A FRAMEWORK TO PROTECT IOT DEVICES FROM ENSLAVEMENT IN A HOME ENVIRONMENT

Khalid Al-Begain[1], Murad Khan[1], Basil Alothman[1],
Chibli Joumaa[1] and Ibrahim Rashed[2]

[1]Kuwait College of Science and Technology, Kuwait
[2]Computer Engineering Department Kuwait University, Kuwait

ABSTRACT

The Internet of Things (IoT) mainly consists of devices with limited processing capabilities and memory. Therefore, these devices could be easily infected with malicious code and can be used as botnets. In this regard, we propose a framework to detect and prevent botnet activities in an IoT network. We first describe the working mechanism of how an attacker infects an IoT device and then spreads the infection to the entire network. Secondly, we propose a set of mechanisms consisting of detection, identifying the abnormal traffic generated from IoT devices using filtering and screening mechanisms, and publishing the abnormal traffic patterns to the rest of the home routers on the network. Further, the proposed approach is lightweight and requires fewer computing capabilities for installation on home routers. In the future, we will test the proposed system on real hardware, and the results will be presented to identify the abnormal traffic generated by malicious IoT devices.

KEYWORDS

Botnet, IoT, Malicious Activities, Abnormal Traffic Detection.

1. INTRODUCTION

The applications of IoT spread into different places such as homes, offices, buildings, and other environments. In addition, these devices provide several services such as controlling home appliances in a smart home, remotely monitoring an agricultural farm for humidity, temperature, etc., and industry for automating robots, manufacturing systems and controlling various hardware. As these devices have different services, ubiquity and inconspicuousness become two important characteristics of these devices [1]. Therefore, the attackers always target these devices to gain different advantages, such as launching a DDoS attack on different servers and then asking for ransom. In recent years, IoT devices proliferated in different fields of engineering, health, smart home, and smart cities, and it is estimated that 50 billion devices will be connected within the next few years. Therefore, sophisticated security mechanisms are needed to provide enough security to these devices.

Recently, several solutions to protect IoT devices from enslavement have been presented. For instance, some of these security mechanisms are based on employing deep learning models to train a neural network and then using it to detect the malicious activity pattern in the network traffic originating from the IoT devices. However, such solutions are favourable in those situations when the IoT devices are provided with high processing power and enough memory

David C. Wyld et al. (Eds): SIGEM, MLTEC, SEAPP, ITCON, NATL, FUZZY, CSEA - 2022
pp. 171-178, 2022. CS & IT - CSCP 2022 DOI: 10.5121/csit.2022.122012

[2]. One of the solutions is to make a cluster of the Raspberry Pi and then control the entire home network with these devices [3, 4]. However, in such situations, it would not be easy to maintain the management of the clusters. Lightweight security is a favourable solution for protecting IoT devices from enslavement. One of the reasons is that IoT devices have limited memory and processing power, and therefore, they can easily support lightweight security protocols [5, 6]. However, such solutions are mainly designed for IoT devices which again require extra management on the network layer. Therefore, modifying the network layer protocols requires additional work and management.

In order to handle the issues in neural networks, clusters, and lightweight-based security solutions for IoT, this article presents a security framework for a home environment. The working mechanism of the proposed scheme consists of two main parts; first, an attacker launches an attack to enslave an IoT device by installing malicious code. Similarly, the enslaved IoT device, a bot, infects the other IoT devices within the same network cluster with the same malicious code. Further, the attacker configures the bots to launch a DDoS attack on the victim server. Secondly, we devised a security mechanism to detect abnormal traffic from the bots on the edge router. The edge router is programmed to block abnormal traffic from the bots.

Further, any open port will be blocked to prevent future connections to the IoT devices. Finally, the edge router will share the information about the abnormal traffic with the rest of the routers attached to it.

The rest of the paper is divided into the following parts. Section 2 presents a thorough literature study of the current botnet and related security mechanisms. Section 3 presents the conceptual idea of the proposed scheme. Section 4 presents an overview and brief explanation of the experimentation study. Finally, the conclusions are given in Section 5.

2. RELATED WORKS

In recent literature, researchers suggested a number of techniques to protect IoT devices from malicious attacks. These techniques are based on a number of parameters, such as the processing power, memory, communication range, etc., of the IoT devices. However, it is still challenging to design a generic security system that can incorporate all the above-mentioned parameters. For instance, the authors in [7] focused on tackling the networks of devices that have been infected with malware by modelling the behaviour of malware spread, the classification of malicious traffic, and the analysis of traffic anomalies. This paper introduces a system for ANTicipating botnEts (ANTE) signals based on machine learning techniques. By learning to recognize different forms of botnets throughout their execution, ANTE's architecture allows it to adapt to a variety of circumstances. In order to maximize the accuracy of categorization, ANTE automatically picks the best optimal machine-learning pipeline for each type of botnet. A similar study is presented in [8] to detect botnets using the autoencoder machine learning technique. A large-scale IoT network traffic data is encoded using a long short-term memory auto-encoder in order to minimize the dimensionality of features (LAE). With the use of a deep bidirectional long-short-term memory (BLSTM), the authors propose that it is possible to categorize network traffic samples properly (BLSTM). To validate the efficacy of the proposed hybrid DL technique, extensive experiments were performed on the BoT-IoT data set. A weather station, smart fridge, motion-activated lighting, a remotely operated garage door, and a smart thermostat were among the IoT devices included in the testbed setup. Bot-IoT also includes millions of samples of IoT botnet attack traffic.

As machine learning techniques require a sufficient amount of processing power and memory, therefore, it is only appropriate for IoT devices that have such features and capabilities. For

lower-capability IoT devices that may exist in a variety of home appliances, It is necessary to use other techniques which are faster and require a limited amount of processing power and memory. For instance, a lightweight security scheme is designed to limit network access using segment units set with various device features, network information, and service types [9]. The architecture's capacity to prevent the propagation of threats on the IoT network was validated by the suppression of botnet creation in the botnet creation experiment testbed using the Mirai virus. In the same context, another scheme is presented using a fuzzy logic mechanism to prevent IoT devices from enslavement [10]. This paper proposes a unique approach capable of detecting IoT-Botnet attacks while avoiding the difficulties related to the limitations of knowledge-based representation and binary decisions. The contribution of this research paper is to present a detection method for the IoT-BotNet attack using Fuzzy Rule Interpolation (FRI). These advantages assist the Intrusion Detection System (IDS) in producing more realistic and comprehensive alerts. The suggested technique was used for an open-source BoT-IoT dataset from the Cyber Range Lab at UNSW Canberra Cyber. The proposed technique was assessed and found to have a detection rate of 95.4%, according to the study. Due to its fuzzy nature, it was able to successfully smooth the boundary between regular and IoT-BotNet traffic, and it was able to create the appropriate IDS warning in the case that the knowledge-based representation failed.
Intrusion Detection Systems (IDS) are widely used to handle abnormal traffic and block illegal access to an IoT device [11, 12]. For instance, in [13], the authors proposed a three-layer IDS that detects a variety of prominent network-based cyber-attacks on IoT networks using a supervised method. The system is capable of classifying the type, profiling the usual behaviour of each IoT device, and determining the sort of attack that has been launched. The system is tested in a smart home testbed that includes eight prominent commercially accessible devices. The effectiveness of the proposed IDS architecture is assessed by deploying 12 attacks from four major network-based attack categories. The system is also tested against four multistage attack scenarios with complicated event chains. As this system is based on supervised learning, there is a fair chance that the system will respond in a significantly large amount of time if a greater number of IoT devices are connected to the home network. One way to avoid the use of supervised learning is to perform IoT botnet isolation and detection on access-level routers that enable automated detection of unprotected IoT devices, isolation based on the access router's internal firewall, an update mechanism based on a CVE online service, and self-optimizing scanning [14]. The researchers used two testbeds to perform a quantitative evaluation of the proposed approach using both virtual and real hardware devices.

The paper [15] presents an IoT botnet testbed that emulates IoT devices in a DETER-lab-based infrastructure (NCL). It has all the ancillary services like a DNS, CNC, ScanListen/loader, and a victim server that a botnet needs for full operation. The paper showcased a virtualization method using (QEMU) by emulating a Raspbian OS with limited and fixed resources for each emulated device. There were 10 IoT-emulated devices connected to gateways and routers in a contained environment. The botnet used for experimentation was "Mirai", whose source code was altered to remove the errors faced in the emulated environment. All the technical details about setting up the testbed were shown, and validation of the testbed was achieved by using a UDP flood and TCP SYN flood attack on the testbed's victim server and monitoring the packet traffic to see disruption of the victim server upon being attacked.

The proposed approach presented in this paper is similar in principle to the system presented in the above-mentioned manuscript. However, the major difference between our proposed scheme and [15] is our scheme is a lightweight one. In addition, we also consider the home edge router's limited memory and processing power when scanning and detecting the network traffic. Also, the knowledge gained by a home edge router is published with the rest of the routers to reduce the time for processing and to detect abnormal traffic patterns.

3. PROPOSED SCHEME

The working of the proposed scheme is further divided into two phases: 1) DDoS Attack Phase and 2) DDoS Attack Detection and Prevention Phase.

3.1. DDoS Attack Phase

In the attack phase, an attacker infects a smart home device, such as a washing machine, refrigerator, etc., by scanning for open ports using or performing a brute force attack on random IP addresses. As soon as the attacker finds an open port, it establishes a connection to the smart home device to inject the malicious code. The attacker later uses this malicious code to launch a DoS attack from the infected device. Similarly, the infected devices distribute the malicious code with the devices attached to the same network. The spreading of infection to other devices is continued until all the devices on the home network are infected. The attacker also uses the switch/router attached to other switches and routers for spreading the infection to other home networks via an infected device. The infected devices have the functionality of automatically scanning the network for other devices, and as soon as they find any other device, they infect them by sending them the malicious code. Similarly, these infected devices, which are also called bots, can perform a number of activities, such as scanning other devices on the network, sending malicious codes to the infected devices, sending spam emails, and can launch an attack. The entire working mechanism of the DDoS attack phase is presented in Figure 1.

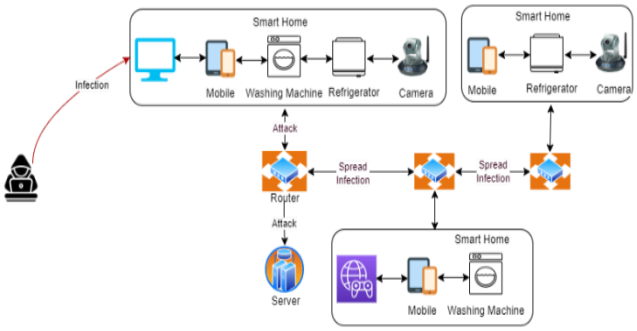

Figure 1. The attack scenario

Fig 1. shows the mechanism of how an attacker infects a device and then spreads the infection to the network.

3.2. DDoS Detection and Prevention Phase

In the prevention phase, the home router uses a set of mechanisms to block the DDoS attack launched by the bots. As we already discussed, it is difficult and time-consuming to add neural network models to identify any malicious traffic generated from home devices. Also, neural networks always require huge amounts of data to be trained to differentiate between legitimate and abnormal traffic. We also know that home routers are always available with limited processing and programming capabilities. Therefore, it would be difficult to program and configure them with neural network capabilities. In order to deal with the abnormal traffic generated by the bots, we divided the working mechanism into the following steps.

3.2.1. Detection

In order to detect the abnormal traffic generated by the bots, each packet distant from a server is checked for the destination IP address. Further, a counter on the destination IP addresses will be set. If, for a particular destination IP address, the counter exceeds a pre-defined threshold, then the traffic will be considered abnormal. In a similar context, each device that generated similar traffic will be blocked.

3.2.2. Filtration

One of the possibilities in the case of step 1 is that there are difficulties in differentiating between normal and abnormal traffic. In this regard, we developed a filtration mechanism based on defining various thresholds similar to step 1. However, the difference between the threshold used in step 2 is that there legitimate and abnormal traffic can be classified into two separate categories. Finally, the outcome of the filtration step will help in traffic classification and separation between normal and abnormal traffic.

3.2.3. Screening

In this step, all the logs and entries saved in the home devices and the home router are checked regularly to avoid any possible attack in the future. It also helps in identifying malicious actions by comparing the logs of normal and abnormal traffic.

3.2.4. Publishing

In order to reduce the processing time on the rest of the routers attached to the current router, the current router shares the malicious actions information with the routers attached to it via a wired connection. However, we also programmed the rest of the routers to repeat steps 1 to 3. Further, adding the information from the current router may also help in identifying the malicious code as quickly as possible. One of the main reasons for publishing the information to other routers is to deal with malicious traffic and prevent the DDoS attack in the early stages.

Finally, the mechanism of detection and prevention of the DDoS attack is given in Figure 2. The proposed idea of the prevention of the possible DDoS attack is simple and requires less amount of time to process the packets from infected devices. Also, the malicious network traffic generated from the bots is handled and blocked. These bots are also identified, and the open ports used by the attacker are closed for any suspicious connections.

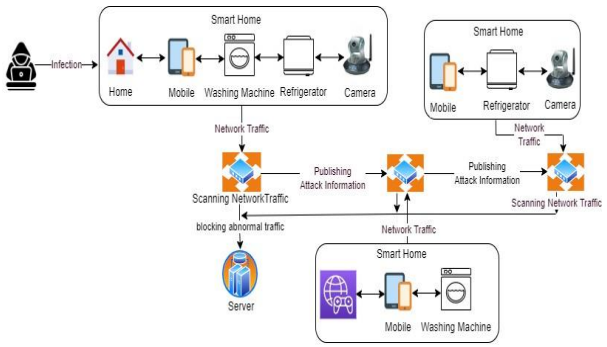

Fig 2. Prevention of DDoS attacks from infected home devices

4. RESULTS AND DISCUSSION

In this article, we present a conceptual idea of our proposed DDoS prevention system for home environments. To validate the proposed system, a fully isolated testbed is set up at the Network Security Laboratory at KCST to inject the malicious code into the home network by brute forcing all the available ports to establish a connection. For this purpose, we will set up different Raspberry PI with variable configurations connected to a home router to emulate the different IoT devices embedded in the different home appliances. The traffic generated from each home device will be scanned to detect abnormal traffic for a specific period and a specific destination address. If the home devices are sending data to a common destination IP address, then the traffic will be classified as abnormal traffic. The abnormal traffic will be discarded, and all the open ports will be closed. A snapshot of the system is presented in Figure 3.

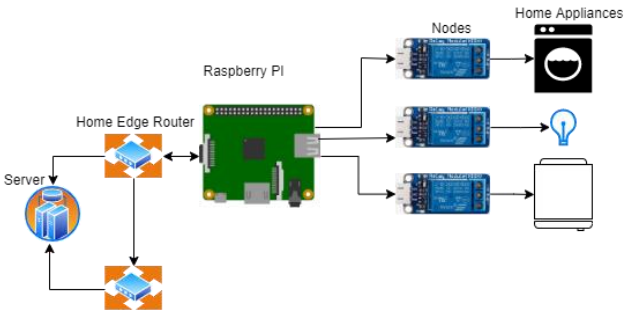

Fig 3. A testbed scenario of the proposed system.

5. CONCLUSION

This paper provides a framework for injecting malicious code into an IoT network to enslave home devices. Further, a detection mechanism is devised to scan the traffic originating from the home devices for possible malicious activities. As soon as a malicious activity, i.e., a DDoS attack, is detected by the home router, the traffic coming from the home devices is blocked, and the results are published to the routers connected to the current router. This is a light weighted solution that could be useful for home devices and routers with limited processing capabilities. In the future, we are planning to set up a similar structure using real hardware and testbed in the form of Raspberry Pi and home routers.

ACKNOWLEDGEMENT

The paper is a result of the project, which is fully funded by the Kuwait Foundation for Advancement of Science (KFAS) under Project No. (PR17-18QI-03).

REFERENCES

[1] B. N. Silva, M. Khan and K. Han, "Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities," *Sustainable Cities and Society*, vol. 38, pp. 697-713, 2018.

[2] B. Jan, H. Farman, M. Khan, M. Imran, I. U. Islam, A. Ahmad, S. Ali and G. Jeon, "Deep learning in big data analytics: a comparative study," *Computers & Electrical Engineering*, vol. 75, pp. 275-287, 2019.

[3] K. Doucet and J. Zhang, "Learning cluster computing by creating a Raspberry Pi cluster," in *Proceedings of the SouthEast Conference*, 2017.

[4] J. Coelho and L. Nogueira, "Enabling Processing Power Scalability with Internet of Things (IoT) Clusters," *Electronics,* vol. 11, no. 1, p. 81, 2021.
[5] R. Fotohi and H. Pakdel, "A lightweight and scalable physical layer attack detection mechanism for the internet of things (IoT) using hybrid security schema," *Wireless Personal Communications,* vol. 119, no. 4, pp. 3089-3106, 2021.
[6] V. Rao and K. V. Prema, "A review on lightweight cryptography for Internet-of-Things based applications," *Journal of Ambient Intelligence and Humanized Computing,* vol. 12, no. 9, pp. 88358857, 2021.
[7] A. B. de Neira, A. M. Araujo and M. Nogueira, " Early botnet detection for the internet and the internet of things by autonomous machine learning," in *16th International Conference on Mobility, Sensing and Networking (MSN)*, 2020.
[8] S. I. Popoola, B. Adebisi, M. Hammoudeh, G. Gui and H. Gacanin, "Hybrid deep learning for botnet attack detection in the internet-of-things networks," *IEEE Internet of Things,* vol. 8, no. 6, pp. 4944 - 4956, 2020.
[9] J. Lim, S. Sohn and J. Kim, "Proposal of Smart Segmentation Framework for preventing threats from spreading in IoT," in *International Conference on Information and Communication Technology Convergence*, 2020.
[10] M. Al-Kasassbeh, M. Almseidin, K. Alrfou and S. Kovacs, "Detection of IoT-botnet attacks using fuzzy rule interpolation," *Journal of Intelligent & Fuzzy Systems,* vol. 39, no. 1, pp. 421 - 431, 2020.
[11] A. R. Khan, M. Kashif, R. H. Jhaveri, R. Raut, T. Saba and S. A. Bahaj, "Deep learning for intrusion detection and security of Internet of things (IoT): current analysis, challenges, and possible solutions.," *Security and Communication Networks,* vol. PP, p. 1, 2022.
[12] Y. Otoum, D. Liu and A. Nayak, "DL-IDS: a deep learning–based intrusion detection framework for securing IoT," *Transactions on Emerging Telecommunications Technologies,* vol. 33, no. 3, p. e3803, 2022.
[13] E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos and P. Burnap, "A supervised intrusion detection system for smart home IoT devices," *IEEE Internet of Things,* vol. 6, no. 5, pp. 9042 - 9053, 2019.
[14] C. Dietz, R. L. Castro, J. Steinberger, C. Wilczak, M. Antzek, A. Sperotto and A. Pras, "IoT-botnet detection and isolation by access routers," in *9th International Conference on the Network of the Future (NOF)*, 2018.
[15] A. Kumar and T. J. Lim, "A secure contained testbed for analyzing IoT botnets," *International Conference on Testbeds and Research Infrastructures,* pp. 124 - 137, 2018.

AUTHORS

Khalid Al-Begain is the founding President of Kuwait College of Science and Technology. He served as the President of the European Council for Modelling and Simulation (ECMS) (20062018) and as President of the Federation of European Simulation Societies (EuroSim) (2010-2013). He was the co-founder and chairman of the first National Welsh Industrial Cyber Security Summit in Newport, UK, in 2014, organized jointly with Airbus, General Dynamics and the UK NCSC. He worked in many organizations and countries, including Hungary, Jordan, Germany and the UK, where his last position was as a Professor of mobile networking at the University of South Wales and Director of the Centre of Excellence in Mobile applications and Services. He won numerous awards, including the John von Newman Computer Award (1986) and the Inspire Wales Award for Science and Technology (2013). In 2006, he received Royal Recognition from Her Majesty Queen Elizabeth II for his contributions to the British scientific community. He supervised 28 successful PhD projects and examined 28 PhDs. Over the years, he led many major national projects securing over GBP20 million in funding for research and consultancy. He registered two granted patents, authored two books and edited 26 books, in addition to over 200 papers in refereed journals and conferences. He was the general chair of 31 international conferences.

Murad Khan received a BS degree in computer science from the University of Peshawar, Pakistan, in 2008. He has completed his Master's and PhD degrees both in computer science and engineering from the School of Computer Science and Engineering in Kyungpook National University, Daegu, Korea. Dr. Khan is currently

working as an assistant professor at the Kuwait College of Science and Technology, Kuwait. Dr. Khan also served as Brain Pool Fellow at Kyungpook National University, Daegu, Korea, from December 2019 to December 2021. Dr. Khan published over 100 International conference and Journal papers along with two book chapters and is an editor of books in Springer and CRC Press. Dr. Khan served as an editorial member of various special sections in world-renowned journals such as Computer & Electrical Engineering, Transactions on Emerging Telecommunications Technologies, etc. He also served as a TPC member in world-reputed conferences and as a reviewer in numerous journals such as IEEE Communication Magazine, Future Generation Computer Systems, IEEE Access, etc. His area of expertise includes ad-hoc and wireless networks, architecture designing for the Internet of Things, Communication Protocols designing for smart cities and homes, Big Data Analytics, etc. Email: m.khan@kcst.edu.kw URL: https://www.kcst.edu.kw/default/viewpeople?id=3

Basil Alothman joined Kuwait College of Science and Technology (KCST) as Assistant Professor at Computer Science and Engineering Department. Dr. Basil graduated from De Montfort University, Leicester, UK, with a PhD in Computer Science. He received his MSc in Computer Science from the University of Hertfordshire, UK and his BSc in Computing and Information Systems from the University of Dubai, UAE. Dr. Basil is mainly interested in cybersecurity science or, more specifically, computer and network security issues, mobile security, computer privacy, OSINT, reverse engineering, cloud and VM security, big data security, IoT security, and Botnet detection techniques.

Chibli Joumaa has been an Associate Professor of Computer Engineering in the Faculty of Engineering and Computer Science of the Kuwait College of Science and Technology (KCST) since April 2020. In addition to his role in the Computer Science and Engineering department, he oversees accreditation-related processes in collaboration with the coordinators, dean, and President. He has previously occupied several teaching, administrative, and managerial positions in reputed educational institutions. Dr. Chibli Joumaa holds a bachelor's and master's degree in electrical engineering from the University of Balamand in Lebanon in 2004 and a master's in Network Telecommunication and System Architecture from France in 2005. He received his PhD in Computer Engineering from the University of Technology of Belfort-Montbeliard, France, in 2010. He is the author of many publications and has attended many professional training and workshops for accreditation and academic advancement.

Dr. Ibrahim Rashed Ebrahim Alrashed received his PhD and MS degree in computer engineering from The University of Southern California, Los Angeles, CA in 1997 and 1993. Since 1997 he has been a faculty member in the department of computer engineering at Kuwait University where he is currently an associate professor. His research interests includes network security, mobile and wireless networks, cloud and edge computing and blockchain.