from the physical world through the sensors installed on smart devices, thus, widening the range of possible applications.” Through the IoT, the concept of smart devices is realized. It can impact broad domains including “personal and enterprise environments (Furfaro, et. al).” While the goal of IoT is to improve the quality of life, it also becomes a target of cyber criminals. As the devices become more interconnected, the potential risks for attack vectors also increases. According to Furfaro and other researchers, it is estimated by 2020 that billion devices will be connected to the Internet. Thus, the security cost will increase by “20 % of the annual security budgets.” However, security policies are still not up to par to the advancement.

Furfaro and others identified the “presence of manufacturers that lack experienced with networked devices” as an important factor in IoT industry security. They use the system to increase production and minimize the cost, however, they end up neglecting the implementation of the security designs. The haphazard development and deployment also play a role on the security issues. When privacy and security design is not integrated to the system development of the IoT technology, the vulnerability is increased. For instance, a device who connects to different devices can collect an amount of data through the server. The authentication can be a vulnerable especially if server vendors are controlled by different users.

Kolias and others had identified the most severe security and privacy threats in IoT. These are the leakage of personally identifiable information (PII), leakage of sensitive user information, and unauthorized execution of functions. With the leakage of PII, the main issue is the “geofencing through the GPS technology, where mobile push notifications from apps are provided when device owner enters an area.” Because of its location precision, “IoT retail applications can be used to target these users for advertising and asset tracking.” It acts as a user tracking device implicating the consumer’s privacy through data mining. Since IoT devices are connected wirelessly, there is an insecure wireless communication leading to vulnerabilities, such as “jamming, eavesdropping, or message injection.” Kolias and others added that attackers can “manipulate the execution of the wireless protocol via the transmission of forged media access control (MAC) layer messages, precisely in the 802.11 (Wi-fi) protocol.” Thus, denial-of-service (DoS) and Man-in-the-middle can be utilized to take advantage of the system. The authentication process is also very limited in IoT commercial products. Therefore, a simple hashing can be easily generated.

**IoT Limitations and Environment**

The distributed IoT consider a heterogenous network authentic configurations as described by Krishna. It can be attributed to the limitations associated to the Internet-based IoT. One of these limitations is the architectural compatibility from a network of heterogenous network composed of sensors, Bluetooth, and others. Thus, different security protocols should be integrated based from the devices used in the network. Another limitation is the functional differences, where the differences in the cycle of devices causes varying key validation periods. “The limited resources and constrained bandwidth can lead to the differences affecting the frequent key verification, which is used to measure the degree of trust to invalidate the intruded parts of the network (Krishna).” There is also a deliberate delay and modification in IoT deployment because of the “sparse immediate relay nodes”. This, in turn, affects the performance of the IoT and can be used by the intruders to their advantage. By causing further delays on the active route paths, the maligned nodes can cause the compromise of the security keys. Thus, the attackers can modify the data and change the destination node. They can also cause the spread of malware. An example, according to Furfaro is the first malware in the IoT was Linux.Darlloz, which was discovered by Symantec in 2013. Unfortunately, because of the limited resources to the devices, using antivirus is not possible as it could strain the device.

The IoT utilizes the features from cloud to enable virtual environment manage the resources in the network. Thus, security keys play a role in the confidentiality and validation of the IoT channels. Krishna stated that the “Service-oriented architecture (SOA) for IoT middleware consists of modules such as service composition, service management, and object abstraction.” Through the service component layer, a workflow is generated in “executable SOA processes.” This occurs through the web service definition language used by the service component layer. It helps in the dynamic discovery of the devices and checking the functional status for connectivity.

**Design Metrics in Security and Trust Management Systems**

Per Krishna, the security and trust in the IoT protocols are based on the validation, confidentiality, and authentication of the system. Therefore, it is necessary to examine the properties of trust management system of the IoT technology. These properties are the degree of reputation, degree of trust, degree of communication, and trusted node. The degree of reputation is measured as a “function of public and private keys that are exchanged between the nodes. The degree of trust is based from the maximum available bandwidth and the number of key mismatches.” The degree of reputation is the ratio of degree of reputation to the degree of trust rate. A node is then considered trusted based from the rate of the successful and failed transactions to the number of keys exchanged in the server. Therefore, to evaluate the trustworthiness of the IoT, it should be expected for the user to receive information that they believe to be secured and true and it is received in quality and on time. It is done by defining a reference trust that can be used before sending a message to an object by using a threshold value. If it does not meet the adjusted threshold value function, it can cause leakage of information. The leakage of sensitive information in IoT is caused by a bad protection during data transmission, for instance, not using the Transport Layer Security. Some hardware does not support the public-key cryptography so they are incapable of supporting the SSL/TLS protocol. As a result, the data are transmitted in plain text, which gives the attacker an easy access.

Below are the security threats retrieved by Krishna from IEEE.

**Types of Security Threats and Attacks in Sensor Networks.**

**Reproduced with permission of IEEE**

|  |  |  |
| --- | --- | --- |
| Type of Security Attack | Nature of Attack | Proposed Security and Trust  System |
| Bad mouthing attack | Malicious nodes defame the  trusted nodes or increase  the trust values of  compromised nodes. | Direct trust rate is more than  the threshold value and  indirect trust considers mean  and variance of probability  (Sun et al. 2008b) |
| Colluding and mobile  attack | After retrieving the secret  keys, the malicious nodes  attack the trusted nodes and  broadcast the compromised  nodes as valid nodes. | Verify and validate time-based  sequence numbers of secret  key broadcast message  (SKBM) and authentication  key disclosure message  (AKDM) (Tas & Tosun  2011). |
| Node inconsistencies | Nodes act as untrusted nodes  and create inconsistency in  the network. | Validate the number of awards  and penalties to assess the  degree of trust for consistent  and inconsistent nodes (Deng  et al. 2009). |
| Node selfishness | Nodes act as non-cooperative  nodes and disobey the  neighboring nodes. | Measure the probability of node  selfishness based on the rate  of energy consumption (Bao  et al. 2012) |
| Malicious impersonation  attack (e.g., man-in-the  middle) | Malicious nodes impersonate  the trusted cloud and  service providers to target  the users. | Measure the cost, trust, and  reputation degrees of service  provider (Zhu et al. 2015) |

Sensor nodes used in wireless and IoT are vulnerable with the attacks as shown in the table above.

**Case Study**

Furfaro and other created a scenario to investigate the exploitations of smart objects in the IoT network. They used the features of SMALLWORLD, a software platform to support the assessment of the security-related issues. The architecture is composed of five layers which are the physical layer, abstraction layer, core service layer, agent engine, and the API layer. It can be used either in site or in cloud. The IoT scenarios are used to assess the cybersecurity issues and suitable risk evaluation. It is focused on data leakage attacks, in a depicted smart home setting. The virtual environment hosted in SMALLWORLD hosts some nodes that will interact on the outside world, internet, and local network. A malicious code is run in the virtual machine. There are also other nodes running in the virtual environment, which are the personal computer, multimedia system and a tablet. The real devices involved in the scenario are the smart surveillance camera, which is simulated as connected to the home LAN, and infected Android mobile phone, which can exploit LAN through the Wi-Fi access point and Internet provided by mobile network subscription.

In the simulation, two agents are injected in the personal computer and malicious node in the VM. In the scenario, the PC is used to access the internet and the surveillance camera. The malicious node, on the other hand, is used to send commands to steal the data.

In the proposed scenario, the remote attacker uses the “Android Stagefright Integer Overflow vulnerability, which occurs when parsing crafted MP4 files, to run the commands. It is designed to worked with HTML5 compliant browser to exploit. It is done by adding MP4 files consisting two files, which when the sizes are added together causes an integer flow. The attack is done by “adding payloads of the multimedia message the binary code of a backdoor.” The malicious code is then sent to the user’s email or other links or applications. Once downloaded, it executes “a background telnet service listening on port 1035 which performs tasks intended to steal information stored on the phone without the user being aware of it. The attacker remotely controls the malicious application by connecting to the backdoor port through which he can access a command shell prompt” (Furfaro, et. al).

The commands can start a network scan to find other devices in the IoT network. It then gathers information, for instance, a device model, and then sent to the “malicious Command and Control (c&c) server. The server checks other vulnerabilities based from the transmitted result.

Attacking the LAN, the attacker can send “spoofed Address Resolution Protocol (ARP) messages, which will associate the smartphone’s MAC address with the IP address of the default gateway (Furfaro, et.al).” This will transmit the LAN traffic towards the attacker. Now, he can check the packets and get more information. When the personal computer is used to access the surveillance camera, it sends the credentials without the encryption. The attacker can then use this to edit the configuration to be accessible in the Internet. Afterwards, the attacker can use the gathered information for their advantage.

**Securing the Network**

Based from the described scenario above, installing a firewall is necessary to secure the smart home. It is necessary to configure the firewall in a way that it separates the devices to the router and other external devices. When the phone is used to connect to the network, firewall will be bypassed. Therefore, another countermeasure should be employed by identifying the devices to be protected, grouping them into logical groups, identifying which devices are critical and not, and isolating them in a sub-group or sub-network. The subdivision can be done by using Virtual LANs to minimize the compromise of the entire network.

Key encryption is also highly recommended. It would be best if each layer will have security mechanisms in order to ensure that the information received is to be trusted.

**Current Security Policies**

Security policies in recent years have started to catch up with the Internet of Things. Until now security has been sort of an afterthought. Manufacturers of connected devices used established methods of authenticating users and protecting data, but a knowledgeable and determined hacker will always find a way. Smart objects are commonly interconnected using a wireless IEEE 802.15.4 network and its existing security mechanisms (Raza, Duquennoy, Hoglund, Roedig, & Voigt, 2014, p. 2654). “In the context of the Internet of Things such an approach fails to provide end-to-end security in terms of authentication, integrity, nonrepudiation, and confidentiality. Clearly, additional or alternative mechanisms are required” (Raza, Duquennoy, Hoglund, Roedig, & Voigt, 2014, p. 2654). Last year, Dell computer released a statement outlining their corporate vision for security moving forward. It outlines a 5-step process for improving security without necessarily diluting the end user experience. Number one on the list is putting security first above all else as a priority from design and manufacture all the way to the store shelf. Other points include constant auditing of the network and compartmentalizing traffic using virtual networks. Many major technology companies, including those like Google, IBM, Cisco, Samsung, and Microsoft, have formed various consortiums to try and settle on an industry standard regarding communication and security between smart devices.

According to a Symantec Report, “both Industrial IoT ecosystems, like the Industrial Internet Consortium (IIC), and consumer IoT ecosystems, such as the AllSeen Alliance, are still very early in defining standards for this rapidly evolving area. Symantec published its Security Reference Architecture” and coordinated with other organizations to address the issue. Effective security layers should be implemented along with the strong SSL/TLS encryption technology.

**References**

Greenberg, Andy. (2015). Hackers Remotely Kill Jeep On The Highway-With Me In It. Wired. Retrieved from http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Greenemeier, Larry. (2011). Hack My Ride. Scientific American. vol.304(6), 18.

Huansheng, N., Hong, L., & Yang, L. (2013) Cyberentity Security in the Internet of Things. Computer, vol.46(4), 46-53.

Kirk, Richard. (2015). Cars of the future: The Internet of Things in the automotive industry. Network Security, vol.2015(9), 16-18.

Milo, Paul. (2011). They could hack-jack your car. Evaluation Engineering, vol.50(5), 6.

Noor, Ahmed K. (2015). The connected life: the internet of everything coming to a building near you. Mechanical Engineering-CIME, vol.137(9), 36-41.

Raza, S., Duquennoy, S., Hoglund, J., Roedig, U., & Voigt, T. (2014) Secure communication for the Internet of Things. Security and Communication Networks, vol.7(12), 2654-2688.

Furfaro, Argento, Parise, and Piccolo. "Using Virtual Environments for the Assessment of Cybersecurity Issues in IoT Scenarios." Simulation Modelling Practice and Theory 73 (2017): 43-54. Web.

Sujithra, & Padmavathi, G. (2016). IOT security challenges and issues - an overview. World Scientific News, 41, 232-239. Retrieved from <https://search-proquest-com.offcampus.lib.washington.edu/docview/1790168322?accountid=14784>.

2016 Internet Security Report. Retrieved from <https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>.

Krishna, M. Bala. Trust Impact