https://doi.org/10.48009/3_iis_2020_168-178
Issues in Information Systems
Volume 21, Issue 3, pp. 168-178, 2020

A MULTI-LAYER APPROACH TO DETECTING AND PREVENTING IOT-BASED BOTNET ATTACKS

Bryon Miller, Northeast Alabama Community College, millerb@nacc.edu
Xihui Zhang, University of North Alabama, xzhang6@una.edu

ABSTRACT

As the Internet of Things (IoT) becomes ubiquitous and cybersecurity attacks rapidly evolve, IoT devices must be secured. Their infection can lead to compromised networks, stolen information, service disruptions, and botnet attacks. Botnet attacks, such as Distributed Denial of Service (DDoS), strengthen with larger numbers of devices and IoT devices make great targets for this reason. As IoT devices grow in number, the strength and risk of these massive attacks grow. Infamous botnet attacks, such as Mirai, have proven this to be a serious threat. IoT security faces unique challenges including detection difficulties, device limitations, and user attitudes and education. This paper reviews and analyzes 21 articles providing information on tools and techniques for securing IoT devices against these threats. A multi-layer approach to IoT-botnet detection and prevention is suggested consisting of: the outer layer consisting of ISP architecture; the middle layer consisting of advanced detection methods and DDoS detection and mitigation; and the inner layer consisting of user attitudes, education, and security best practices. By addressing security challenges at multiple points along the botnet lifecycle and within each layer, our proposed approach provides a holistic strategy for detecting and preventing botnet attacks.

Keywords: Botnet, Internet of Things, IoT, DDoS, Cybersecurity

INTRODUCTION

The Internet of Things (IoT) technology, defined as technology that is a physical extension of Internet connectivity, has evolved and expanded rapidly over the past several years and has become a ubiquitous technology in society today (Nguyen et al., 2019). These devices can include anything from security cameras and WiFi-connected baby monitors to smart speakers, smart plugs, and smart TVs. "The rapid growth of these devices has had profound impacts in settings such as the automotive industry, aviation, smart homes, medical wearables, agriculture, and smart cities" (Celik et al., 2019, p. 5). While this technology brings with it many conveniences, solutions to daily problems, automation for menial tasks, and other benefits, it also comes with security risks. While beneficial, these devices were not designed with security as the top priority and this is evidenced by the fact that they regularly collect and transmit unencrypted data (Rochford, 2019). They are also susceptible to malware infections just like any other Internet-connected device. Krishnan et al. (2019, p. 1896) add that, "IoT devices come with little to no security features, open ports, default security credentials and are poorly maintained/not updated regularly." As a result, bad actors have targeted them for malware that allows the devices to be controlled by a single, malicious controller. Most of these attacks begin with fairly simple malware that allows remote access and control by another device. After gaining access to enough devices, they amass a large network of the "bots" to create what is known as a botnet. The more devices available, the larger the network can become. These large botnets can then be leveraged to mount a massive distributed denial of service (DDoS) attack that can cripple large web services or similar targeted services.

This information is particularly concerning because of the rapid rate at which IoT technology is being developed and released. IoT device development and adoption are exploding. One estimate predicted that there were about 8.4 billion Internet-connected devices in 2017 and that in 2020 that number would increase to 20-50 billion (Kim et al., 2018; Kimani et al., 2019). The Cisco Annual Internet Report (2018-2023) White Paper (2020) lists increasing machine-to-machine interactions, IoT device growth, and increasing mobile IoT adoption as some of the top trends in IT. Some studies note IoT's growth and influence related to other technologies such as 5G (Nieto et al., 2018), smart power grids (Kimani et al., 2019; Yilmaz & Uludag, 2019), and industrial systems (Lee et al., 2018). Yet another study predicted that, by the end of 2020, "25% of cyberattacks will have involved IoT devices" (Gartner as cited in Nguyen et al., 2019, p. 1). As a consequence of these statistics, we can confidently predict that the number of attacks utilizing botnets, and the strength on these botnets, will increase even more in the future as the number of

IoT devices increases and security struggles to keep up. That is, unless researchers, security professionals, and IoT device owners do their part to fight back.

This article will review the current literature surround botnets, IoT device security, and the intersections of both. This information is analyzed to determine what is being done and could be done, to prevent, detect, and resolve IoT vulnerabilities and botnet attacks. Further, the analysis explores potential areas for future research that may be done. Finally, findings from these analyses are summarized and combined into a multi-layer model of detection and prevention. From this model, suggestions are made to researchers and security professionals that deal with IoT security. As the already massive field of IoT continues to rapidly expand, more and more research will need to be done. Additionally, more and more security professionals will become involved in this work, if they are not already. As such, work must be done now to advance research in this area to prepare for future attacks.

LITERATURE REVIEW

Current literature related to botnets, IoT devices, and attacks mounted with these technologies reveals some keys to understanding how botnets develop, how to prevent them from controlling our IoT devices, and why we should work towards more effective methods of detection and prevention. Firstly, several articles discuss the basics of botnet development, structure, attack vectors, and other relevant features. To fully cover these areas would be far beyond the scope of this paper, however, there are a few data points that will be useful for future discussions. To begin, Nguyen et al. (2019, p. 1) explain that, "Botnet is a network consisting of the infected IoT devices, referred to as bots, controlled by one or more attackers (botmasters) that remotely control the bots to perform malicious activities." Typically, new devices are added to this network without the device owner's knowledge using malware that can be installed and/or executed remotely. Shorman et al. (2019, p. 2) list some key characteristics of botnets including that "most of them are Linux based, reside on the RAM of compromised IoT device, generate very high volume of traffic floods, and the infected IoT devices are distributed all around the world." They also add that botnets are difficult to detect because they minimally affect the performance of the IoT devices. A final relevant point is that botnets can cause tremendous damage to host devices and external systems. This point is better illustrated when discussing the types of attacks mounted using botnets.

Secondly, there are definite reasons to be concerned about the threat of botnets as their host devices, namely IoT devices, grow in number. One reason discussed in the introduction is that botnets grow more powerful as they grow in size and their attacks have more weight behind them. DDoS attacks are a perfect example of this. Since the number of IoT devices online continues to expand rapidly, the risk of these massive attacks also expands. Another reason is that the areas where these devices are now in operation include very critical areas such as energy, healthcare, military, industrial systems, and other areas that could have severe and wide-ranging effects if attacked (Al-Duwairi et al., 2020; Kimani et al., 2019; Lee et al., 2018). These are areas that could cripple an economy, compromise a military mission, or cost the life of a healthcare patient. While many IoT devices are home appliances or business convenience items, this is not the case for all IoT devices. These risks are real and must be considered when researching and working with IoT security.

Thirdly, the literature indicates that there are multiple types of attacks that botnets can conduct, but the most common and most dangerous, is a distributed denial of service, or DDoS, attack. Other forms of attack include keylogging, phishing, spamming, click fraud, identity theft, and proliferation of malware (Koroniotis et al., 2019). Lastly, current research suggests multiple methods for detecting malware and potential botnets as well as methods for protecting IoT devices. Some of the articles that were reviewed offered one or more new methods for detection or prevention, while others focused on improving existing methods. Since identifying and summarizing some of the most promising botnet detection and prevention methods is the primary focus of this article, the methods uncovered through this literature review will be discussed in a later section.

RESEARCH METHODOLOGY

For this study, 21 articles were selected for analysis. These articles were selected using search criteria including keywords such as botnets, Internet of Things (or IoT), cybersecurity, and Distributed Denial of Service (or DDoS). Articles with combinations of these keywords were given preference. Some articles mentioning only one keyword were excluding. For example, articles mentioning DDoS and/or cybersecurity, but not mentioning IoT or botnets

(the focus of this paper), were excluded unless they significantly addressed an issue related to IoT security or botnets. Preference was also given to more recent research. There are two key reasons for this. Firstly, cybersecurity is rapidly evolving, IoT devices are becoming more prevalent, and significant botnet attacks are relatively new to the list of mainstream cyber-attacks; therefore, older literature is less likely to be focused on the specific issues addressed in this research and more likely to offer solutions that have been improved with more recent research. Secondly, the number of articles related to cybersecurity, DDoS, IoT security, etc. increases as the time frame increases. Since there were limited resources and time constraints with this research project, the quality of literature was prioritized over the quantity of literature. To be consistent, only articles published less than 3 years ago were considered. After scanning through the articles, the literature was further distilled down by choosing only works that mentioned botnets, IoT devices, DDoS attacks with some relation to IoT or botnets, or detection/prevention methods that were found in other cybersecurity literature and proven to be useful for use with IoT security or botnets.

RESULTS

The literature reviewed was selected by topic and includes research concerning DDoS attacks, botnet attacks, botnet detection, IoT devices, and cybersecurity methods from similar fields that may apply to the presented security risks. A total of 21 articles were reviewed and five areas were derived from the review.

Three Unique Challenges

Detection. One of the greatest challenges presented by botnets is difficulty detecting them. This is especially challenging with IoT devices for several reasons. Firstly, they have device limitations (discussed later) that may prevent them from efficiently running more traditional antivirus or scans. Secondly, users may neglect these devices as less significant and not monitor them to the level that they do their network, computers, and other devices. This is discussed further in another section. Lastly, many IoT devices suffer from poor security vulnerability management leaving them with little or no security functions, default passwords that are easily located, and old firmware/software in need of updating (Kim et al., 2018). One study found that "70% of [IoT devices] are not encrypted during communication and 60% of them have a weak web interface and have not been updated for security" (Kim et al., 2018, p. 2). These deficiencies not only make the devices less secure but can also make it more challenging to detect malware and other malicious files. On a related note, DDoS attacks also face a detection issue as botnet devices that are a part of these attacks are often difficult to distinguish from legitimate, non-malicious clients. They "easily confuse the traffic; thus it becomes difficult to trace it" (Reddy et al., 2018, p. 1). They are innately deceptive as a result and a challenge to stop without temporarily shutting down the service.

Device limitations. Susceptible IoT devices are often smaller, less complex devices that will operate using low power. They often do not require as much computational power as other Internet-connected devices and have limited ability and storage to keep their cost and size down (Al-Duwairi et al., 2020). Additionally, analyzing IoT systems can be challenging as existing analysis techniques may require high computational costs, high energy consumption, and bring with them scalability concerns (Celik et al., 2019). Fortunately, the limited resources available to IoT devices also limits the functionality of the malware that can be installed and run on the device (Nguyen et al., 2019). This means that more complex malware that requires greater computing power and energy is not typically a viable option for an attacker.

User attitudes and education. Users often view these devices as less significant and less likely to pose a security risk. As a result, they may not be secured at the same level as many other devices. For example, they are often unattended and are not physically accessed for routine checks or maintenance often enough to ensure their security (Al-Buwairi et al., 2020). Unfortunately, this puts the devices at risk of being infected and misused as a part of a botnet attack and puts the network at risk of further infection. As in many other areas of cybersecurity, end-users can play a major role in securing IoT devices and their networks. At the same time, changing attitudes and properly educating these users can be a challenging endeavor since security is not typically their top priority. Not to mention that they are sometimes difficult to access as they may be located in hard to reach spaces and there may be a large number of the devices in use for a given organization.

Methods of Detection and Prevention

Advanced detection methods. Considering the fact that some older IoT devices will be very difficult to fully secure, detection is perhaps the most important step to take to ensure these devices are not misused. Even for newer devices, the likelihood that any connected device is fully secured for an extended period of time is highly unlikely, so detection is again critical to the security of these devices. The research suggests multiple different methods of detection and some have very high success rates. A few of them are described in this section.

Neural networks and PSI-Graphs were found to be a successful tool for detection. Neural networking is a growing field and is being used in cybersecurity to detect and defend against various forms of attack. One article exploring the Marai botnet malware found a promising neural networking tool called a sparse autoencoder could be used to detect botnet malware. Kumar and Bhama (2019, p. 8323) explain as follows: "A sparse autoencoder is a neural network-based anomaly detector trained to reconstruct its inputs after some compression. During compression, the sparsity factor ensures that the activation rate stays low so that a neuron in the hidden layer activates only for a small fraction of the training sample. Compression ensures that the network learns meaningful concepts and the relations among its input features." This allows for data collection and analysis that leverages deep learning to identify anomalies in network traffic. They also utilized a detection technique based on CPU usage to identify cryptojacking network traffic. These techniques were an improvement over previous methods and demonstrated a 99.69% accuracy rate with a misclassification rate (of cryptojacking traffic) of only 1.5% (Kumar & Bhama, 2019).

PSI-graphs, or printable string information graphs, show the relationship structure of functions containing printable strings in potentially malicious files (Nguyen et al., 2019). These executable files are one way to identify that a device has been targeted by botnet-associated malware. Nguyen et al. (2019) demonstrated that using their method, one which combines the use of neural networks with PSI-graphs, led to the discovery of the IoT botnet life cycle and it achieved detection accuracy of 98.7%.

In an effort to transform one of the weaknesses of IoT devices into a strength, Jung et al. (2020) showed that power consumption modeling, within a deep learning model based on a convolutional neural network (CNN), can be used to reliably detect IoT botnets. In this method, an IoT device is assumed to have a normal pattern of power consumption. This pattern is derived from an 8-layer CNN-based deep learning model. The system monitors the devices for deviations from this pattern. These deviations are associated with malicious behaviors and may, therefore, be used to detect them. This method achieved up to 96.5% classification accuracy for botnet detection.

The concept of Internet-wide vulnerability scanning is not a new one but is now becoming a useful and readily available tool for security professionals. The goal of these scans is to identify vulnerable devices, including IoT devices, and then alerting administrators of the vulnerabilities. Kim et al. (2018) describe a model where scanning techniques such as ZMap and Shodan are improved through an IP alive scan, a reactive handshake scan, and an OS fingerprinting module. Through this suggested model they demonstrated noticeable improvements to the performance of ZMap which could make these scans more effective at discovering vulnerable devices. Applying this model to current scans may allow more vulnerable devices to be discovered and at a quicker pace.

Conti et al. (2020) explore an "attestation-enabled secure and scalable routing protocol for IoT networks" as a means of detection. Essentially, remote attestation, which has been proven as a useful tool for spotting malware, is improved upon by incorporating the routing protocol for low power and lossy (RPL) networks. Since IoT devices, especially in a large network, present unique challenges to detection, a unique method is often necessary to meet their needs. In this case, RPL allows the devices to use an attestation technique that requires less power, memory consumption, and network overhead. The resulting attestation method, dubbed SARP, demonstrated adequate performance, a lightweight structure, and better security compared to high-quality techniques.

Crowdsourcing is a technique that has become a popular method of solving problems, raising money (crowdfunding), and generating new ideas. Nieto et al. (2018) suggest that it can also be a valuable tool in detecting and mitigating cybersecurity threats. There are several ways to accomplish this, but one example is by enlisting social media users in a reward-based activity where they identify a threat, collect and submit evidence, and are rewarded. One perk of this method is that it leverages the large number of users in the world against a problem that involves a large number of potential bots. A second idea put forth by Nieto et al. (2018) is to crowdsource

information from the IoT devices themselves. This could be accomplished by having software installed that searches for malware and alerts the user of the issues. This information collected from several IoT devices could help researchers and professionals understand how new malware is being spread, what it looks like, and where new botnets are developing.

Since legacy systems and software is a common occurrence in industrial fields, industrial IoT devices often utilize legacy software and interact with legacy systems. Lee et al. (2018) explain that this creates a situation where IoT will suffer from the same security vulnerabilities associated with the legacy systems and software. To address this issue, they recommend utilizing a whitelist-based firewall and intrusion detection system in tandem. It was demonstrated that this method can detect anomalies in control system connections without any packet loss or delay.

The term intrusion detection system (IDS) is mentioned a few times in the reviewed literature and the concept of anomaly detection and abuse detection is widespread. One article suggests that IDS is important, but that it has its flaws. Shorman et al. (2019) explain that many forms of anomaly detection lead to several false alarms and common methods of abuse detection often fail to detect less popular or unknown attacks. To address these challenges, they propose an "evolutionary unsupervised network-based algorithm to detect IoT botnets…utilizing the OCSVM algorithm" (Shorman et al., 2019, p. 2). OCSVM is another algorithm that makes use of machine learning, as with previous detection methods, to learn typical behavior on a network and identify atypical behaviors as anomalous. Their proposed algorithm outperformed unsupervised comparison algorithms. It produced more true positives, less false positives, and was able to detect IoT-botnet attacks in five seconds.

Kimani et al. (2019) have compiled a list of plans for attack mitigation including a list of intrusion detection systems such as signature-based, anomaly-based, host-based, network-based, and stack-based. Signature-based IDS check attacks for unique signatures by comparing them to previous attack data. Anomaly-based IDS searches for vulnerabilities by applying artificial intelligence to analyze network traffic for anomalies. Host-based IDS works on the network host to collect and analyze network traffic associated with the host. Network-based IDS is similar to host-based but it is capable of monitoring the entire network. Stack-based IDS works closely with the TCP/IP stack by monitoring packets throughout the OSI layers.

Honeypots are not a new concept, but they are particularly useful in cybersecurity. A honeypot is essentially a trap for would-be attackers. It appears as a normal IoT device but sets off an alarm or alert of some sort when it has been tampered with in any way. "The best definition of a honeypot system was given by Spitzner, stating that a honeypot is a resource whose value lies in being probed, attacked, or compromised" (Pauna et al., 2019, p. 502). Pauna et al. (2019) expand on this concept by suggesting self-adaptive honeypots for use in IoT security. Self-adaptive honeypot systems work by allowing the execution of certain actions within the SSH server console. This was further improved by Pauna et al. (2019) by adding rootkit malware detection capabilities and then by suggesting the use of deep Q-learning (DQN) algorithms to make the decision process fully automatic. Finally, this technique is narrowed down to use with IoT devices. It was tested and found to be a successful IoT honeypot system. It is capable of learning optimal reward functions, which are "functions that positively compensate any download command and negatively compensate the exit command" (Pauna et al., 2019, p. 509). The ability to self-adapt is a promising improvement to already proven honeypot techniques.

Another study utilized honeypots on a global scale to collect data but then used that data within a framework for modeling and clustering attacker activity. Sun et al. (2019, p. 470) propose this novel framework which "combines a Bayesian probabilistic graphical model and a graph-based clustering algorithm." The Bayesian model uses the attacker activity temporal information with Multivariate Hawkes Process, which is a special type of point process that has found success in prediction modeling and data clustering, to identify latent influence between attackers. By analyzing attacker patterns in this way, they were able to collect meaningful data about attacker behavior and reasonably predict attacker behavior. This data and prediction method could be used to prepare for and detect attacks based on previous behaviors captured by IoT honeypots.

Koroniotis et al. (2019, p. 779) have proposed a Bot-IoT dataset which may be used as "the baseline for allowing botnet identification across IoT-specific networks." The contribution of this dataset will be useful to anyone using testing a signature-based or anomaly-based detection method. It also has applications outside of these methods as it

contains valuable information on network forensics analytics and various botnet scenarios. This data will also be useful for training users, systems, and artificial intelligence to detect a variety of botnet attacks.

DDoS detection and mitigation. Security information and event management (SIEM) based detection and mitigation have shown some potential for IoT-botnet DDoS attacks. According to Al-Duwairi et al. (2020, p. 2186), "SIEM-systems are primarily used in the security field to correlate events reported by various network security defense technologies (e.g., intrusion detection systems, firewalls, bring your own device solutions, operating systems syslogs, etc.) deployed within an enterprise network." Results from this correlation can be used to determine if there is a security incident. This is applied to IoT by forwarding traffic logs to the SIEM system, analyzing them for abnormal behavior, and then alerting network administrators when an attack is detected (Al-Duwairi et al., 2020). This technique is most useful when attempting to detect DDoS attacks that originate from IoT botnets, which are one of the most common attacks performed with botnet devices. It is included here because part of botnet detection and mitigation is detecting and mitigating their attacks.

Another suggestion for mitigating DDoS attacks is to use Software-Defined-Networking/Network-Function-Virtualization (SDNFV). Krishnan et al. (2019) layout an improved SDNFV which integrates with multi-layer cooperative security intelligence to create what they call DDoS Threat Analytics and Response Framework (DTARS). DTARS improves network security against DDoS and other volumetric attacks by expanding the core defense perimeter to a wider, multi-access edge computing (MEC) perimeter. This perimeter allows security to identify these types of attacks closer to their source. DTARS was shown to be a feasible and lightweight framework that is effective at detecting threats.

Yilmaz and Uludag (2019) outline their Minimally Invasive Attack Mitigation via Detection Isolation and Localization (MIAT-MDIL) framework as a means for protecting the smart grid from IoT-based denial of service (DoS) attacks. In their framework, detection is achieved by measuring and identifying anomalies at multiple points in a chain of data transmission. This distributed intrusion detection system (IDS) accomplished speedy detection of threats. Once detection occurs, the system begins to mitigate by localizing the incoming data, disregarding it, and isolating the offending sources until they are secured and operating correctly. The beauty of this system is laid out in their statement that it is "a timely, distributed, scalable, and nonparametric intrusion detection system (IDS)…that is protocol-agnostic and free from data-type assumptions" (Yilmaz & Uludag, 2019, p. 19).

Reddy et al. (2018) classify DDoS attacks by vulnerabilities, behaviors, rate dynamics, and impact and then discuss an existing model to detect and prevent DDoS attacks. Network traffic analysis, via misuse detection or anomaly-based detection, is highlighted as the primary means of identifying DDoS attacks. They also compile a list of DDoS attack tools, used to overcome attacks, including Trin00, Tribe Flood Network (TFN), Stacheldraht, Mstream, and Code Red. They explain their algorithm of detection, defense, and report as following three main steps: 1) "algorithm starts by analyzing the incoming traffic, whether it is normal traffic or DDoS traffic," 2) "if it is DDoS traffic, then it will specify the types of DDoS attacks," and 3) "if the attack is identified, then the algorithm enters into the defensive state" (Reddy et al., 2018, p. 4).

Security best practices. Practicing good cyber hygiene is important for users of all kinds of networks and devices, but it is especially important with IoT devices. There are a few best practices that stand out and should be practiced. First, change the default passwords for these devices. It is often easy to overlook this step and one study has estimated that 80% of IoT devices have a default password set and still in use (Kim et al., 2018; Salim et al., 2020). Second, update firmware and software regularly (Salim et al., 2020). This is a good practice for any device, but again it is often overlooked. Shim et al. (2019, p. 135) reiterate that many IoT devices have "security problems because many users do not download and install security patches for their smart thermostat, doorbell, or baby monitor." A report by Cisco showed that "90% of network devices were running with known vulnerabilities, and there were 28 vulnerabilities per device on average" (as cited in Kim et al., 2018, p. 1). Installing fixes for these vulnerabilities is essential to securing them from attacks. Third, utilize a whitelist-based firewall. Lee et al. (2018) showed how this method was effective at blocking some bad actors and could be updated as needed to protect an industrial network and industrial IoT devices. Fourth, disable any unused or unsecured features or services. One example of this is Telnet which, despite posing well-known security risks, is commonly enabled and utilized on IoT devices (Pauna et al., 2019). Disabling this service in favor of a more secure option, or at least using a strong password and limiting the use of the service, is enough to make meaningful improvements to a device's security.

ISP-side architecture. ISP-side architecture is yet another area where the war against botnets can be waged. Foorsec architecture is one promising example of this area of IoT security. Lauria (2017) explains that this architecture is comprised of six logical modules that work together to footprint, report, and secure compromised IoT devices. The collection of IP addresses is accomplished via external processes such as honeypots, firewalls, etc. Footprinting is then conducted using geolocation and the WHOIS lookup service. Reporting is sent to appropriate contacts via email or another communication method. Finally, security is hopefully achieved by the alerted user or IoT device owner addressing the vulnerabilities of the device(s). Lauria (2017, p. 16) concludes: "Hence, we think that full implementation of the proposed architecture, placed on the ISP side, can both reduce the number of already compromised IoT devices and slow down the spread of IoT botnets, in those scenarios where remote access to customer IoT devices for the purpose of fighting IoT botnets is granted by a legal agreement between customer and ISP."

Deep learning again shows up in the literature when looking into ISP-side architecture. Ko et al. (2019) essentially take the concepts of unsupervised deep learning and stacked self-organizing maps (SOM) and apply them to Netflow data sets collected by ISPs. They were able to successfully develop two methods for analyzing this data. One utilizes Apache Spark to conduct fast and easy distributed computing. The other utilizes a "dynamic feature selection unit…to select a minimal number of features for each layer of SOM" (Ko et al., 2019, p. 3). They were able to use this approach to detect a variety of attacks such as UDP flood, TCP SYN flood, Distributed Reflection Denial of Service (DRDoS), and ICMP flood. In some cases, only the first layer of the SOM was necessary, demonstrating the effectiveness of this method.

User education and attitudes. While many of the reviewed articles do not suggest or detail the best methods to educate end-users and security professionals, some of them do suggest that changing attitudes toward IoT devices and educating their users on how to properly secure them are important steps to securing the devices and their networks. Some of the suggestions that could be derived from the literature include making users aware of the risks associated with IoT devices, educating them on security best practices, and enforcing security when possible. Shim et al. (2020, p. 528) list user awareness as one of "the most critical issues that researchers need to investigate and address." Salim et al. (2020) suggest educating users as an important step in securing IoT devices from DDoS attacks. Enforcing security could include tasks such as requiring strong passwords and disabling risky services by default. In the workplace or another more controlled environment, this can be easier to implement in some cases since there may be less action required by the end-user. In the case of consumer IoT devices, manufacturers should be careful to follow these suggestions rather than merely opting for the cheapest or most convenient option. Furthermore, governments can take steps towards educating the public and passing litigation that requires user education and training as it relates to IoT security (Salim et al., 2020; Shim et al., 2020). Shim et al. (2020) add that some organizations will struggle to meet the security demands associated with IoT growth and should focus on attracting new talent to keep up.

DISCUSSION

A Multi-Layer Approach and Implications

A multi-layer approach. The literature seems to suggest that there are many methods of detecting and preventing IoT-botnet attacks. There also seems to be a consensus, as in other areas of security, that a multi-faceted approach will be more effective than only utilizing one method of protection. Therefore, a multi-layer approach to IoT security is recommended. The suggested multi-layer approach to IoT-botnet detection and prevention consists of three layers (see Figure 1). Beyond the outer layer exists the source of botnet threats (the botnet control server, the attacker, etc.); in the center of the inner layer is the user and/or the IoT device that is the target. The outer layer is primarily focused on the space outside a local network's defense perimeter. The middle layer is primarily focused on interactions occurring near the perimeter and across the network. The inner layer is primarily focused on the user and the preventative actions near the IoT devices themselves. The perimeters can be fuzzy and there may be some overlap in the areas. Some methods will be useful in multiple layers. In the outer layer, we see external detection and protection in the form of ISP-side architecture. There may also be other external architecture that can be improved, but the reviewed literature seems to focus on this single area. The middle layer consists of the detection of botnet malware which may be accomplished through the multiple methods discussed above and the detection and

mitigation of botnet-based DDoS attacks. The inner layer includes efforts to alter user attitudes, user education, and the implementation of security best practices. Existing literature describes IoT as a complex and multi-faceted sector of technology (Shim et al., 2020) and, as such, it needs this multi-layered approach to its security.

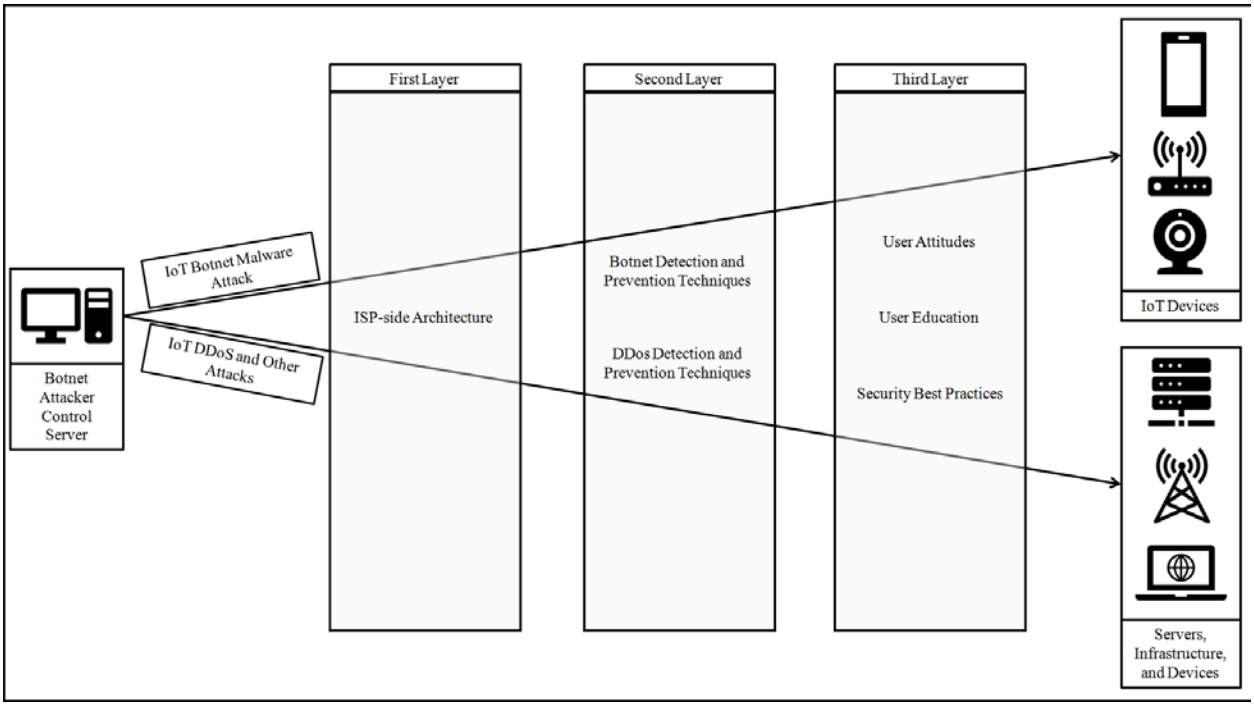

Figure 1. A Multi-Layer Approach to IoT-botnet Detection and Prevention

Implications. For researchers, this collection and review of current literature should serve as a starting point for future research into multi-layer approaches to IoT security. They may also find gaps in this approach that could be filled by new techniques or additional layers. This approach is meant to be a general foundation that can be improved upon. It may be expanded or narrowed in scope. For practitioners, this paper should serve as a guide to the various options for detecting and preventing IoT-botnet attacks. Furthermore, it should illustrate the importance of using more than one method of protection and briefly outline a multi-layer approach that can be tailored to fit an individual or organization's specific needs. For end-users, the hope is that this paper will help to educate them on the risks associated with IoT devices, the importance of IoT security, and some of the methods that may be used to detect and defend against botnet attacks. At the same time, the paper may also help to change the carefree, risky attitudes that are often associated with IoT devices and their vulnerabilities.

Limitations and Future Research

Limitations. The research conducted for this paper was subject to a few limitations. One potential limitation is that there may be more literature relevant to this subject that is either older than the age requirement or not found in the academic database that was utilized. While more recent literature was preferred due to reasons outlined in the research methodology section, expanding the timeframe to five to ten years and further analyzing those articles could reveal some additional insights and contribute to future research. This limitation could be overcome with the proper time and resources allocated for further research. A second limitation is that research in this area of cybersecurity is rapidly changing. As such, it is necessary to continue conducting research, updating current detection and prevention methods, exploring and developing new methods, and disseminating this information quickly to researchers and practitioners. A third limitation is that the bulk of the research reviewed focused on detection, rather than pure prevention or post-attack mitigation. Detection plays a large role in security and is very important for IoT security as well. It is possible, however, that another key to successful botnet prevention lies in protection and post-attack mitigation. Furthermore, an offensive approach to botnets may also need to be explored.

Future research. Playing off of this study's limitations, future research should expand on this work by analyzing older literature, or more general literature relevant to the topic, to find other concepts and techniques that may be useful for this cause, addressing new botnet malware as it arises, and exploring other security methods outside of mere detection. Additionally, some suggestions did not appear to be as well-covered. For example, Salim et al. (2020) suggest that governing bodies should legislate that ISPs provide preventative measures to decrease the amount of DDoS and attacks. Unfortunately, there was no hard data to review for this suggestion in the literature and no guide on how to best accomplish this. Future research could explore areas similar to this where there are fewer data and guidance. A more practical expansion would be to implement the multi-layer approach to IoT security suggested in this paper to find how effective and feasible it is in practice.

Concluding Remarks

IoT technology is, in many ways, a blessing and a curse. The conveniences and improvements it brings into our lives are welcomed wholeheartedly. Unfortunately, with that welcoming comes privacy concerns, security risks, and new vectors for large scale cyber-attacks. IoT-botnets, and associated attacks like DDoS, are one of these unwelcome issues. As IoT continues to expand, botnets will have the potential to become even larger, and, as a result, DDoS attacks could become even more powerful. This is a serious threat that needs to be addressed. In this paper, it is suggested that a multi-layer approach be taken to secure IoT devices from botnet malware and attacks and to detect these attacks when they do occur. Existing methods may be used in each of the three layers to create a more secure Internet, local network, and device. Some more advanced methods in these areas show true promise including neural networking, machine learning, deep learning, and powerful intrusion detection systems; but, even less advanced best practices such as changing default passwords and disabling unused ports and services can be an effective form of prevention. The best methods to use in each layer still need to be researched and debated, but it is clear that no one method is a cure-all for this issue. Instead, security professionals would do well to incorporate multiple methods within the various layers. As IoT grows and its risks evolve, it will become even more important to heed this advice and to adapt to the evolving climate. The approach suggested in this article should be used as a starting point and will hopefully make the world of IoT just a little more secure.

REFERENCES

Al-Duwairi, B., Al-Kahla, W., AlRefai, M. A., Abdelqader, Y., Rawash, A., & Fahmawi, R. (2020). SIEM-based detection and mitigation of IoT-botnet DDoS attacks. *International Journal of Electrical and Computer Engineering, 10*(2), 2182-2191. https://doi.org/10.11591/ijece.v10i2

Celik, Z. B., Fernandes, E., Pauley, E., Tan, G., & McDaniel, P. (2019). Program analysis of commodity IoT applications for security and privacy: Challenges and opportunities. *ACM Computing Surveys, 52*(4), 74.1-74.30. https://doi.org/10.1145/3333501

Cisco annual Internet report (2018–2023) white paper. (2020, March 9). https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

Conti, M., Kaliyar, P., Rabbani, M. M., & Ranise, S. (2020). Attestation-enabled secure and scalable routing protocol for IoT networks. *Ad Hoc Networks, 98*, 102054, 1-12. https://doi.org/10.1016/j.adhoc.2019.102054

Jung, W., Zhao, H., Sun, M., & Zhou, G. (2020). IoT botnet detection via power consumption modeling. *Smart Health, 15*, 100103, 1-17. https://doi.org/10.1016/j.smhl.2019.100103

Kim, H., Kim, T., & Jang, D. (2018). An intelligent improvement of internet-wide scan engine for fast discovery of vulnerable IoT devices. *Symmetry, 10*(5), 151, 1-16. https://doi.org/10.3390/sym10050151

Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection, 25*, 36-49. https://doi.org/10.1016/j.ijcip.2019.01.001

Ko, I., Chambers, D., & Barrett. (2019). Feature dynamic deep learning approach for DDoS mitigation within the ISP domain. *International Journal of Information Security, 19*, 53-70. https://doi.org/10.1007/s10207-019-00453-y

Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2019). Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: bot-IoT dataset. *Future Generation Computer Systems, 100*, 779-796. https://doi.org/10.1016/j.future.2019.05.041

Krishnan, P., Duttagupta, S., & Acuthan, K. (2019). SDNFV based threat monitoring and security framework for multi-access edge computing infrastructure. *Mobile Networks and Applications, 24*(6), 1896-1923. https://doi.org/10.1007/s11036-019-01389-2

Kumar, C. U., & Bhama, P. R. (2019). Detecting and confronting flash attacks from IoT botnets. *The Journal of Supercomputing, 75*(12), 8312-8338. https://doi.org/10.1007/s11227-019-03005-2

Lauria, F. (2017). How to footprint, report and remotely secure compromised IoT devices. *Network Security, December 2017*, 10-16.

Lee, S., Lee, S., Yoo, H., Kwon, S., & Shon, T. (2018). Design and implementation of cybersecurity testbed for industrial IoT systems. *The Journal of Supercomputing, 74*(9), 4506-4520. https://doi.org/10.1007/s11227-017-2219-z

Nguyen, H., Ngo, Q., & Le, V. (2019). A novel graph-based approach for IoT botnet detection. *International Journal of Information Security*, 1-11. https://doi.org/10.1007/s10207-019-00475-6

Nieto, A., Acien, A., & Fernandez, G. (2018). Crowdsourcing analysis in 5G IoT: Cybersecurity threats and mitigation. *Mobile Networks and Applications, 24*(3), 881-889. https://doi.org/10.1007/s11036-018-1146-4

Pauna, A., Bica, I., Pop, F., & Castiglione, A. (2019). On the rewards of self-adaptive IoT honeypots. *Annals of Telecommunications, 74*(7-8), 501-515. https://doi.org/10.1007/s12243-018-0695-7

Reddy, M. C. K., Kumawath, S., Krishna, T. G. S., & Sneha, T. M. (2018). A classification of DDoS attacks and its approach for attack prevention. *i-manager's Journal on Computer Science, 5*(2), 1-7.

Rochford, J. (2019). Accessibility and IoT / smart and connected communities. *AIS Transactions on Human-Computer Interaction, 11*(4), 253-263. https://doi.org/10.17705/1thci.00124

Salim, M. M., Rathore, S., & Park, J. H. (2020). Distributed denial of service attacks and its defenses in IoT: A survey. *The Journal of Supercomputing, 76*, 5320-5363. https://doi.org/10.1007/s11227-019-02945-z

Shim, J. P., Avital, M., Dennis, A. R., Rossi, M., Sørensen, C., & French, A. (2019). The transformative effect of the Internet of Things on business and society. *Communications of the Association for Information Systems, 44*, 129-140. https://doi.org/10.17705/1CAIS.04405

Shim, J. P., Sharda, R., French, A. M., Syler, R. A., & Patten, K. P. (2020). The Internet of Things: Multi-faceted research perspectives. *Communications of the Association for Information Systems, 46*, 511-526. https://doi.org/10.17705/1CAIS.04621

Shorman, A. A., Faris, H., & Alijarah, I. (2019). Unsupervised intelligent system based on one class support vector machine and Grey Wolf optimization for IoT botnet detection. *Journal of Ambient Intelligence and Humanized Computing*, 1-17. https://doi.org/10.1007/s12652-019-01387-y

Sun, P., Li, J., Bhuiyan, M. Z. A., Wang, L., & Li, B. (2019). Modeling and clustering attacker activities in IoT through machine learning techniques. *Information Sciences, 479*, 456-471. https://doi.org/10.1016/j.ins.2018.04.065

Yilmaz, Y., & Uludag, S. (2019). Timely detection and mitigation of IoT-based cyberattacks in the smart grid. *Journal of the Franklin Institute*, 1-21. https://doi.org/10.1016/j.jfranklin.2019.02.011