Exploiting Telnet Security Flaws in the Internet of Things

James Klein and Kristen R. Walcott

University of Colorado, Colorado Springs,
jklein@uccs.edu and kwalcott@uccs.edu

Abstract. The Internet of Things (IoT) is a developing technology which allows any type of network device inside a home to be linked together. IoT is based on older Wireless Sensor Network (WSN) technology and has been reduced to smaller size and scale for home use. However, both the original WSN and developing IoT technology has inherent security flaws. This paper identifies and evaluates security issues and their underlying causes in IoT technology. We focus on IoT reliance on known exploitable network ports and the difficulty of recovering from such attacks. Most IoT implementations utilize Telnet to communicate between devices. We explore the vulnerability of Telnet connections through a simulated IoT environment. Our results show that Telnet vulnerabilities can be exploited by attackers and grant access over IoT devices allowing the modification of devices and subtle spying on any data being transmitted.

Keywords: Internet of Things (IoT), Telnet Vulnerabilities, Security

1 Introduction

We live in a world with a constantly evolving battle between new technologies and threats to those technologies. To stay ahead in the evolving technological world, companies often base new systems and technologies on older ones. This practice makes it easier for new technologies to advance more quickly, and to drive the market and increase profit margins. Unfortunately, this haste also leaves in known security vulnerabilities at the fundamental levels in new technologies that never are addressed and which are supplied to the public. The problem is a systemic one as IoT continues to connect various devices together.

As IoT technology has advanced, viruses and attacks against this sort of technology have become more common to the point where they are a constant threat. There are daily attacks against IoT environments because they are easy to gain control of due to lack of security and are high value targets [1]. Part of this is due to modern IoT technology evolving from WSNs and inheriting some of its flaws and vulnerabilities. An example of this is that some IoT environments utilize network port 23 (Telnet) to communicate [2]. This practice originated in the WSN technology and has continued into the modern IoT.

Successful Telent attacks against IoT networks have jumped since 2014 [3]. Due to exploits like Telnet, every modern device that can connect and utilize this technology has become a risk. In the past, we would not have considered our toasters capable launching Distributed Denial of Service (DDoS) attacks, but today it is possible. Our drive to upgrade everything in our environment with technology means that we do so without considering the security risks and leave ourselves vulnerable. Refrigerators, televisions, and garage doors are just some of the more common devices which now include wireless technology that can be exploited [4].

Every environment with an IoT device is at risk and can be exploited with the right conditions. This has both local and global consequences. Locally, a compromised IoT environment can provide all sorts of personal information such as credit card numbers, usernames and passwords, bank account information, and even give physical access to homes through IoT locks. On a larger scale, a compromised system can be used to compromise more systems, and multiple systems can be used to launch DDoS attacks. These types of security issues are a major risk and if not corrected IoT technology could destroy itself in its infancy because security problems were not exposed and addressed [5].

To better understand how vulnerable IoT is given exploits in IoT, we need to examine IoT and relate exploits at a conceptual and practical level. At the conceptual level, we look at the WSN roots for vulnerabilities that can be addressed. For a practical analysis, a simulated test environment will be constructed to see the extent of IoT's vulnerabilities and to consider ways to make it more secure. One practical vulnerability we focus on is that IoT is reliant on wireless networking, routers, and protocols, such as Telnet. While these devices come with some basic security features, they are not always enabled by default or configured correctly. Moreover, if the security is overcome, then everything connected becomes vulnerable as there are no redundant security measures.

In this research, we look at the history of the IoT technology so we can understand where the inherited security issues originated, examine how IoT can be used both in industry and in the home so we can consider what kind of security is needed, and finally analyze some potential security vulnerabilities to investigate possible mitigation [6]. Utilizing the above, we created a simulated IoT environment with the inherited Telnet security risk in IoT and allowed outside attackers to attempt to exploit the environment. Our results show that having vulnerable Telnet systems in an IoT environment allows potential attackers access to the IoT environment, and any other wireless devices connected to it to a worrying degree.

In this paper, we make the following contributions:

- Analyze potential security vulnerabilities in IoT systems. (Section 2)
- Experimentally demonstrate Telnet security vulnerabilities in IoT. (Section 3)
- Discuss the observed vulnerabilities and causes in a simulated IoT system. (Section 3.5)

2 IoT Technology

IoT attempts to connect all separate wireless devicesas well as allow for remote connection and control of them. Most IoT devices use WSN technology as a backbone. In this section, we discuss the role of WSNs in IoT and some vulnerabilities that are then inherited.

2.1 The Role of WSNs in IoT

WSNs were initially limited in use, so there were not many opportunities for hacking or security exploitation. The first Wireless Sensor Networks were developed as Distributed Sensor Networks (DSN) at the Defense Advanced Research Projects Agency (DARPA) in 1978 [7]. Later, WSNs were created to utilize wireless and modern networking technology to be easily able to communicate, and the sensors themselves are small and powerful, yet also cheaper and more disposable to make the technology viable.

IoT utilizes the same basic technology as a WSN, but, instead of being used for wide scale corporate technologies, it is scaled more specifically to the home environment. IoT uses home routers and wireless receivers to correlate data useful specifically in a home environment and helps run a home more efficiently and effectively by automating some of the functions normally done manually. IoT took the basic WSN technology to the next step, but instead of reengineering it from the ground up and including new modern security in it, quite a bit has been taken and reused leaving potential security issues waiting to be exploited.

Securing of private information becomes more important when coupled with IoT [8]. When an IoT network is running in a home, it naturally stores more personal information as it is automating personal living preferences and attempting to make normal mundane tasks simpler. Thus, much personal data and preferences are stored and sent over the IoT. If it is not well protected, it could easily be intercepted and stolen. That in turn could lead to an increase in personal security risks, stolen identities, and public data that should be private.

2.2 IoT Security

IoT and the underlying WSN technology have a number of inherent security problems and risks. For the WSN issues, these underlying problems came with the original technology and have carried through to the current IoT implementations. These concerns need to be taken into consideration so they do not continue to undermine the security of the entire technology. The evolution of the technology from WSNs into IoT has also created some new concerns which need to be solved and implemented to ensure that the increased amount of private data contained by the IoT does not cause security vulnerabilities to its users.

WSN Security Concerns Most original WSN wireless sensors do not naturally encrypt the data it will be transmitting. Home wireless setups do not

encrypt the data passed over it wirelessly by default, thus this issue has continued forward into IoT implementations. When you transmit your data, you do not want everyone to be able to grab and use it, so the device must have some form of encryption to protect the data before it is transmitted. Of course data security is one of the largest concerns with use of the technology, especially in the medical field. If the data is tampered with or stolen from a Man-in-the-Middle attack it can cause all sort of problems for both the doctor and patient [9].

Most WSNs can be setup to use Symmetric Key Cryptography to encrypt their messages, but devices using the routing potential of the MANET can also use Public Key Cryptography [10]. Wireless sensors do not need to have the ability to decrypt encrypted messages unless specified. They only need the ability to pass encrypted messages transmitted through them.

Another possible method of keeping the data secure would be to create a network tunnel between the wireless sensor and the collector. Though the tunnel physically goes through many devices, it logically could connect the two together keeping any data transferred between the two secret. The drawback of tunneling is it would require extra power usage from the wireless sensor which would really only be feasible if the wireless sensors were directly hooked up to power and not running on batteries, such as in an IoT implementation.

Security concerns vary depending on the specific usage of the WSN and run the whole range of a minor concern (such as agriculture implementations) to extremely high (such as when used for health concerns). One of the largest security vulnerabilities IoT has is Denial of Service (DoS) attacks [11]. These attacks are effective against IoT technology because of the wireless sensors cannot send their data to the collector, then the whole IoT becomes useless. While for some IoT functions DoS attacks may not matter, it is very important when the data gathered is used in real time and the wireless sensors not reporting could endanger lives, such as in healthcare BAN uses or natural disaster alerts.

Another major threat is physically tampering with a wireless sensor. It may send false data or hacked into for the same effect [12]. A node sending false data could be worse than a node not sending data because it could leave those analyzing the data to believe everything is working when in fact it is not. These two security threats provide the biggest security downfalls to WSN technology.

We also do not currently have reliable solutions to DoS and physical tampering. Some wireless sensors have the ability to sense if they are being tampered with, but that capability utilizes the sensor's other resources and makes it less efficient. One can also increase the transceiver size or increase the amount of wireless sensors, neither of which is generally possible due to WSNs lack of resources. Overall these WSN problems also plague IoT systems and will need to be solved in the future for IoT technology to become more widely utilized.

IoT Security Concerns The IoT has taken the underlying WSN technology and advanced it, but with additional functionality comes additional security threats and concerns. An example would be the IoT ability to trigger specific actions based on proximity or GPS location [13]. For example, the IoT can

track a user's GPS location through their phone and trigger events, such as lights coming on or going off when the phone and user enters or leaves a room.

Another concern is considering what data the IoT stores [14]. If there are multiple users in a single area with sensors, the system has to be able to tell one from another to properly identify and use their preferences. It is convenient for a user to store a lot of metadata in their profile for the IoT system to use. While things like personal preferences seem obvious, additional data like credit card numbers is also common, to easily allow purchases online through IoT televisions or video game systems. The IoT allows for a number of ways for credit card data to be compromised, such as storing it or transmitting it without encryption. Having stolen credit card data linked to a name or even a social security number are a huge risk, but these types of data can be commonly stored in the IoT with little to no security. Privacy and keeping private data secure is one of the most important security issues with IoT.

Yet another common IoT security threat is giving automated command of appliances to the IoT controller. This use is convenient since the controller could check to make sure the oven is off once people are in bed or to ensure the shower is the perfect temperature. The biggest threat here however is that an outsider will be able to hack into an IoT network or just log into an unsecured one and take over command of these appliances. The examples of this threat are numerous, such as turning on an oven in the middle of the night and causing a fire; causing flooding from a shower, dishwasher, or washing machine; or a refrigerator's temperature being turned up and food spoiling. The threats from this type of attack are numerous and range from annoying to life threatening.

A lot of modern houses have home security systems which include door codes, intruder alarms, motion detectors, and possibly cameras. All of these can be considered wireless sensors and linked to the IoT for user control [15]. However, if an outsider is also able to access and control them they gain almost complete control over their target's home. Worse, it is generally in a way the user will not know allowing the attacker to spy through cameras, unlock doors for themselves, and shut down alarms that might go off.

So far the focus has been on using IoT in a home environment, however IoT is also able to connect to the Cloud to stretch its reach even further allowing its user to access and control anything attached to it from anywhere their phone has reception [16]. Utilizing IoT in this manner introduces many additional security issues due to the vulnerability of the Cloud and allows those looking for access a lot more ways to case problems. Cloud usage also expands the list of IoT vulnerable devices to other computer controlled devices outside the home, such as cars. The additional risks gained by connection the IoT framework to the cloud increase the security risks exponentially.

Medical uses of the IoT bring additional risks as affecting someone's medical conditions can be deadly. While being able to remotely access and analyze the data from a pacemaker or insulin pump is extremely useful, lack of security on these devices also make it extremely dangerous [17]. Also, accessing personal medical records through poorly secured or unsecured IoT connections creates

a big problem. Lack of IoT security and correct setup make all of these things possible and shows the dangers of the lack of IoT security even more clearly.

Finally, most modern IoT implementations have a Telnet vulnerability [18]. In some implementations Telnet is used because the sensors have a minimal amount of memory to keep costs down and Telnet does not encrypt so it keeps the overhead low. In other implementations SSH or other encrypted traffic is used, yet still leave the Telnet vulnerability in their systems for unknown reasons. Regardless of why this vulnerability is prevalent in most implementations, it is becoming a massive threat in the IoT world.

These threats represent only some of the possible problems substandard security can cause with the IoT. The threats caused both by the underlying WSN technology and the newer IoT are both pressing and valid. Proper setup and installation of the IoT technology is possible, but the variety and severity of the consequences for setting it up incorrectly seem to indicate an expert should be the one doing so and that is rarely the case. The default settings on IoT technology and the innate security risks need to be addressed by the manufacturers to help solve some of these problems. The alternative is that an IoT security program similar to anti-virus software needs to be developed and offered which can monitor and detect these possible issues in real time. One issue specifically with the IoT is that a lot of the devices have network capabilities added to them haphazardly without proper testing or review and no security is added to them.

3 Testing of IoT Security and Vulnerabilities

The biggest potential problem facing upcoming and emerging technologies is the security issues that threaten to shake the public's confidence in a product, removing any foundation it may have had before it has the chance to shine. The emerging IoT technology could have positive widespread implications for society, but if security is not a priority in its development then there will be risks. When this knowledge becomes public, any opportunity for the technology to take root and grow will be threatened.

3.1 Experiment Design

A primary IoT concern is that IoT's WSN roots have left potential problems and issues in the underlying product that could cause security issues. One example is that some modern IoT implementations have chosen to use the Telnet network port (port 23) to communicate between the sensors and controller over the Wi-Fi or home wireless network like it was used in WSN set ups.

The Telnet vulnerability means that an incorrect Telnet setup on a wireless network running IoT could leave the whole system vulnerable to intruders or other security issues. Also, if another exploit can be used on a wireless network allowing access to the port, everything connected to the IoT in the home would be compromised. To address this challenge, we will be simulating an IoT network

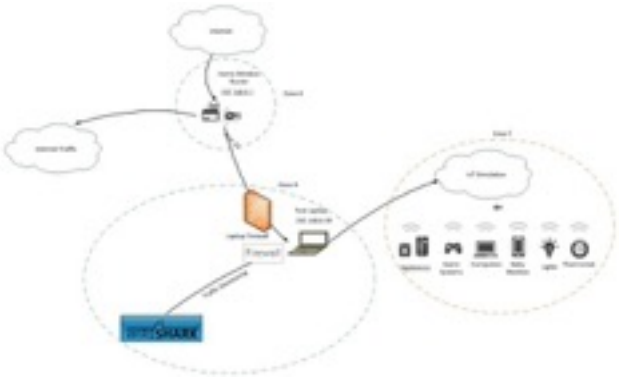

Fig. 1. Experiment Network

leaving this port open to attack and analyzing the attacks against it to attempt to compile metrics showing this known vulnerability.

The challenges of running and testing IoT technology and trying to exploit possible security faults are numerous. First since the technology is still in its infancy setting up the technology and doing actual testing is a challenge. The technology can be a challenge to find and expensive. All of the current implementations are custom work, there are not any beginner's kits you can buy and quickly install to test on. Finally, lack of comprehensive domain knowledge or best practices makes setup and troubleshooting of an IoT system a challenge. While there are plenty of articles on how the technology should theoretically work or conceptual ideas of how to implement it, there currently are not any widely available practical guides or solutions for how to make it work. The lack of practical information means that not only the basic setup is a challenge, but getting it to run in a stable enough way to try to test it for security problems becomes problematic.

To address these challenges in the experiment a laptop will be configured and set up a simulated IoT environment. Realgames has a Home I/O Smart Home Simulation, which will be used. The simulated environment will give a basic, but realistic simulation of an IoT home setup which will show the types of things accessible to both a legitimate user and to those infiltrating the network.

3.2 Security Test Environment Setup

The IoT simulation was set up on a home network and the laptop configured on the network like a honeypot where any intruders would be routed towards the IoT setup. The honeypot setup is important to point possible attackers towards the IoT setup as opposed to anything else on the network and so its security settings can be easily changed as necessary for the experiment.

As shown in Zone A in Figure 1 , the wireless network router was configured to take all the Telnet port 23 traffic and forward it to the experiment laptop

in Zone B. This includes forwarding traffic through the router's and laptop's firewalls, which were configured with rules to allow that traffic access.

The laptop in Zone B was a Dell Inspiron 15 running an AMD A6 Processor with 4GB of RAM and a 64-bit instance of Windows 10. It had the most recent Windows 10 patches and updates. The test was utilizing a system that is as modern and updated as possible and has as few known vulnerabilities or issues as possible so that the likelihood of those types of issues affecting the results is less likely. Additionally, a user account with normal privileges was be running and accessible the majority of the time to the attackers, while an administrator account was be running in parallel to track the activity on the laptop and the network. A few protected files were created and put into the "My Documents" folder of the user account to help determine the level of complexity of the attacks.

In addition, the experiment framework is running the AVG Zen Free antivirus and firewall, which is configured with a password to keep it from being turned off. However, there is a setting adjustable by any user. Wireshark is installed and configured on the administrator account to capture all the network traffic passing over the network and record the data for evaluation. Also HoneyBOT, which is a honeypot software, tracks what ports were being utilized. We additionally created a program that tracked what files were changed and when the system was running on the administrator account so that what files were accessed would be clear. Finally, a telnet server instance was set up on the laptop to allow those trying to access it to have a connection.

Zone C in Figure 1 shows the simulated IoT setup on the laptop. In the Realgames IoT simulation there are a number of devices. By default lights, doors, alarms, security system, and cameras are all usable and configurable. In addition the there is a companion program which allows for programming of additional devices. We configured a television, refrigerator, and home thermostat to add additional devices to the simulation. All the devices in the simulation are Wi-Fi devices that pass data over the wireless network which could be captured, changed, or stolen by an attacker.

3.3 Experiment Results and Evaluation

In the first phase of the experiment, we configured the environment with the IoT simulation fully running and confirmed that the network traffic was utilizing the honeypot correctly to attract anyone exploiting the network. We accessed the test environment from outside the network. This setup allowed the laptop to act as a vulnerable IoT device where we assume the security of the network has already been breached and that the vulnerable telnet port can be utilized to access other IoT and network devices.

The experiment ran for five days. Due to destructive attacks upon the IoT setup against the equipment, the environment was no longer able to continue the experiment. Once we opened up the security, we expected to need to broadcast out the vulnerable IP address, but within hours, both of the telnet server's sockets were being utilized as shown in Figure 2.

Fig. 2. Telnet Socket Utilization

During the five day period when the experiment was running, there were six documented attacks. Three were subtle attacks consisting of viewing the exploited machine for data, attempting to install subtle monitoring programs on it, or attempting to track when a user was or was not using the machine. The other three attacks were more direct and consisted of directly attempting to install viruses, attacking hardware wirelessly attached to the network through Wi-Fi and destroying the wireless router the experiment was being conducted through, as shown in Zone A in Figure 1 .

3.4 Results

We tracked a number of different things in the experiment. One important metric we captured was how frequently the Telnet server sockets were utilized through the HoneyBOT software that was running and tracking port connections. Figure 2 shows that the Telnet connections were nearly at 100% utilization throughout the whole experiment. The dips back to zero in Figure 2 reflect that each day we would reset the Telnet server's connections to allow new connections to utilize the sockets. Within hours of that reset, they would be reutilized.

Out of the ten possible connections over the five days, five of the connections didn't directly make any changes, or interfere with the system. We equate these with the three subtle attacks as they were either only watching, or making indirect or minor changes to the system. The only sign of these attacks was a hidden program which tracked when a user was on the machine was installed and created a text file on the vulnerable machine showing when the machine was being used. The creation of the text file was noticed by our file tracking software along with the port and traffic data we were capturing for the experiment. This enabled us to readily see the changes, but without those steps which wouldn't be a normal part of IoT security, these attacks would have been invisible.

The other three attacks were much more direct. Six attempts were made to install a keylogger on the vulnerable box during one attack. The installed antivirus stopped these attempts, which lead to them attempting to modify

the antivirus or uninstall it. In the other two direct attacks the attackers were able to access other wireless devices connected to the experiment's environment. The printer was accessed wirelessly through the vulnerable machine's Wi-Fi connection and it was power cycling constantly until it was rebooted and removed from the wireless network. In the final direct attack the attackers were able to access the wireless router's administration settings (they had been set to the defaults for this experiment) and make it completely inoperable.

We also tracked the changes to the dummy documents that had been placed to see how often they were accessed or changed using the file change tracking program installed. The files were all accessed each day shortly after resetting the Telnet sockets to allow new connections. None of the files were altered. The files with varying protection levels were still only accessed once, not multiple times, as was expected if hackers were attempting to brute force passwords.

3.5 Evaluation and Discussion

We logged the connections and the IP addresses of those connecting and attempted to trace them back through traditional means. Tracing the IP addresses lead back to Akamai Technologies in Massachusetts, which is a cloud provider. The probable scenario is that the attacks were launched from elsewhere and utilized that cloud access point as their last stop before attacking intentionally to mask the origin of the attacks. Without additional tools, it becomes nearly impossible to fully trace the origin of the attacks and while the data would prove interesting, it is not critical to the experiment's results.

Next we analyzed what changes were being made to the environment by the malicious attacks. We examined the data captured during the attacks from the honeypot, Wireshark, and the file change capture utility in addition to the Windows logs. Looking at the access record of the dummy files only being accessed once each day shows that the most likely scenario is that the automated bot accessed them when it connected, then when it couldn't break their passwords they were downloaded off the vulnerable machine for later analysis.

In addition through this data we determined that there were connections from six different IP addresses with one that reconnected each time the connections were reset and the others changing each time. The one that continued to connect daily was not responsible for any of the direct attacks. We surmise that those connections were utilizing the vulnerability to wait and watch for vulnerable data they could use or exploit. An example of this would be entering credit card information, which could then be taken and exploited without revealing their presence on the exploited machine. These sort of attacks are difficult to track due to their subtle nature.

The number of connections each day and the speed with which they connected to the vulnerable network leads us to believe that the connections were being made by bots which were scanning IP addresses and attempting to connect to vulnerable Telnet systems. This indicates that more attacks would have been likely had the experiment's environment allowed it. We also noted that once an IP had connected, they remained connected until we reset the server. This

implies that had the server not been reset they would have continued monitoring and attempting to exploit the vulnerable system for as long as possible.

When analyzing the antivirus after the experiment's conclusion, we found that some changes had been attempted to its settings. In anticipation of this a password had been set on some areas of the antivirus and while the attackers were able to make some modifications to it (such as setting its scan schedule to once a year), they were unable to disable it completely and leave the system vulnerable. This shows that after the initial connection was established by the botnet, control was most likely transferred to a human to launch additional and more complex attacks.

The direct attacks would be particularly effective against IoT devices and networks and that type of environment would have been vulnerable to the keylogger or installation of any other sort of malicious program. In addition the direct attacks did not only exploit the vulnerable box or the text environment, but also other devices without security connected through the Wi-Fi. These attacks emphasize how once an attacker has exploited a vulnerable IoT device it can utilize all its connections to other unprotected devices, gaining more influence over everything connected and attacking them in turn.

Our assessment of the complexity of the attacks derives from the assumption that botnets were being used for the initial discovery of our vulnerable network, and the evidence we found of attacks against the system. The more subtle attacks are of moderate complexity due to the understanding that waiting and listening will gain you more potentially useful information, and the subtle user tracking done. The more direct attacks had a much lower level of complexity, seeming only interested in causing as much direct damage to the environment as possible.

Overall, from our study we learned that there are still attackers actively looking to exploit vulnerable Telnet machines. There are bots scanning IP space for these vulnerable connections and ready to attempt to exploit them. There are enough different attackers doing this that we saw both subtle and direct attacks of varying complexity levels. In an actual IoT environment the security on the devices would not be enough to overcome the types of attacks we logged and detecting or recovering from them could be a challenge in an IoT environment. In summary, IoT systems retaining vulnerable Telnet connections are dangerous and a lot of damage can be done through them to vulnerable systems.

4 Threats to Validity

One potential threat is that to get the Telnet service running for the simulation we had to stand up a telnet server to allow outside hosts to connect. In an actual IoT environment this would not be necessary as the devices are configured to send and receive Telnet traffic. The server was only able to handle two Telnet connections at a time, which limited the potential of the experiment. We believe we still were able to show Telnet's vulnerabilities as both connections were utilized nearly one-hundred percent of the time, however more data could have been captured if this had not been limited.

A second concern is that the environment was set up and configured in a home environment. This was important to the experiment as this technology is primarily being produced for this environment. However, that does mean that uncontrolled or unexpected factors may have been at work in the environment. One example is that the wireless printer was not considered in the environment, yet was utilized by the attackers. While acknowledging that this makes some aspects of the environment potentially uncontrolled, it also allows us a more realistic look at how these attacks may occur in their expected environment.

Finally, in our experiment we decided to focus on the Telnet vulnerabilities in IoT as they can be directly traced back to the original WSN predecessor. While we acknowledge that only some IoT implementations utilize Telnet while others use SSH or other encrypted traffic, the majority of the concepts still apply. While we explore Telnet vulnerabilities in depth, most attacks of these types attack both Telnet and SSH and exploit the fact that in either implementation default usernames and passwords are left in the devices and exploitable [19].

5 Related Work

WSNs are not a new concept and a lot of papers have been written about them [8], [20], [21], [22], [23], [24], [25], [26], [27]. These papers often cover the basics of how a WSN works and give a lot of good data about how they can be used. However, they rarely look at security matters and those papers that do not take into account the evolution of the technology and give possible problems, exploits, or vulnerabilities currently applicable.

Most papers discussing WSNs do not cover IoT, and most IoT papers do not mention WSNs [1], [2], [5], [6], [7], [10], [11], [12], [13], [14], [18], [19]. However, there is an important link when considering the security of modern IoT systems since some of the vulnerabilities that were inherent in the old system and have continued to be a problem when inherited by the IoT when they could have been fixed. Understanding the history of the IoT and how it is evolved is essential to getting a full grasp on the security problems still in the system.

Most of the literature on the IoT discusses the positive points of it and how convenient it is without discussing the security aspects [3], [4], [14]. Even those that do bring up the topic of security usually focus on a single aspect of that problem, instead of addressing the whole scope. There are a number of security issues in the IoT and failing to fix or address a single one still leaves the system vulnerable to data being stolen or exploited.

Finally, privacy must be considered. While information regarding personal information and the dangers of it being stolen are becoming more prevalent, few of these specifically address storing this type of information on your personal network where the IoT could access it [6], [7], [15], [16], [17]. Some of the devices on the Internet of Things, particularly those with cameras, provide ability to put those using them and their personal data at risk. Devices that hold and store personal information that can be used to get more information or access other accounts must be better protected in this sort of environment.

In addition, many large technology companies are beginning to slowly put information out about their own IoT approaches, guidelines, and products. The additional research and best practices produced by these companies could give a lot of extra information on how the field of IoT will continue to develop and show additional security information and vulnerabilities not considered here.

6 Conclusions and Future Work

IoT has grown from the WSN technology and has been incorporated into many more modern devices, sensors and network concepts to enable a technological system which provides endless possibilities for the technology in the future. However, due to the reliance on previous technologies, there are innate security issues to be addressed in the new technology. These security flaws must be a main concern in the future of IoT technology.

This research shows that there are known security issues and holes in the current IoT technology. Identification and education is the first step in solving any problem. The data gathered in the experiment shows the damage that can be done through a known Telnet vulnerability. IoT needs to look back at the vulnerabilities it inherited from the WSN technology and fix those problems before continuing to move forward. The potential security risks that comes with that vulnerability are being demonstrated on a daily basis across the world through attacks on various IoT networks.

We learned that having a Telnet vulnerability grants an attacker a variety of ways to exploit data and wireless systems. Once the outer shell of security has been penetrated, an attacker has access to everything else inside the IoT environment including other devices connected through the Wi-Fi network. With the lack of security on IoT networks, attackers who find vulnerable systemscan quickly exploit that device(s), gain more access, or install spying programs to capture personal data.

In the future, we will look into other vulnerabilities in IoT environments, especially those inherited from backbone systems such as WSNs. We will also consider automated correction mechanizms for when IoT devices attomatically detect intrusion and analyze automated intrustion detection techniques.

References

1. Kolias, C., Kambourakis, G., Stavrou, A., Voas, J.: Ddos in the iot: Mirai and other botnets. Computer **50**(7) (2017) 80–84
2. Pa, Y.M.P., Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T., Rossow, C.: Iotpot: A novel honeypot for revealing current iot threats. Journal of Information Processing **24**(3) (2016) 522–533
3. Atzori, L., Iera, A., Morabito, G.: The internet of things: A survey. Computer networks **54**(15) (2010) 2787–2805
4. Misra, G., Kumar, V., Agarwal, A., Agarwal, K.: Internet of things (iot)–a technological analysis and survey on vision, concepts, challenges, innovation directions,

technologies, and applications (an upcoming or future generation computer communication system technology). American Journal of Electrical and Electronic Engineering **4**(1) (2016) 23–32
5. Jing, Q., Vasilakos, A.V., Wan, J., Lu, J., Qiu, D.: Security of the internet of things: perspectives and challenges. Wireless Networks **20**(8) (2014) 2481–2501
6. Weber, R.H.: Internet of things–new security and privacy challenges. Computer law & security review **26**(1) (2010) 23–30
7. Roman, R., Zhou, J., Lopez, J.: On the features and challenges of security and privacy in distributed internet of things. Computer Networks **57**(10) (2013) 2266–2279
8. López, T.S., Kim, D., Canepa, G.H., Koumadi, K.: Integrating wireless sensors and rfid tags into energy-efficient and dynamic context networks. The Computer Journal **52**(2) (2008) 240–267
9. Roman, R., Najera, P., Lopez, J.: Securing the internet of things. Computer **44**(9) (2011) 51–58
10. Gan, G., Lu, Z., Jiang, J.: Internet of things security analysis. In: Internet Technology and Applications (iTAP), 2011 International Conference on, IEEE (2011) 1–4
11. Suo, H., Wan, J., Zou, C., Liu, J.: Security in the internet of things: a review. In: Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on. Volume 3., IEEE (2012) 648–651
12. Kolias, C., Stavrou, A., Voas, J., Bojanova, I., Kuhn, R.: Learning internet-of-things security" hands-on". IEEE Security & Privacy **14**(1) (2016) 37–46
13. Zhou, L., Chao, H.C.: Multimedia traffic security architecture for the internet of things. IEEE Network **25**(3) (2011)
14. Tan, L., Wang, N.: Future internet: The internet of things. In: Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on. Volume 5., IEEE (2010) V5–376
15. Airehrour, D., Gutierrez, J., Ray, S.K.: Secure routing for internet of things: A survey. Journal of Network and Computer Applications **66** (2016) 198–213
16. Botta, A., De Donato, W., Persico, V., Pescapé, A.: Integration of cloud computing and internet of things: a survey. Future Generation Computer Systems **56** (2016) 684–700
17. Moosavi, S.R., Gia, T.N., Nigussie, E., Rahmani, A.M., Virtanen, S., Tenhunen, H., Isoaho, J.: End-to-end security scheme for mobility enabled healthcare internet of things. Future Generation Computer Systems **64** (2016) 108–124
18. Bertino, E., Islam, N.: Botnets and internet of things security. Computer **50**(2) (2017) 76–79
19. Angrishi, K.: Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets. arXiv preprint arXiv:1702.03681 (2017)
20. Pathan, A.S.K., Lee, H.W., Hong, C.S.: Security in wireless sensor networks: issues and challenges. In: 2006 8th International Conference Advanced Communication Technology. Volume 2. (Feb 2006) 6 pp.–1048
21. Cook, D.J., Das, S.K.: How smart are our environments? an updated look at the state of the art. Pervasive and mobile computing **3**(2) (2007) 53–73
22. Werner-Allen, G., Lorincz, K., Ruiz, M., Marcillo, O., Johnson, J., Lees, J., Welsh, M.: Deploying a wireless sensor network on an active volcano. IEEE internet computing **10**(2) (2006) 18–25
23. Nittel, S.: A survey of geosensor networks: Advances in dynamic environmental monitoring. Sensors **9**(7) (2009) 5664–5678

24. Khamukhin, A.A., Bertoldo, S.: Spectral analysis of forest fire noise for early detection using wireless sensor networks. In: Control and Communications (SIBCON), 2016 International Siberian Conference on, IEEE (2016) 1–4
25. Lai, X., Liu, Q., Wei, X., Wang, W., Zhou, G., Han, G.: A survey of body sensor networks. Sensors **13**(5) (2013) 5406–5447
26. Zulkifli, C.Z., Noor, N.M., Zamzuri, A., Ali, M., Semunab, S.N.: Utilizing active rfid on wireless sensor network platforms for production monitoring. Jurnal TeknologiI **78**(2) (2016) 63–72
27. Kumar, P., Lee, H.J.: Security issues in healthcare applications using wireless medical sensor networks: A survey. Sensors **12**(1) (2011) 55–91