5-25-2018

Internet of Things Security: Ongoing Threats and Proposed Solutions

Samuel Strba
Portland State University

Internet of Things Security: Ongoing Threats and Proposed Solutions

by

Samuel Strba

An undergraduate honors thesis submitted in partial fulfillment of the

requirements for the degree of

Bachelor of Science

in

University Honors

and

Computer Science

Thesis Adviser

Charles Wright, Ph.D

Portland State University

2018

Table of Contents

Abstract

This paper will describe the security vulnerabilities posed by Internet of Things (IoT) devices, and potential solutions to alleviate these vulnerabilities. It will describe how IoT devices work, and how they differ from conventional devices such as personal computers in utilizing the Internet. Then the paper will describe the security threats associated with IoT devices, and how a lack of proper security in IoT devices exacerbates this problem. Finally, it will describe proposed solutions to improve IoT device security. IoT devices are seeing increasing deployment in the field, and the continued growth of the Internet of Things along with the lack of security in such devices continues to raise concerns of how security is and should be handled in these devices. The Mirai botnet attacks of 2016 highlighted the potential for IoT devices to be hijacked and be exploited for malicious purposes such as distributed denial of service (DDoS) attacks. Solutions such as router security and ethernet firewalls are proposed to protect vulnerable devices in the absence of manufacturer intervention. While cybersecurity researchers will be in constant battle against the latest threats and malwares, they must continue to combat these issues to uphold Internet security.

Introduction

A trend in modern technology is the increasing deployment of Internet of Things, or IoT. Devices that are categorized under the IoT umbrella include electronic devices such as computers, smartphones, appliances, televisions, traffic control systems, and connected cars. These devices use an Internet connection to transfer data, as well as to receive software and firmware updates. The term, "Internet of Things," first appeared in 1999 in reference to supply chain management, but in the past decade has been applied to home electronics, healthcare, utilities, and transportation[8]. Internet of Things is sometimes also referred to as "Internet of Everything," or IoE[17], and mainly distinguishes itself apart from conventional use of Internet connectivity by computers for information sharing and media streaming. Rather, Internet of Things devices use the Internet for specialized functions such as data collection and device firmware updates.

Statistics show rapid increase in the number of IoT devices in use. In 2004, about a half billion devices used an Internet connection, and personal computers were the primary device that connected to the Internet[17]. In 2010, about 2 billion devices had Internet connectivity, mainly computers and smartphones[17]. Since then, there has been a massive expansion in the number of Internet-connected devices. 2014 statistics show that over 8 billion IoT devices were in use, including televisions, wearables, connected cars, tablets, and general IoT devices such as home appliances and monitoring systems. Current statistics are varied, but indicate that there are anywhere between 18 billion[17] to 35 billion[13] IoT devices connected to the Internet, and that number expected to continue increasing as more companies implement IoT functionality in their

products. Trends in the increase of Internet-connected devices show that personal computers are experiencing a more modest growth when compared to devices like smartphones, tablets, and Internet-connected accessories and appliances[17]. The increase in the number of Internet users, high speed networks, and decreasing hardware costs all facilitate the growth of the Internet of Things[17].

One technicality in Internet of Things is the categorization of electronics as IoT devices. Strictly speaking, IoT could apply to any device that has Internet connectivity. On one end of the spectrum, devices such as desktop computers, laptops, tablets, and smartphones utilize complex hardware and software systems to perform a multitude of tasks such as word processing, mathematical computation, audio-video processing, online communication, and media streaming. On the other end, devices such as smart appliances and light bulbs may only use the Internet for simple purposes such as allowing users to operate them remotely, enabling communication with other devices on a network, and collecting data and usage analytics. Devices of any complexity that use the Internet in any way could theoretically be considered IoT devices. Therefore, this paper will focus on consumer electronics with IoT functionality such as home appliances, wearable accessories, and remote monitoring systems. These are devices that use the Internet for specific operations and are otherwise not traditionally associated with Internet connectivity.

Compared to devices like personal computers, tablets, and smartphones that have highly sophisticated software and firmware, IoT devices are typically simpler, do not use complex systems-on-chips, do not use cutting-edge technology, and are much cheaper to develop[17]. IoT devices use wireless protocols such as Wi-Fi, Bluetooth, 4G-LTE, radio frequency identification (RFID), and embedded sensors[8]. Not all IoT devices connect directly to the Internet, but may

rather use a short-range protocol like Bluetooth to connect to an intermediary device such as a smartphone or a wireless hub connected to a router, which has Internet connectivity, that can transfer data between the Internet-connected device. This is the case with devices such as RFID tags or FitBit wristbands. Other devices such as smart televisions may use Wi-Fi to connect to the Internet and prompt the user for the network's password to authenticate the connection. There are many reasons companies are increasingly pushing for IoT functionality in their products. Companies can collect user data through the devices such as the ways users interact with their products, the customers' interests, and their lifestyle habits to improve their advertising to the customers and learn what users want from their products[8]. Devices such as smart light bulbs can connect to a home network and be controlled remotely by a user through a smartphone application designed for this purpose. If the product designers become aware of a major firmware problem that interferes with the functionality of the product, they could attempt to release an update to the product that could fix the issue without requiring more costly hardware revisions. IoT functionality therefore makes it easier for companies to tailor advertisements to customers and can reduce the costs in product revisions, if modifications that would normally require the product to be redesigned and redistributed can instead be implemented through firmware updates.

Many people express concern regarding security in the increasing development and deployment of IoT devices. A part of the issue is companies competing with each other for product features, and security as a result is given much less priority[2]. The developers may not take the time to release security patches if their main concern is to entice consumers with features that products their competitors do not have. Complex devices such as computers and

smartphones generally have much stronger security. Operating systems like Microsoft Windows, Mac OS, iOS, Android, and most Linux-based operating system distributions receive frequent updates and patches to address security flaws. These operating systems often have built-in antiviruses and firewalls, and support a wide variety of aftermarket security solutions that the consumers can install. The developers of these operating systems consider security much more important since they often make extensive use of the Internet for a variety of applications and because users could unintentionally compromise them with malware mistakenly downloaded from the Internet or from an infected flash drive. Therefore strong security is needed to keep consumers safe from malware when surfing the Internet or from identity theft when entering sensitive information. Installing an antivirus or a firewall on an IoT device would prove difficult, if not impossible, without considerable revisions to the product design, due to the minimal hardware and firmware the products use to function as they are designed to. The consequences of the weak security found in IoT devices will be discussed in the next section.

Security Threats

There are many reasons IoT devices are likely to be be hacked. As previously mentioned, IoT devices have a reputation for having inferior security compared to conventional computers that utilize the Internet. A 2014 security report by HP found that there were an average of 25 vulnerabilities per IoT device, 80 percent of devices did not use complex passwords (e.g. “admin” or “password”), if at all, 70 percent did not encrypt data communications, and 60 percent of devices had vulnerable firmware or user interfaces[3]. Most of them do not give users

the ability to install antiviruses or firewalls, unlike personal computers. This is not to say that the consumers do not bear any responsibility for the insecurity of IoT devices. Users may keep the default passwords on their devices or set up otherwise weak passwords, and may neglect installing updates when they are available. The vulnerability of IoT devices makes them easy targets for hackers.

Bertino and Islam explain several common vulnerabilities characteristic of many IoT devices. The devices may have an insecure online interface, due to an inability to change usernames and passwords or having weak credentials to begin with[3] This can result in privilege escalation to hackers who seek to gain control of these devices[3]. Devices may lack security mechanisms which can make them vulnerable to Distributed Denial of Service (DDoS) attacks, buffer overflowing, and SQL injections[3]. IoT devices often collect personal user information such as locations and as credit card numbers, which may not be encrypted or protected otherwise, and may be compromised if a security breach occurs[3]. Benson and Chandrasekaran describe similar vulnerabilities commonly found in IoT devices. Devices may not receive frequent updates, if any, and may lack a user interface, which can prevent the user from setting a username and password, or from being alerted of updates or suspicious activity[2]. Additionally, the heterogeneity of IoT devices and the tendency for manufacturers to use generic software components across a wide range of products can make devices more vulnerable[9]. A case study by Yogeesh Seralathan et al. investigated security flaws in an IP camera, and found vulnerabilities such as unencrypted data transfer and account credentials, and that the RSTP (real time streaming protocol) URL used to stream data was brute forcible[15]. Developers of basic IoT devices often do not consider security in the product design, and the rudimentary design of the

devices often makes it difficult, even impossible, to install security mechanisms such as an antivirus or a firewall[2]. Additionally, there is a lack of regulation in the design guidelines of IoT devices that concern security, and few proposals exist to standardize security as part of the design of IoT devices[2].

The Mirai botnet attacks of October 2016 highlight the potential for the insecurity of IoT devices to be exploited for malicious purposes. Hackers used the Mirai malware to assemble a botnet comprised of IoT devices and conduct DDoS attacks. A DDoS attack aims to overload a victim server's bandwidth with junk data packets and automated requests so that web service is denied to legitimate users, sometimes even crashing the website. Hackers use botnets comprised of thousands of "zombie" bots that are infected with malware that can flood the target with excessive network traffic, disrupting its service. The Mirai botnet comprised over half a million IoT devices and generated over 620 gigabits per second of traffic[10]. Notable targets included the website of cybersecurity journalist Brian Krebs, French web host OVH, and Internet performance and domain service Dyn,[10] resulting in downtime for many popular websites such as Twitter, Netflix, Reddit, and GitHub for several hours[11]. Whereas most botnets have formed due to unsuspecting computer users downloading malware onto their computers or smartphones that connects it to the botnet, Mirai gained notoriety for targeting IoT devices and infecting them without the user knowing about it.

Mirai primarily targets Linux-based IoT devices that use hardware architectures such as ARM, MIPS, SPARC, and Intel x86[10]. In particular, devices such as DVRs, webcams, and routers that run BusyBox are vulnerable to Mirai[11]. Users who have a device infected with the Mirai malware would not even know their device was infected, unlike personal computers which

would often experience slowdown and display erratic behavior and antivirus warnings indicating a possible malware infection. The hacker uses a Command and Control (C&C) server to control the botnet, a loader server to install the malware onto target devices, and a report server to view the bots that are online[10]. When the attacker or an infected bot launches Mirai, the program randomly scans the IP space for victim devices to install to[10]. For each IP address, the program probes Telnet ports 23 and 2323 to check for a username and password prompt, indicating that there is a device connected to that IP address that could potentially be exploited[10]. Then the program attempts to log in to that device using a list of 62 username and password combinations[10]. If successful, Mirai now has access to the target device and can execute shell commands, as well as access the device characteristics such as IP address, port, and login credentials and relay it back to the report server on port 48101[10]. Mirai uses Linux shell commands such as wget, which makes Linux-based devices vulnerable to the malware[10]. The program scans the hardware architecture and if it's compatible with Mirai, then it executes commands on the target device to download the Mirai binary from the loader server and execute the program code. The target device is now part of the Mirai botnet, and can connect to the C&C server and receive commands coming from it, listen on TCP port 21, and scan the IP space for more devices to infect[10]. The attacker can then command the botnet through the C&C server to launch DDoS attacks on whatever targets they specify, based on the IP addresses of the targets, using HTTP floods for application-layer attacks[10]. Surprisingly, the malware on the infected IoT devices only exists in random-access memory, and is erased when the user reboots the device, although it could be hacked again if another Mirai-infected bot breaks into the device and installs the malware again[10].

Mirai continues to be modified by the blackhat hacking community for illicit purposes, following the release of its source code[11]. Many variants of the malware exist and continue to be deployed today[11]. Attacks facilitated by Mirai and its variants mainly use hit-and-run tactics against smaller targets such as residential IP addresses and online game servers[10]. A US college was hit with a 54 hour app-layer DDoS attack in February 2017 by a Mirai variant[10]. Internet security company Kaspersky discovered a Windows-based spreader for Mirai when over 900 thousand customers of Deutsche Telekom were denied Internet access and their routers were found to have this Mirai variant[10]. Another variant of Mirai was found to have a Bitcoin miner, which would attempt to use the device's resources to "mine" the cryptocurrency and generate virtual revenue for the developers[10]. There exists another IoT malware called Bashlight, which has a similar operation as Mirai, and has been believed to control over half a million IoT devices in a botnet[10]. Other IoT malwares that enslave Linux-based IoT devices include PNScan, Remaiten, and LuaBot, all of which created botnets that carried out application-layer DDoS attacks[10].

IoT botnets can also be commanded to perform other tasks besides carrying out DDoS attacks. Linux/Moose is an IoT botnet that was investigated by the security researchers at ESET, and has been used to conduct social media fraud (SMF)[12]. SMF is an attempt to artificially inflate an account's fanbase by generating likes, follows, and views on social media networks such as Facebook, Twitter, and Youtube[12]. Hackers can use botnets to generate fake accounts, which artificially inflate an account's popularity by using automated scripts to add views, likes, and follows to the account's content[12]. Fraudulent actors can use SMF to make their service seem reputable by inflating the popularity of their associated social media pages, when in fact the

service may be fraudulent. Hackers can also use the botnets for spam propagation and cryptocurrency mining in addition to social media fraud, and can perform them with using IoT botnets as well as botnets made up of personal computers and smartphones.

Other IoT threats have been discovered that do not involve botnets. The Fiat-Chrysler hack of 2014 resulted in 1.4 million vehicle recalls when cybersecurity researchers discovered a wireless network interface vulnerability that a potential hacker could use to disable an Internet-connected Jeep Cherokee while driving[1]. Similarly, a 2015 reports discovered inadequate security in the ConnectedDrive functionality of BMW cars[1]. The US Federal Drugs Administration (FDA) stopped an infusion pump in 2015 due to a security breach, because they discovered that the pumps could potentially be remotely accessed through a hospital's network, although they didn't find any cases of hackers hijacking the pumps[1]. A case study on the August Smart Lock revealed vulnerabilities hackers could exploit to open the lock[16]. While public fears arise from the possibility of critical Internet-connected devices being hijacked, in practice these types of vulnerabilities are more often discovered by security researchers than exploited by hackers with malicious purposes.

This section has described the ways in which IoT devices have been exploited for malicious purposes. It described how IoT devices have been assembled into botnets that have perpetrated DDoS attacks as well as social media fraud and spam propagation. It has also described vulnerabilities in critical devices that hackers could potentially exploit. In reality, these types of vulnerabilities are not exploited by hackers as often as the public fears they are. The next section will describe several proposed methods to improve IoT security.

Proposed Solutions

This section of the paper will focus on several solutions proposed to improve the security of IoT devices. An issue with the establishment of IoT security is the lack of coordinated protocols for product manufacturers, Internet service providers, and computer security researchers to implement in IoT. Bertino and Islam describe several techniques US Computer Emergency Readiness Team (US-CERT) suggest that product developers implement to prevent IoT devices from being exploited, as a response to the Mirai botnet attacks. They suggest using strong, user-defined passwords over weak and generic credentials, and to update IoT devices regularly with security patches[3]. Other suggestions include monitoring TCP ports 23 and 2323, to check for attempts to use Telnet to gain unauthorized control, and to monitor port 48101 for suspicious traffic since infected devices may use this port to spread malware[3]. US-CERT also recommends that consumers only buy devices from reputable companies and understand the capabilities of the devices[3]. Many others suggest that manufacturers are responsible for implementing data encryption systems, strong credentials, and built-in security mechanisms to protect the devices from hackers and malwares.

The issue with this approach is that many companies do not consider security to be a priority in the design of their products. Rather, they focus on adding features that consumers may find attractive. For companies to implement their own security systems would increase the costs of production of the devices, which would in turn increase the product cost to the consumer. Even modifying the product design to support built-in third party security features would

increase the cost of production. Therefore, dedicated external security systems may be implemented to assist product designers in securing IoT devices.

The Internet security provider Bitdefender offers a product called the Bitdefender Box. This device is marketed as an Ethernet-based antivirus and firewall that connects directly to the home network[4]. The user would plug their router to the Bitdefender Box via Ethernet cable, and the device would scan and monitor the network traffic. Bitdefender Box offers vulnerability assessment to detect network security flaws, exploitation prevention to block attempts to exploit vulnerabilities in connected devices, local device security to protect connected computers, smartphones, and tablets in place of a locally installed antivirus, as well as anomaly detection, brute force detection, and data protection[4]. The device uses its own CPU and RAM to secure the network whilst maintaining the speed of the Internet connection[4]. A possible way to standardize this type of solution would be to manufacture routers with built-in antivirus functionality. That way they can protect potentially insecure IoT devices that are connected to them, and prevent them from being exploited. Developers of security solutions like these would be responsible for keeping them up to date with the latest malware definitions and detection heuristics. However it would be unreasonable to encourage consumers to buy the Bitdefender Box for themselves, or a router with a built-in antivirus, since the average consumer may not be aware of the implications of installing the device in regards to the security so as to justify spending money on the device and paying the yearly subscription fees. A possibility is for Internet service providers to incorporate a network-based antivirus system, like Bitdefender Box, as part of the Internet package, to minimal cost to the consumer. Further development in network traffic security can improve security and performance and lower costs.

Hadar et al. describe a lightweight cloud-based vulnerability mitigation framework that can be used to protect IoT devices. The framework consists of the cloud service and the individual client devices, where the cloud crawls for vulnerabilities, creates the mitigations, and distributes them to the clients[9]. The client appliance would be connected to the vulnerable IoT device, through ethernet or wireless connection[9]. It would communicate data between the IoT device and the Internet, receive updates, and execute vulnerability mitigation policies[9]. The providers of the mitigation framework would maintain the malware definitions and the mitigations for them, leveraging the public database Common Vulnerabilities and Exposures (CVE) to obtain the vulnerabilities[9]. Hadar demonstrates the functionality of installing Mirai on an IP camera that is connected to a Raspberry Pi that is running the mitigation program, which is plugged into the router. On the first attempt to install Mirai on the camera, the malware is installed on the camera and the appliance obtains the mitigation policy[9]. Hadar then factory resets the IP camera to clear the malware. On the second attempt to install the malware, the appliance blocks the malware from being installed onto the camera. Unlike Bitdefender Box, this appliance works by blacklisting known malwares from being installed onto the IoT devices they are connected to; it is more lightweight and cost effective compared to similar appliances. Still, the developers who maintain the framework are responsible to ensure that the mitigation policies are constantly curated and the clients are kept up to date with the policies. After all, devices like these would be useless if the developers stopped maintaining them, since they would not be able to defend against new forms of malwares if the developers don't create definitions for them. The vulnerability mitigation framework could be implemented in IoT devices by having the client

appliance built-in to the device, which would be kept up to date by the cloud service, and it would present minimal cost to the manufacturers.

El-Affendi et al. describe a device virtualization solution for ZigBee devices that hides the resource constrained devices (RCD's) behind software-based virtual resources (VR's), which can leverage security protocols and algorithms to protect devices[7]. RCD's are replaced with virtual components on parent gateways, and can act as virtual machines that communicate with each other through the virtual network[7]. The parent gateways provide the virtualization software, which hides the physical IoT devices while being able to perform their normal tasks, as well as other services such as firewalls[7]. The elliptic curve Diffie Hellman encryption algorithm is used to secure communication between the devices and the Internet and certificate-based authentication is used in joining devices to the virtual network[7]. This type of solution works with IoT devices with minimal hardware such as smart appliances and light bulbs, since they usually don't have the computational resources to block attacks on their own. Rather than connect directly to the home network, these devices can connect to a virtual network that can use authentication methods secure the devices and continue to allow them to communicate with each other, blocking unauthorized access in the process. Internet service providers could incorporate the virtualization infrastructure in the Internet plans to provide the virtual network for the connected devices, in addition to the direct Internet connection.

Chowhardy et al. suggest implementing physical layer security, by protecting the sensors the devices use such as cameras, microphones, and wireless transmitters and receivers. Security measures on the physical level are meant to protect user privacy and prevent hackers from tampering with these sensors. Some attacks hackers could perform on the sensors could include

radio frequency interference on RFID systems or node tampering in wireless sensor networks[5]. One technique to prevent hackers from tampering with the hardware would be to put touch sensors near the circuit boards, so if a hacker tries to physically break into a device, then the touch sensors would activate and disconnect the device from the network[5]. This would prevent hackers from tampering with the circuit to gain access to a network or a device. Additionally, hash functions can be used for the device and the network to mutually authenticate each other, preventing a hacker from accessing the network through a hacked device[5]. Physical layer security could however be more costly since the manufacturers themselves would have to implement it in the products.

Schinianakis describes several cryptographic techniques that could be implemented in IoT. Data encryption is essential for providing more secure data storage and transmission, and many techniques exist to encrypt and decrypt data. Schinianakis argues that IoT devices should use lightweight cryptography[14], since these devices do not use complex hardware and should therefore be capable of running simple encryption algorithms. Ciphers such as PRESENT, Midori, ChaCha20, Diffie-Hellman protocol, and RSA are suggested for use in IoT[14]. Specifically, Schinianakis describe elliptic curve cryptography (ECC) as a highly efficient public-key encryption technique that can be used in 8 bit or 32 bit microcontrollers used in these devices[14]. ECC is considered efficient because it has more strength per bit of encryption and a smaller key size compared to RSA or Diffie-Hellman[14], and thus requires little cost to the manufacturer of the device to design hardware that can run using ECC. It is still the obligation of the manufacturers to ensure that the user data is kept in a securely encrypted form, and any transmissions of the data are also encrypted. Encryption schemes could still be broken by a

determined hacker but they offer much stronger security than leaving the data in an unencrypted, human-readable format.

Many others propose solutions for device security. Some argue that the manufacturers of IoT devices themselves should be responsible for ensuring that they are secure and be able to fend off Internet-based attacks. Others argue that third party solutions can improve security without much cost to the device manufacturers. The security of IoT devices is unlikely to match the security of operating systems such as Windows or Mac OS without a considerable cost to the product manufacturers. These operating systems represent years of development, updates, and patches, and require strong security to protect users from malware they could easily obtain while browsing the Internet. There also needs to be a coordinated movement towards the implementation of proper IoT device security. Device manufacturers can consolidate aftermarket solutions to improve device security in a way that is economical to both the company and to the end users.

Conclusion

This paper has described the the Internet of Things landscape and how it is present in our everyday lives. It has explained how IoT devices use the Internet in their operation, and how they differ from devices such as personal computers and tablets. Threats to IoT devices have been described, and examples of attacks such as the Mirai botnet that exploited IoT devices have been discussed. Finally, this paper has described several proposals to improve IoT security.

IoT security continues to be a concern in discourses relating to Internet security. While the Internet of Things promises an innovative platform for product design and development, many fear that it will bring opportunities for malicious actors to exploit vulnerabilities and compromise Internet security. Computer security however has been a concern long before the Internet of Things was ever conceived. Hackers have designed viruses such as the Melissa worm or the ILOVEYOU virus that targeted Windows computers, and have conducted DDoS attacks using botnets comprised of conventional PCs. Even systems that use passwords can be breached by a determined hacker if they use brute-force tactics involving generating every possible permutation of characters, numbers, and symbols to crack the password[6], prompting many developers to encourage the use of two-factor authentication to add another layer of security. Malicious hackers will continue to find ways to exploit security vulnerabilities and disrupt computer systems and Internet services. The nature of cybercrime is constantly evolving, with different types of malwares being created and exploiting different vulnerabilities in hardware and software systems. It is the responsibility of security researchers to continue to combat the latest threats on the Internet and for developers and users to keep their software and firmware up to date. While it will always be a battle to defend Internet security against constantly evolving malwares and attack vectors, it is necessary for developers to be vigilant and consumers to exercise caution and proper judgement to make the Internet a safer place.

References

[1] Asplund, Mikael, & Simin Nadjm-Tehrani. "Attitudes and Perceptions of IoT Security in Critical Societal Services." *IEEE Access*, vol 4, pp. 2130-2138, Apr. 2016.

[2] Benson, Theophilius, & Balakrishnan Chandrasekaran. "Sounding the Bell for Improving Internet (of Things) Security," in *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, ACM, 2017, pp. 77-82.

[3] Bertino, Elisa, & Nayeem Islam. "Botnets and Internet of Things Security." *Computer*, vol. 50, no. 2, pp. 76-79, Feb. 2017.

[4] *Bitdefender Box*. Accessed: Mar. 18, 2018. [Online]. Available: https://www.bitdefender.com/box/

[5] Chowdhardy, Shivani, et al. "Security solutions for physical layer of IoT," in *2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)*, IEEE, 2017, pp. 579-583.

[6] Crossman, Matthew A., & Hong Liu. "Study of authentication with IoT testbed," in *2015 IEEE International Symposium on Technologies for Homeland Security*, IEEE, 2015, pp. 1-7.

[7] ElAffendi, M. A., and A Lateef Alamudy. "Could Virtualization be the Ultimate Solution for IoT Resource Constrained Devices Problem? A Multilevel Security Framework Based on Device Virtualization," in *2017 International Conference on Computer and Applications*, IEEE, 2017, pp. 232-237.

[8] Gubbi, Jayavardhana, et al. "Internet of Things (IoT): A vision, architectural elements, and future directions." *Future Generation Computer Systems*, vol. 29, no. 7, pp 1645-1660, September 2013.

[9] Hadar, Noy, Shachar Siboni, and Yuval Elovici. "A Lightweight Vulnerability Mitigation Framework for IoT Devices," in *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, ACM, 2017, pp. 71-75.

[10] Kambourakis, Georgios, et al. "The Mirai Botnet and the IoT Zombie Armies," in *2017*

IEEE Military Communications Conference, IEEE, 2017, pp 267-272.

[11] Kolias, Constantinos, et al. "DDoS in the IoT: Mirai and Other Botnets." *Computer*, vol. 50, no. 7, pp, 80-84, July 2017.

[12] Paquet-Clouston, Masarah, et al. "Can We Trust Social Media Data? Social Network Manipulation by an IoT Botnet," in *Proceedings of the 8th International Conference on Social Media & Society*, ACM, 2017, pp. 1-9.

[13] Radovan, M., & B. Golub. "Trends in IoT Security," in *40th International Convention on Information and Communication Technology, Electronics and Microelectronics*, IEEE, 2017, pp. 1302-1308.

[14] Schinianakis, Dimitris. "Alternative Security Options in the 5G and IoT Era." *IEEE Circuits and Systems Magazine*, vol. 17, no 4, pp. 6-28, November 2017.

[15] Seralathan, Yogeesh, et al. "IoT security vulnerability: A case study of a Web camera," in *2018 20th International Conference on Advanced Communication Technology*, IEEE, 2018, pp. 172-177.

[16] Ye, Mengmei, et al. "Security analysis of Internet-of-Things: A case study of August Smart Lock," in *2017 IEEE Conference on Computer Communications Workshops*, IEEE, 2017, pp 499-504.

[17] Yeo, Kiat Seng, et al. "Internet of Things: Trends, Challenges, and Applications," in *2014 International Symposium on Integrated Circuits*, IEEE, 2014, pp. 568-571.