CYBERSECURITY OF INTERNET OF THINGS DEVICE RELATED TO NATIONAL SECURITY

Shubham Kumari Sheela[1],Ttrapti Saxena[2], Ritesh Sadiwala[3]
[1]*MTech Scholar*, [2]*Assistant Professor*, [3]*Associate Proffesor*
[1]*Department of Electronics and Communication Engineering, Bhabha College Of Engineering, Bhopal, India*
[2]*Department of Electronics and Communication Engineering, Bhabha College Of Engineering, Bhopal, India*
[3]*Department of Electronics and Communication Engineering, Bhabha College Of Engineering, Bhopal, India*

charushila9418gmail.com1 traptisaxena3@gmail.com2 ritesh14ci@gmail.com3

Abstract — **The Internet of Things (IoT) is a complex system of electronic devices interconnected through the Internet. The technological race among adversary nations to the United States of America is acatalyst for building the IoT. IoT devices range in size and shape to include but are not limited to smartphones, medical devices, light bulbs, satellites, routers, refrigerators, and televisions. Thepurpose of this research project was to analyze the cybersecurity of the IoT devices to provide recommendations for ameliorating the security of IoT devices. This project intended to answer what are the cybersecurity attack vectors of IoT devices, can the cybersecurity weaknesses within IoT devices be identified and mitigated, what is the national security threat related to IoT device cybersecurity? The findings conclude that IoT devices are subject to cyber-attacks through the principal IoT device components, which include hardware, software, and wireless connectivity.**Keywords — ***Internet of things,* ARPA, DoD, Cybersecurity**

I. Introduction

Kevin Ashton, an assistant brand manager at Procter & Gamble and a British technology pioneer, first coined the phrase Internet of Things (IoT) in 1999 (Arata & Hale, 2018). The basics of IoT affect more than technological development; IoT is a layered expansion of Internet services. The things component in an IoT environment are the devices, instruments, vehicles, buildings, and other items integrated with electronics, circuits, software, sensors, and networking capabilities. Wired and wireless networking capabilities connect the things to form the Internet of Things (Gokhale, Bhat, & Bhat, 2018).

Although the term IoT was coined in 1999, Ashton considered IoT devices to be radio- frequency identification (RFID) technology with a unique method of identification (Gokhale et al., 2018). RFID is a technology that uses electromagnetic fields or radio waves to transmit information that identifies a physical item. RFID is formed from a set of identification technologies. The technologies are comprised of different sensor operating techniques and of varying radio frequency characteristics (Dobkin, 2008). A historical examination of the components of RFID and wireless communication is used to support the foundation of IoT. An examination of the RFID tag contribution begins the historical examination.

RFID tags. RFID tags, or low-cost transponders, are part of the RFID system affixed to an object. RFID has existed since 1970 though the widespread use of RFID technology required the development of cost-efficient small integrated circuits. RFID tags are a vital component of IoT. RFID tags are appended to an item, and information is transmitted wirelessly within the environment of the item connected to the Internet (Frith & Ozkul, 2019). An example of RFID technology is the RFID clothing tags placed on clothing to prevent theft. If the clothing item's RFID tag is not correctly turned-off or removed, the RFID tag attached to the item wirelessly communicates theft alert to the business.

Wireless-telegraph. The first stages of wireless communication began with the wireless telegraph. Guglielmo Marconi is credited with the invention of the wireless telegraph in 1896. The first successful wireless telegraph used radio waves to transmit signals across the Atlantic Ocean in 1901. During the communication, alphanumeric characters were transmitted between two parties in an analog signal (Garratt et al., 1994). Wireless technology has led to the creation of technologies, including radio, television, communication satellites, mobile telephone, and mobile data, capable of transmitting information throughout the world. Since 1901, technological advancements have fostered a new focus on wireless networking, cellular technology, mobile applications, and the IoT (Stallings & Beard, 2016).

Wireless rescue. Wireless telegraph technology was first used in Maritime search and rescue in 1909 to rescue the crew and passengers of White Star Line's Republic after the USS Florida crashed into the Republic. The wireless telegraph was used to send as a distress signal to ships within the area. Only two passengers from the Republic perished. The first wireless distress signal was not the modern-day SOS but the letters CDQ (Edwards, 2020).

Marconi's company, Wireless Telegraph and Signal Company, Ltd. (changed to Marconi's Wireless Telegraph Company, Ltd. in 1900), first coined the use of CDQ as a maritime distress signal. However, the use of SOS as a distress signal was changed by the International community since the SOS was a more natural pattern to detect (McEwen, 1999). The first wireless distress signal alert to ships in the area is a concept like the RFID tags that alert a business to theft.

The wireless telegraph became essential to aiding ships in times of distress (McEwen, 1999). The wireless distress signal technology was improved to alert military bases of approaching aircraft during World War II. The beginning of if friend or foe technology (IFF) was an innovative technology developed to decern enemy aircraft from friendly aircraft (Dobkin, 2008).

II. LITERATURE REVIEW

Since 1999, the speed of information distribution, acquisition, storage, and retrieval, has changed, and the transfer of information through the Internet has impacted human life (Fraire et al., 2018). IoT cybersecurity is a vital concern in a world where hackers seize opportunities to invade IoT devices. Personal data is like a house, and each IoT device connected to the house is a door or window to the personal data. Multiple IoT devices connected to the house offer hackers more entry points. John Margulies, a cybersecurity consultant and owner of Evil Associates, as quoted in The Internet of Things and the Explosion of Interconnectivity, the threat to personal data increases as more devices are connected to the Internet. IoT devices have risks, including compromised personal security, suitable power sources, and data overload. IoT device advantages are efficiency and safety (Ornes, 2016).

The literature review ensues with the cybersecurity for IoT devices to provide recommendations for ameliorating the security of IoT devices. First, cybersecurity attack vectors of IoT devices are addressed, followed by an examination of methodologies to identify and to mitigate IoT device cybersecurity weaknesses. The literature review concludes by examining the relationship between national security threats and IoT device cybersecurity.

IoT Device Cybersecurity Attack Vectors

Device attacks. Understanding IoT device attack vectors requires an exploration of key terminology. Key terms are the taxonomy of attack terms, including attack, vulnerability, exploit, threat, and threat agent (Whitman & Mattord, 2016). According to the glossary term guide found in Army Doctrine Publication (ADP) 3-90, an attack is a continuing offensive action against an adversary (ADP3-90, 2019). Joint Publication 3-12 (JP 3-12) defines a cyber-attack as "Actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain, and is considered a form of fires" (JP3-12, 2018, p. GL-4). A glossary term found in Whitman and Mattord (2016) presents that an attack is harmful or malicious activities conducted to compromise information and the systems that support it; however, the activities may or may not be deliberate. Moreover, an attack is active or passive and direct or indirect.

Attack surface mapping and threat modeling.

According to Gupta (2019), determining the attack vectors in an IoT device begins with mapping the attack surface of the device. An attacker gathers as much intelligence about the product to include the device, documentation, prior research, or any online resources. Intelligence is used to map the attack surface. Mapping the attack surface of an IoT device includes three high-level vectors, namely the embedded device, programming (e.g., firmware, software, and application), and radio communications.

Hardware. The embedded devices are the components that constitute the design of the device. The embedded device is the thing in IoT. An example of IoT embedded devices is the smart home. The smart home consists of components such as gateways, smart switches, smart locks, smart bulbs, hubs, and any other IoT device (Gupta, 2019). The embedded device is the hardware, which includes any physical components (Cisco, 2014).

Performing a visual hardware inspection of the IoT hardware requires an assessment of both the external and internal components which provide attack vectors to an IoT device.

External components provide rapid access to the inside of an IoT device, and internal components provide components to gain command and control of an IoT device. Components that require little effort to compromise make natural attack vectors. Easy attack vectors are considered critical vulnerabilities (Gupta, 2019).

External. External components may include and are not limited to input and output (IO) ports, power buttons, headphone jacks, volume control, camera, docking connectors, Secure Digital (SD) card slots, Global Positioning Satellite (GPS) antenna port, and Universal Serial Bus (USB) port. External inspection and mapping are used to research and find vulnerabilities to be used in an attack. Knowledge of the physical IoT device is essential to an attack, and access to at least two devices is essential in the event one device fails. The external inspection is vital to planning an internal inspection (Gupta, 2019).

Internal. The internal component inspection includes diagraming and cataloging the internal components of the IoT device integrated circuit board (Gupta, 2019). Each electronic component is essential and includes resistors, capacitors, transistors, memory, and communications. Resistors, capacitors, and transistors supply power flow. Transistors also serve as switches (Guzman & Gupta, 2019). Memory components include random access memory (RAM), Read-Only Memory (ROM), and ROM memory hybrids (Electronically Erasable Programmable ROM: EEPROM and Flash). ROM chip data is created during manufacturing; RAM erases when power to the RAM chip is removed, and EEPROM chips or flash memory have data written after the chip is manufactured (Cisco, 2014). Communication components are either serial or parallel in design. IoT serial communication is more cost-effective than parallel communication. Moreover, parallel communication requires more resources than serial communication (Guzman & Gupta, 2017). Internal components that offer an attacker rapid escalation to a privileged state include memory and communication components (Gupta, 2019).

Radio. Current day IoT devices use radio or wireless communication protocols to communicate with the Internet or to communicate with IoT devices nearby. The Federal Communication Commission (FCC), in the United States, governs wireless technology frequency assignments, which include government exclusive, non-government exclusive, and government/non-government shared entities (Stallings & Beard, 2016). Standard wireless protocols available for IoT devices include Bluetooth, Wi-Fi, ZigBee, and Z-Wave (Guzman & Gupta, 2019). The FCC assigns each protocol a specific frequency range (Stallings & Beard, 2016).

Proprietary protocols exist for devices such as IoT gateways and hubs (Guzman & Gupta, 2019).

Each wireless protocol has a vulnerability found with line-of-sight communications. Objects such as walls, buildings, and weather weaken the wireless radio signals (Stallings & Beard, 2016). The distance between devices impacts the ability to attack protocols such as Wi-Fi, Bluetooth, ZigBee, and Z-Wave. However, attackers exploit radio communications by using technology to capture data. Captured data with weak encryption are vulnerable to cyber-attacks (Guzman & Gupta, 2019).

Bluetooth. Bluetooth is a wireless communication protocol available on computers, cell phones, and IoT devices (Armis, 2018d). Bluetooth's short-range communications protocol has

8.2 billion devices in use (Seri & Livne, 2019b). Bluetooth was introduced in 1998; moreover, the Linux based operating system module, BlueZ, has existed since 2001 to support Bluetooth. Samsung's Tizen and Amazon's Fire operating systems use the BlueZ module; furthermore, Linux is an open-source operating system that has allowed BlueZ to be a foundation for several Linux based operating system IoT devices (Seri & Livne, 2019b). The default setting for devices with Bluetooth capabilities is set to the on position. The default setting is a quick method to interconnect IoT devices such as headphones and keyboards. Most users accept the default Bluetooth setting, which is always listening for other Bluetooth devices (Seri & Vishnepolsky, 2017a).

BlueBorne. According to US-CERT, Bluetooth weaknesses contribute to a collection of vulnerabilities known as BlueBorne. Millions of unpatched devices, including IoT devices, computers, and cell phones, are a potential target. BlueBorne vulnerabilities allow a remote attacker to control affected devices (CISA, 2017). BlueBorne is an attack vector that does not require device pairing or discovery. Bluetooth connections are exploited to obtain total control of the targeted device (Armis, 2018d).

Wi-Fi Trojan. The Emotet trojan has reemerged as a worm module, which spreads through unsecured Wi-Fi networks. The worm-like characteristic of Emotet exploited the wlanAPI.dll to discover nearby wireless networks. Emotet conducted a brute-force attack on password-protected connections or accounts; moreover, compromised Wi-Fi networks provided Emotet with resources to propagate the malware. Resources exploited by Emotet include non- hidden shares and the user or administration accounts. Compromised administrative accounts set the stage to install the persistence portion called Windows Defender System Service (Threatwatch, 2020).

Mirai. The Mirai malware created a botnet (e.g., several malware-infected devices networked together) that exploited administrative credentials using a brute force attack. IoT devices infected by Mirai included webcams, Digital Video Recorders (DVRs), and routers. A historical Distributed Denial of Service (DDoS) attack impacted hundreds of thousands of IoT devices in September 2016. IoT devices are exploited through weak credentials (Fernández- Caramés & Fraga-Lamas, 2020).

IoT botnet. An IoT botnet is composed of several IoT devices infected with malware controlled by a remote bot-master using command and control channels. Network attacks include DDoS attacks, confidential data extrication attacks, and phishing attacks. IoT botnet malware targets IoT Central Process Unit (CPU) configurations. Targeted CPUs include ARM, MIPS, MIPSel, Motorola, PowerPC, and Intel x86 (Nguyen et al., 2019).

Studies conducted have discovered an IoT botnet life cycle. The IoT botnet malware life cycle formed four phases, including scanning, attacking, infection, and violation. During the scanning phase, the bot-master scanned the Internet to locate IoT devices with open Telnet ports or other services (Nguyen et al., 2019). Once the bot-master found a vulnerable IoT device, a brute-force attack was launched with known default credentials. The command and control server was notified of an available successful login attempt. Successful login attempts trigger the download and execution of a payload binary; furthermore, some territorial malware removes other malware. Malware detection was impeded as the malware runs in memory and removes files used during the infection. Finally, the IoT botnets perform attacks, including, however, not limited to DDoS, Hypertext Transfer Protocol (HTTP), and User Datagram Protocol (UDP) flood attacks (Nguyen et al., 2019).

Wireless sensor networks. Wireless sensor networks (WSN) reply on wireless networks to collect and transmit data; moreover, surveillance applications benefit from WSN's low cost and uncomplicated communications. Sensor power sources are non-renewable; furthermore, the sensor's network lifespan ends with power source expenditure. WSN security is required in security-sensitive environments, including military environments. WSN security is a primary research area (Fotohi, Firoozi & Yusefi, 2020). Two examples of WSN attacks include the battery sleep and battery depletion attack.

Battery sleep. Sensor node weaknesses contribute to sensor threat attack vectors. WSN's are vulnerable to sensor Denial of Sleep (DoSL) attacks. The sensor DoSL attack prohibits the sensor from entering an energy-saving mode and going to sleep. The DoS attack is a significant attack vector on network sensors; moreover, the DoSL attack drains the sensor battery in a few days compared to the standard life expectancy of sensor batteries. The battery is drained of power reserves, while the radio is prohibited from entering an energy-saving sleep mode (Fotohi, Firoozi & Yusefi, 2020).

Battery depletion. Radio communications in a WSN consume a high amount of energy. The WSN nodes can be subject to attacks like DoS attacks, which is a cyber-attack designed to prevent authorized users from using a service. In the case of a battery attack, the attack prevents the sensor from sleeping to conserve power. The result of the cyber-attack is an unauthorized physical attack designed to disable a sensor node by exhausting the battery completely. The term is a unique term named depletion-of-battery (DoB) attack (Shakhov & Koo, 2018).

Routers. The malware, VPNFilter, targeted routers with unpatched vulnerabilities. The slow destructive nature of VPNFilter targeted several manufacturers. In Heart's 2018 article, the VPNFilter malware attacked over 500,000 Small Office/Home Office (SOHO) routers around the world since 2016. Over fifty-four countries were infected with malware, which included household Internet devices. The router

VPNFilter infection resulted from unpatched system updates and default login credentials (Heartfield et al., 2018).

Emerging satellite technology. Satellite technology is the driving force behind an incredibly connected world with billions of interconnected devices communicating to track man and machine. Joint satellite and IoT technology are under development. The development of satellite network hardware and software specialty tools will require swift components to facilitate IoT applications (Majumdar, 2019).

National Security

According to Nicco Mele, Harvard lecturer and digital strategist, "Today, national security is fragile, with power shifting to technologically equipped terrorist groups, revolutionary movements, criminal enterprises, murky collectives such as Anonymous, and even isolated individuals with an Internet connection" (Pope, 2019, pp. 4-5). The United States' critical infrastructure is a combination of public and private owners and operators as well as other entities. Critical infrastructure categories include information technology, industrial control systems, cyber-physical systems, and the Internet of Things devices (Critical Infra Cyber, 2018).

National cyber strategy. According to United States President Donald Trump, Cyberspace security is a foundation for America's national security and prosperity. Cyberspace is embedded in American's economic and defense systems; furthermore, adversaries conduct malicious cyber-attacks on public and private sectors with a more significant occurrence and Avant-Garde while exploiting America's cyberspace liberty. (National Cyber Strat, 2018).

National defense strategy. Space and cyberspace are warfighting domains under the Department of Defense (DoD) whose investment priorities include resilience, reconstitution, space operation assurance, and cyber defense. Cyber defense capabilities continue to be integrated into the full spectrum of military operations (National Defense Strategy, 2018). Cyber operations are embedded in space operations. Space depends on cyberspace operations, and vital portions of cyberspace are provided through space operations (JP3-14, 2018).

Space Operations. The Joint Chiefs of Staff governs the Space Operations doctrine that outlines the scope of space operations. The embedded nature of space operations and cyberspace operations is unique compared to military operations in the air, land, and sea domain. Military operations depend on commercial space systems for communications, tagging, tracking, and locating as well as other support (JP3-14, 2018).

Cyber Operations. The Joint Chiefs of Staff governs the military Cyberspace Operation doctrine that outlines the scope of cyberspace operations. Adversaries may exploit the global market by threatening the United States company supply chains. The impacts of threats cover the entire system life cycle, which includes design, manufacturing, production, distribution, operation, maintenance, and disposals (JP3-12, 2018).

DoD cyber strategy. The United States and its allies must engage in a long-term strategic commitment to expand cyberspace competition with adversaries, including the governments of Russia, China, North Korea, and Iran. Adversary nations such as China erode economies through data exfiltration from the United States public and private sector. Russia continues to interfere with the United States democratic processes, and the malicious cyberspace activity continues to rise (DoD Cyber Strategy, 2018). The Department of Defense Cyber Strategy has three goals. The United States military will fight and win wars in the cyberspace domain, which is embedded in the land, air, sea, and space domain.

National Security Strategy. The United States National Security Strategy's goal is to embrace the protection of the American people, the American way of life, and American interests. Private or government information network protection is critical to the United States National Security Strategy's goals. Decisive actions to enhance cybersecurity are a joint taskforce among all entities, including the United States Government, private industry, and the public, with each securing operations under their command and control (National Cyber Strategy, 2018).

Discussion of the Findings

Historically, the Internet of Things (IoT) device development's early foundation began with ideas and technology which contributed to the wireless telegraph. The technology was driven by a race with adversary nations who compete with the United States for world power status. Business and medical sectors drive private non-military technology development. The purpose of this research project was to analyze the cybersecurity of the IoT devices to provide recommendations for ameliorating the security of IoT devices. The project questions analyzed are: What are the cybersecurity attack vectors of IoT devices? Can the cybersecurity weaknesses within IoT devices be identified mitigated? What is the national security threat related to IoT device cybersecurity? The Discussion of the Finding supplies major findings, implications and recommendations, a comparison of literature, and limitations to the study.

Perspectives

The literature review supplies evidence that IoT device cybersecurity is vital and that attack vectors require mitigation. The IoT device attacks vectors and mitigation deserve attention to the point that the national security of the United States is a factor. The significant findings are based on three examinations of IoT device perspectives, including industry-driven, tactical, reactive operations, and strategic planning.

Industry driven perspective. The IoT industry is driven by the three IoT device components, namely hardware, software, and communications. A cybersecurity IoT device environment must have cybersecurity embedded into all three components. The individual components may be secure when set apart in isolation; however, when meshed, the components pose a risk to each other (Gupta, 2019). Each component is examined to determine how the component is related to the

customer-supplier relationship (Rutherford, 2019). The February 2020 NIST publication NIST IR 8276 Draft proposes the terms acquirers and suppliers; moreover, the publication proposes guidelines helpful in managing IoT device development from a customer-supplier perspective (Boyens, 2018).

Hardware. The hardware of an IoT device offers external and internal attack vectors. The external attack vectors included any areas an attacker attaches to a device to exploit internal device resources. Internal attack vectors included integrated circuits, software, and radio (Guzman & Gupta, 2019). Concerns about integrated circuitry hardware trojans have been considered in the cybersecurity community. IoT devices such as refrigerators with malicious circuitry is a potential attack vector directed to a larger target due to the lack of refrigerator security. A disgruntled employee or third-party source could sabotage a circuitry. A strategically placed IoT device with malicious hardware could be used to eavesdrop on networks or conversations in the break room at a company, in a home, or a military installation. Malicious hardware is a problematic vulnerability to mitigate once in production (Simranjeet et al., 2019).

Software. The second vital component of an IoT device is the software. Software controls the operation of an IoT device, including firmware, operating systems, and applications. Attackers target firmware, operating systems, and applications to gain command and control essential to attack objectives (Guzman & Gupta, 2019). Several IoT device software frameworks are available to manufacturers. Appendix A shows a list of nineteen popular IoT device frameworks. Some IoT device manufacturers create in-house frameworks, and some manufacturers outsource framework development to third-party sources. The IoT device manufacturer is a customer to the third-party vendor. The in-house frameworks have an internal customer, which is the manufacturer's product, with software development being the internal supplier (Gupta, 2019).

Reactive tactical perspective. Cybersecurity for IoT devices is often put in place after the design is complete leaving the cybersecurity placement as a last-minute reactive response. IoT devices are often deployed or installed with default or factory settings, including weak or default passwords, which later requires a reactive tactical response. Deployed IoT devices needing software patches are left unpatched. The weak credentials and unpatched software provide an attack vector. IoT device developers plan cybersecurity as an afterthought, which results in a reactive approach to cybersecurity. Emergency patches to the software are created and deployed; however, not all IoT devices users are cybersecurity specialists (Hare & Diehl, 2019).

Attack vectors. Old IoT device attack vectors can repeat, which occurred with Emotet (Binary Defense, 2020). IoT device systems can be tested for vulnerabilities at any time during production through penetration testing (Guzman and Gupta, 2019). As presented earlier, recent IoT devices named attacks include BlueBorne, VPNFilter, Emotet, and Mirai. IoTSF offers guidelines to mitigate the named attacks and future attacks.

IoTSF. IoTSF has fourteen guidelines for developing a new IoT device; moreover, the guidelines include steps for securing current IoT devices and future IoT devices. IoT device cybersecurity is contingent upon the device data and the device environment. Added security features are contingent upon resource and IoT device cost projects (IoTSF, 2019).

Penetration testing. Gathering information or intelligence about an IoT device is vital to the attack and is accomplished through the penetration test. The penetration test is usually a sanctioned investigation of a device or system to determine existing vulnerabilities, and the penetration test investigated was designed by two authors, Aaron Guzman and Aditya Gupta.

Strategic perspective. The United States has embraced a more initiative-taking tactical level cybersecurity strategy for IoT device cybersecurity. In 2018, leading organizations, including NIST, the DoD, and White House, updated or created new guidelines designed to emphasize a national interest in cybersecurity. In 2019 and 2020, NIST published new guidelines to aid IoT device development. Each document presents strategic level cybersecurity guidance for government and private industry to follow. The guidance documents are directed toward private industry and government-related cybersecurity strategic planning to include NISTIR 8228, NISTIR 8259, NISTIR 8259A, DoD Cyber Strategy, JP3-12, JP3-14.

III. Implications and recommendations

IoT development has been driven by two primary factors, including the technology race and a business or medical need. The beginnings of IoT devices pre-date the Internet; moreover, the 19th Century wireless telegraph was one of the beginning technologies which contributed to current technology developments. The technology race with adversary nations to the United

States continues to push IoT device development with business and medical sectors reaping society benefits. The use of wireless technology in Search and Rescue has proven the value of early wireless networking. The implications and recommendations of the research show that attack vectors and risk migration are a threat to national security.

Implications. The implications of this research study revealed that NIST, Whitehouse, and most DoD publications provide IoT device cybersecurity guidelines to manufacturers and suppliers. The publications link national security to IoT device cybersecurity. The term IoT appeared in most of the publications to enforce the connection between IoT device cybersecurity and national security (National Cyber Strategy, 2018).

The NIST mitigation standards suggest customer service needs as a planning point to the IoT device life cycle. Supplier situational awareness of potential cybersecurity attack vectors is essential to protect the customer. Customers are the critical

infrastructure, military, and civilian IoT devices ranging from smartphones, weapons, and cars to refrigerators and medical devices. Not all customers are cybersecurity specialists, programmers, or IT professionals. Robust cybersecurity must be built into IoT devices (Critical Infra Cyber, 2018).

Software developer training lacks the necessary skills to avoid cybersecurity risks.

Software development mistakes such as the buffer overflow found in the 1998 Morris Worm continue to be repeated. Software development curriculum and continuing education need risk mitigation concepts to narrow attack vectors produced by software flaws (Hong, 2016). Software developer training is essential to managing cybersecurity risks.

Third-party software and hardware suppliers are a potential attack vector source.

Unchecked hardware and software development processes are a risk to the IoT device development lifecycle. IoT devices placed in production with default settings and credentials augment cybersecurity risks. The continued emergence of new attacks, including specifically named attacks such as BlueBorne (CISA, 2017) and Wi-Fi VPNFilter (Heartfield et al., 2018), are supporting examples. While Emotet was an old attack directed toward the financial industry, Emotet has evolved to invade wireless components (Binary Defense, 2020).

IoT device cybersecurity will exist as new attack vectors will develop. Strategic level cybersecurity planning reduces the attack vectors to provide more focus on resources on defeating adversaries like China, Russia, Iran, and other adversaries who choose to use IoT device technology to attack the United States. The United States' 2018 updates to key policies are evidence connecting IoT device cybersecurity to national security threats (DoD Cyber Strategy, 2018).

Recommendations. Further research is needed in the areas which require more focused research. Three focus areas include software curriculum modifications to address programming flaws, outsourcing hardware, and software to an adversary, or third-party vendors, IoT device certification and IoT device cybersecurity terminology. Each recommendation is geared toward lessening the IoT device attack vectors and relates IoT device cybersecurity to national security.

More stringent software developer standards through college curriculum and continuing education teach the importance of structured software design. The software development life cycle of an IoT device is an essential inclusion to the software development curriculum.

Software developers need education designed to help them avoid software flaws that lead to adversary exploitation or logic errors (IoTSF, 2019).

IV. Comparisons

The literature comparison focuses on terminology and standards. Consistent terminology across the civilian curriculum, DoD doctrine, and industry is needed to defeat an adversary or provide a proactive offensive to IoT device cybersecurity attacks. Lack of consistent terminology is a weakness which points to a lack of standards.

The cybersecurity community definition for an attack varies in one academic resource by Whitman and Mattord (2016) compared to military and national security definitions. The definition was cited earlier was taken from the text glossary; however, chapter 2 excluded the wording intentional or unintentional. The use of intentional and unintentional in the definition of attack is not mentioned in two military doctrines, including Army publication, ADP 3-90, and JP 3-12. JP 3-12 is a doctrine published by the Joint Chiefs of Staff to provide cyberspace guidance across all military operations.

NISTIR 8276 Draft proposes the terms acquirers and supplies as compared to IoTSF and NISTIR 8259 (IoTSF, 2019; Fagan et al., 2020b). The term customer is used in published policy and guideline documents compared to the acquirer. The term within an organization should be consistent even when in draft status.

The DoSL and the DoB attacks presented were similar terminologies for an attack on WSN. Both DoSL and DoB attacks inferred that the sensor was attacked in a fashion like a DoS attack. The constant sensor stimulation degraded, disrupted, and denied the IoT device's sleep period needed to conserve battery resources (Shakhov & Koo, 2018). A consistent set of cybersecurity vocabulary affects the seriousness of cybersecurity and affects future leaders, whether military or civilian. The definition of terms such as an attack and introduction of cyber community acronyms needs guidance to provided consistency needed to defeat adversaries (Pope, 2019). The NIST, DHS, DoD, or IoTSF can provide guidance or a repository for terminology.

Limitations

Limitations of this research study include the exclusion of most popular news items produced by cybersecurity firms as a method of communicating current cybersecurity information. Google Scholar search limitations occurred where articles required substantial subscription fees to obtain articles. The overwhelming amount of information from sources requiring monies to access relevant studies limits businesses seeking knowledge where their budget limits expenditure towards cybersecurity research. Three avenues of more in-depth exploration include hardware malware, college curriculum, and wireless technology.

V. Conclusion

19th Century wireless telegraph was one of many technologies that contributed to current Internet of Things (IoT) device technological developments, although Ashton coined the term IoT in 1999. Early wireless technologies such as if friend or foe, RFID, and aircraft Electronic Locator Transmitter as well the first artificial satellite were technological contributors. The first artificial satellite, Sputnik, and nuclear weapon detonation by the Russian government sparked a technology race. The ARPANET, an early predecessor to the Internet, combined with a Coke machine, was a first in IoT devices. The technology race with adversary nations, Russia, China, Iran, and other adversaries, continues to push the United States' IoT device development with business and medical sectors reaping the benefits. Business and medical drive IoT device investments that benefit society and infrastructure, although military and government utilize private sector

infrastructure. IoT device cybersecurity is necessary to protect IoT device assets and data. The purpose of this research project was to analyze the cybersecurity of the IoT devices to provide recommendations for ameliorating the security of IoT devices. Considerations include what the cybersecurity attack vectors of IoT devices are, can the cybersecurity weaknesses within IoT devices be identified and mitigated, and there is a national security threat related to IoT device cybersecurity. The literature review section provided a selection of research for the reader, which sources ranged from books, journal articles, and Google Scholar or library searches. Wireless communication is subject to jamming or interception, and weak encryption resources within heavily constrained IoT devices cause IoT device cybersecurity attack vectors. Emerging technologies are the next attack vector, which includes satellite and LiFi. The attack vectors will never be eliminated; however, risk mitigation will lessen the attack vector surfaces.

Mitigating attack vectors is conducted through the adoption of standards, training, and best practices. NIST has published new standards to guide businesses when creating IoT devices for consumer use. The standards include IoT device manufacturer guidelines aimed at designing cybersecurity into IoT devices from design conception. Intermediate NIST standards include software developer standards designed to provide a robust software development lifecycle.

REFRENCES

[1] Arata, H. & Hale, B. (2018). Smart Bases, Smart Decisions. The Cyber Defense Review, 3(1), 69-78. Retrieved from https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Smart%20Bases%20Smart%20Decisions_Arata_Hale.pdf?ver=2018-07-31-093711-343

[2] Armis. (2019c). The dangers of Bluetooth implementations: Unveiling zero-day vulnerabilities and security flaws in modern Bluetooth stacks. Retrieved from https://info.armis.com/rs/645-PDC-047/images/BlueBorne%20Technical%20White%20Paper_20171130.pdf

[3] Bednarz, A. (2019). Evolution of the Internet: Celebrating 50 years since Arpanet. Network World. Retrieved from https://link-gale-com.ezproxy.utica.edu/apps/doc/A595722364/AONE?u=nysl_ce_uticacol&sid=AONE& xid=23096322

[4] Binary Defense. (2020). Emotet Evolves with New Wi-Fi Spreader. Retrieved from https://www.binarydefense.com/emotet-evolves-with-new-wi-fi-spreader.

[5] Browning, D. (2018). IoT started with a vending machine. Retrieved fromhttps://www.machinedesign.com/automation-iot/article/21836968/iot-started-with-a- vending-machine

[6] Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K., Nadeau, E., Piccarreta, B., O; Rourke, D. & Scarfone, K., (2019). Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. NIST 8228. https://doi.org/10.6028/NIST.IR.8228

[7] Boyens, J., Paulsen, C., Bartol, N., Winlkler, K. & Gimbi, J. (2020) Key Practices in Cyber Supply Chain Risk Management. NIST. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8276-draft.pdf

[8] Cofense. (2020). Cofense: Malware Trends Q4 2019. Computer Fraud & Security. Volume 2020, Issue 2, Page 4. https://doi.org/10.1016/S1361-3723(20)30015-4.

[9] Cheruvu, S., Kumar, A., Smith, N. & Wheeler, D. (2020). Demystifying Internet of Things Security Successful IoT Device/Edge and Platform Security Deployment. Apress Open. [Kindle]

[10] Coke Machine. (n.d.). The Only Coke Machine on the Internet. Retrieved from https://www.cs.cmu.edu/~coke/history_long.txt

[11] Critical Infra Cyber. (2018). Framework for Improving Critical Infrastructure Cybersecurity.

[12] Cyber Strategy. (2018). National Cyber Strategy of the United States of America. (pp. II, 1-3) Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/09/National- Cyber-Strategy.pdf

[13] DHS. (2011). Risk Management Fundamentals Homeland Security Risk Management Doctrine.

[14] Dobkin, D. (2008). The RF in RFID: Passive UHF RFID in Practice. Amsterdam: Elsevier / Newnes. Retrieved from https://uclibraryts.on.worldcat.org/oclc/182759189

[15] Dobson, D., Souppaya, M. & Scarfone, K. (2020d). Mitigating the Risk of Software Development Framework. NIST. https://doi.org/10.6028/NIST.CSWP.04232020

[16] DoD Cyber Strategy. (2018). Department of Defense Cyber Strategy. Retrieved from https://media.defense.gov/2018/Sep/18/2002041658/-1/- 1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

[17] Edwards, J. (2020). First Radio Rescue at Sea. Retrieved from https://oceanlinersmagazine.com/2018/01/22/radio

[18] Fagan, M., Megas, K., Scarfone, K. & Smith, M. (2020b). Foundational Cybersecurity Activities for IoT Device Manufacturers. NISTIR 8259. https://doi.org/10.6028/NIST.IR.8259

[19] Fagan, M., Megas, K., Scarfone, K. & Smith, M. (2020c). IoT Device Cybersecurity Capability Core Baseline. NISTIR 8259A. https://doi.org/10.6028/NIST.IR.8259A

[20] Fernández-Caramés, T. & Fraga-Lamas, P. (2020). Teaching and learning IoT cybersecurity and vulnerability assessment with Shodan through practical use cases. Sensors,20(3048). https://doi.org/10.3390/s20113048

[21] Fraire, J., Finochietto, J. & Burleigh, S. (2018). Delay-tolerant satellite networks (Ser. Artech house space technology and applications series). Artech House. https://uclibraryts.on.worldcat.org/oclc/1027692494

[22] Frith, J. & Ozkul, D. (2019). Mobile Media Beyond Mobile Phones. Mobile Media and Communication 7(3):293–302. https://doi.org/10.1177/2050157919850405

[23] Fotohi, R., Bari, S. & Yusefi, M. (2020). Securing wireless sensor networks against denial-of- sleep attacks using RSA cryptography algorithm and interlock protocol. International Journal of Communication Systems, 33(4). https://doi.org/10.1002/dac.4234

[24] Garratt, G., Institution of Electrical Engineers, & Science Museum (Great Britain). (1994). The early history of radio: from Faraday to Marconi (Ser. IEE history of technology series, 20). Institution of Electrical Engineers, in association with the Science Museum.

[25] Gokhale, P., Bhat, O. & S. (2018). Introduction to IoT. IARJSET. Retrieved from https://www.researchgate.net/profile/Omkar_Bhat2/publication/330114646_Introduction

[26] _to_IOT/links/5c2e31cf299bf12be3ab21eb/Introduction-to-IOT.pdf GPS. (2020). How accurate is GPS? Retrieved from

[27] Gupta, A. (2019). The IoT Hackers Handbook. Apress. https//doi.org/10.1007/978-1-4842-4300- 8

[28] Guzman, A. & Gupta, A. (2017). IoT Penetration Testing Cookbook. Packt Publishing.

[29] Hare, F., & Diehl, W. (2020). Noisy Operations on the Silent Battlefield: Preparing for adversary use of unintrusive precision cyber weapons. The Cyber Defense Review, 5(1), 153-168. doi:10.2307/26902668

[30] Hong, J. (2016). Toward a Safe and Secure Internet of Things. New America. Retrieved from www.jstor.org/stable/resrep10509.5

[31] IoTSF. (2019). Secure Design Best Practices Guide. IoT Security Foundation. Retrieved from https://www.iotsecurityfoundation.org/wp-content/uploads/2019/12/Best-Practice- Guides-Release-2_Digitalv3.pdf

[32] JP3-12. (2018). Joint Publication 3-12 Cyberspace Operations. Retrieved from https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16- 134954-150

[33] JP3-14. (2018). Joint Publication 3-14 Space Operations. Retrieved from https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14.pdf?ver=2018-12-10- 100705-667

[34] Kwiat, K. & Born, F. (2018). Simulation for strategic hardware trojans testing. EE-Evaluation Engineering,57(3), 18.

Lukasik, S. (2011). Why the ARPANET was built. IEEE Annals of the History of Computing, 33(3), 4–20.