Use of Honeypots for Mitigating DoS Attacks targeted on IoT Networks

Anirudh M
Department of Computer Science and Engineering,
SSN College of Engineering
Kancheepuram,
anirudhm426@gmail.com.

Arul Thileeban S
Department of Computer Science and Engineering
SSN College of Engineering
Kancheepuram,
arulthileeban023@gmail.com.

Daniel Jeswin Nallathambi
Department of Computer Science and Engineering,
SSN College of Engineering
Kancheepuram,
danieljeswin@gmail.com.

***Abstract*—Every day, a new technology comes up and the primary reason why it fails to attract many people in this era is the concern of privacy and security. Each day, along with the new technology comes a load of vulnerabilities waiting to be exploited. IoT (Internet of Things) is the latest trend and like all technology, it is open for exploitation. The most common attack which is used to bring down a whole network, without even finding a loophole in the security – DoS can be used to pull down any IoT network as well. In this paper, we propose a honeypot model for mitigating DoS attacks launched on IoT devices. Honeypots are commonly used in online servers as a decoy to the main server so that the attack is mitigated to the decoy instead of the main server. Here a similar methodology is used to avoid the whole IoT system from being shut down due to a DoS attack.**

Keywords—Internet of Things, Denial of Service, Honeypot, IoT Security, Security breach.

I. INTRODUCTION

Denial-of-Service (DoS) attack is a type of attack which is used to temporarily or indefinitely shut down the system/network thus disallowing the intended users to access it. It is achieved by pinging the system with a load of spam requests which the system won't be able to handle i.e. the system's processing power will be limited, and loading it with a lot of spam requests will tend to overload and crash it. It is achieved through various methods, the most famous of them being botnets and buffer overflow vulnerability. The most common victims of DoS attacks are high profile organizations such as banking and government organizations which tend to have significant and highly confidential information. The DoS attacks cost them a great deal of time and money apart from loss of data. Though there are many methods or software fixes to avert such attacks, new DoS attacks are being constantly introduced due to ever-growing advancements in the field of hacking.

Internet of Things (IoT) is a recently evolved technology that has taken the world by a storm. Basically, an IoT system consists of several interrelated computing devices, sensors, RFID tags, etc. that are connected to a main server through the internet enabling transfer of data and information without human intervention. Since it is built on the internet the devices of the system need not be in close proximity with each other. The tremendous growth of the internet has enabled IoT's rapid growth and today IoT systems find applications in a variety of fields such as home automation systems, military surveillance systems, sustainable agriculture, healthcare, manufacturing, smart cities and so on. With all the advancements that have been made in the field of IoT over the past years' security issues have been a major concern that has hampered the usage of IoT systems in certain critical fields such as warfare, military surveillance, etc. Since they are built on top of the internet, IoT systems are extremely vulnerable to malicious attacks. One of the several possible attacks on IoT systems, Denial of Service (DoS) attack, is being dealt with in this paper. DoS attacks have been a nightmare for communication networks in general over the years and they pose a major security threat to IoT systems as well. Citing an example here, one major use of IoT is home automation systems. If an attacker attacks the main server of such a system with a DoS attack, the whole system tends to shut down and any appliance within the whole house, sometimes even door locks are rendered inaccessible. This small example shows the significance of security implementation in IoT. In this paper we present a solution to the problem of DoS attacks on IoT systems by using honeypots to divert the attacks as well as capture information about the attacker.

Honeypot is a system which is used to mimic the main system by luring potential hackers who seek to gain unauthorized access to information systems. It is used to study activities, traces left by hackers and to rectify the systems securities in order to prevent future attacks. Generally, it consists of a computer, applications and data that simulate the behavior and acts as a decoy. It is usually a part of firewall so that they can be controlled easily. Based on the design and deployment, honeypots are classified as either production or research honeypots. Research honeypots are run to have a detailed study about the intruder and safety security measures while production honeypots are placed in production network to serve the role of a decoy as part of intrusion detection system (IDS). While Ed Tittel *et al* [8] describes innumerable security measures for preventing and handling attacks using honeypot in various web servers, using honeypot to prevent

978-1-5090-3716-2/17/$31.00 ©2017 IEEE

DoS attacks in IoT is still a 'yet-to-be researched' topic. In this paper, we present a solution how honeypot pillared with a verification system is used to secure an IoT system.

II. Related works

Honeypots have been researched extensively in the past. Several models using honeypots have been proposed for security against various attacks. Sherif M. Khattab *et al* [1] studies the usage of roaming honeypots to mitigate distributed DoS attacks. A random set of servers' is used as honeypots at any given time making it difficult for hackers to find and shut down the honeypots thus enhancing the performance of the system against attacks. Theodor Richardson *et al* [2] describes a technique of using masquerading honeypots to protect back-end servers from attacks. Sherif Khattab *et al* [3] extends the work done in [1] to propose a scheme of honeypot back-propagation to backtrack and find the source of the DoS attack thus further increasing defence mechanisms against DoS attacks. All the above mentioned works the focus is not on mitigating DoS attacks on IoT networks.

With regard to DoS attacks on IoT we would like to highlight the research undertaken and the ideas proposed to deal with this disastrous attack. Sudip Misra *et al* [4] proposes learning automata based approach to deal with DoS attacks in IoT systems. A Learning Automata(LA) based approach is used to build a DDoS prevention strategy in IoT systems built on Service Oriented Architecture (SOA). There has also been research previously undertaken into the usage of honeypots to mitigate DoS attacks in IoT systems. However, at the present juncture this research remains theoretic with only theoretic models being proposed. The practical implementation of honeypots in IoT systems for the purpose of DoS attack prevention is an avenue that remains unexplored. C. Scott *et al* [10] demonstrates a layered approach for securing Supervisory Control and Data Acquisition (SCADA) network using honeypots. Quang Duy La *et al* [5] proposes game theoretic model in which both the attacker and defender try to deceive each other. The defender uses honeypots to deceive and trap the attackers. This research is an extension of the work done by N. Garg *et al* [7] that analyses the effectiveness of using honeypots for deception in networks following a game-theoretic approach. As mentioned previously these works have been confined to theoretic models. With this in mind, we deploy a honeypot based security system for an IoT system in this paper, to block DoS attacks from malicious attackers and also collect information on the attacker so that future attacks might be prevented.

III. DoS attacks in IoT system

The last couple of decades have witnessed the growth of the internet into a global communication platform that has changed our perspective on how we communicate and do business with people around the world. As of Dec 2015 nearly 3.4 billion people worldwide (nearly 46% of the world's population) have access to internet connection. This tremendous growth of the internet has also led to the development of IoT (Internet of Things) which is a network of interconnected wireless devices such as mobile phones, RFID, sensors and so on. The great advantage of IoT is that the devices interconnected need not be homogenous. The communication protocols between each device need not be the same. This could enable IoT to have far reaching effects in various fields such as home automation systems, military surveillance systems, sustainable agriculture, healthcare, manufacturing and so on. IoT can and is making the dream of smart cities and driverless cars a reality.

In IoT based networks new devices that enter the network are configured automatically due to its open nature. This leaves such networks prone to a lot of attacks as described by Weizhe Zhang *et al* [6]. Moreover, since the communication protocols between devices vary, protocols with weaknesses could be exploited by attackers. Such attackers could get hold of sensitive data carried over these protocols. Since most of the IoT based systems are deployed in important and critical processes data privacy is extremely important. Sensitive data passed between devices in the network should not fall into the wrong hands. Attacks on IoT based networks are divided into three categories which are attacks against the front-end devices such as the sensors in the network, attacks against the communication channels between the devices and the servers and lastly attacks against the servers.

As discussed earlier a denial of service attack is one by which the attacker floods the network with numerous spam requests exceeding the handling capacity of the server thus preventing requests from legitimate clients in the network from getting processed. DoS attacks can be launched through various methods/exploits all targeted at denying service to legitimate clients by either overloading the connection handling or processing capability of the server. The open nature of IoT makes it relatively easy for spammers and attackers to infiltrate IoT networks and launch DoS attacks. C. Kwon *et al* [9] shows that such attacks could ultimately cause the server to crash and hence paralyze the network. This could have far reaching consequences depending on the purpose of the network.

Generally, these kinds of attacks are concentrated towards the main server rather than the individual devices connected in the system. The main reason is that it is easier to access the main server rather than the individual devices because the protocol for data transmission in each device might be configured differently and also another main reason is that, by crashing the main server, the whole system is supposedly shut down since another potential user can't access the main server to link to any other device.

978-1-5090-3716-2/17/$31.00 ©2017 IEEE

IV. PROPOSED MODEL

In the proposed model, the system works in two states as depicted in the below diagrams.

A. *Primary Scenario*

Fig. 1 depicts that all requests from clients are passed to the IDS (Intrusion Detection System). Legitimate requests from clients pass through the IDS onto the server. If the IDS detects any anomalies in the requests (Example: Spam requests to initiate a DoS attack), the requests are passed onto the honeypot and the information related to the attacker (IP Address, MAC Address, etc.) are stored as logs in a database.

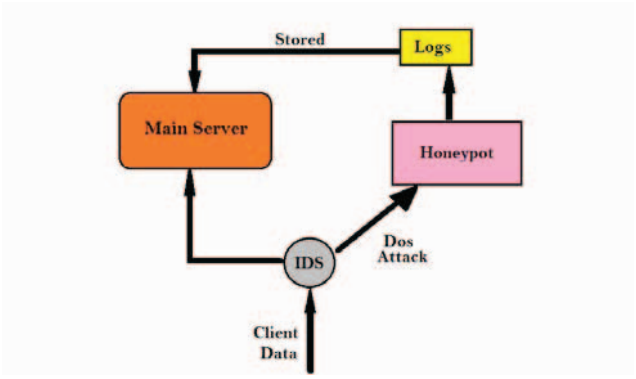

Fig. 1 Primary scenario

B. *Secondary Scenario*

In Fig. 2, there is a collection of logs stored in this case unlike the primary scenario. When a request reaches the IDS, the information of the client is checked with the logs and if it matches, a verification request is shown to the client which checks if it is a spam client and then blocks the client completely off the server if verification fails. Otherwise, if the client passes the verification, the data sent is passed onto the server.

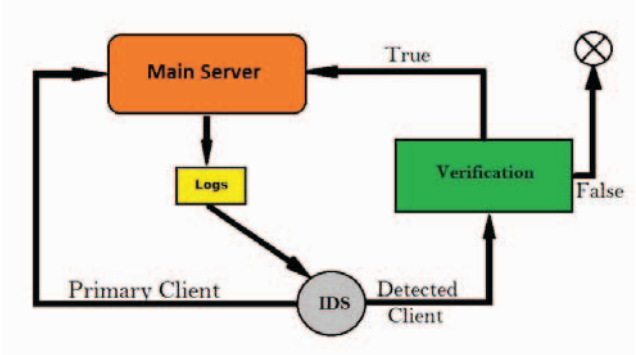

Fig. 2 Secondary Scenario

V. SIMULATION RESULTS

The simulation is built in python using a socket server client model. It replicates an IOT model by having a central server and various nodes linked to it. The clients send in data at varied time periods. The data is just simulated data of constant size so that calculation of efficiency is made simpler. The server collects it and uses it for processing. It acts as a representation of an IOT model which collects various information like temperature, humidity, pressure, etc. The simulation has a variation of number of nodes (bots) from 0 to 100 in steps of 10. The simulation for the proposed model is built and the efficiency is tested here i.e. ratio of data transmitted from client in total to the data received in the server. It is tested in both scenarios with the implementation of the proposed model and without the implementation of the proposed model, with the statistics recorded in Table. 1. This statistical information has also been plotted in the form of a graph and shown in Fig. 3.

TABLE 1
ANALYSIS OF IOT SYSTEM WITH/WITHOUT HONEYPOT

No of Bots	Efficiency with Honeypot (%)	Efficiency without Honeypot (%)
10	99.64	42.17
20	99.24	41.25
30	98.79	41.21
40	98.3	39.09
50	97.75	37.82
60	97.14	36.42
70	96.47	34.88
80	95.73	33.18
90	94.92	31.31
100	94.04	29.29

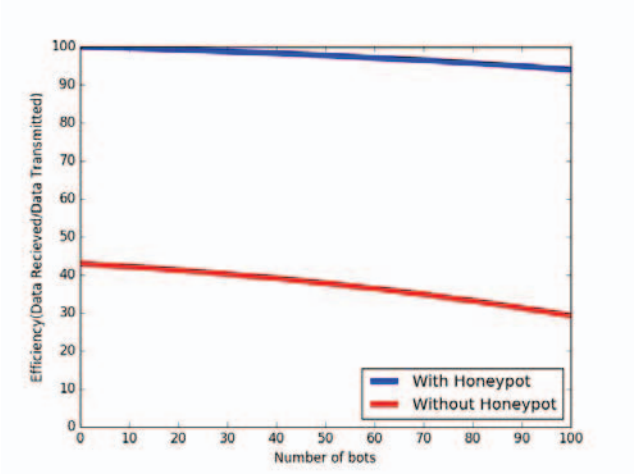

Fig. 3 Behaviour of the IoT system

Fig 3. gives us the complete analysis of the behavior of the IoT system with and without the honeypot. Based on the simulation, the efficiency is calculated at both scenarios and plotted in form of a graph with the x-axis containing number of bots and y-axis containing efficiency and plotted in a scale of 10 units in both axes. This figure clearly shows that there is

978-1-5090-3716-2/17/$31.00 ©2017 IEEE

an increase of 55 to 60% in efficiency when a honeypot is implemented.

VI. Conclusion

Denial-of-Service (DoS) attacks have been a major threat to various networks and systems for years. This paper provides a detailed study of how DoS attack in an IoT system is averted by honeypot system pillared with a verification system to maintain the efficiency (data received/data transmitted). And the simulation results account for the efficiency of the proposed model.
Therefore, outcomes of this work demonstrate the capability of our proposed scheme for implementing honeypot to secure an IoT system.

Future works would be to collect and analyze results for the proposed model implemented in a real-time environment with various microcontrollers interfaced with a central server. This idea of deploying honeypots to handle DoS attacks could also be extended, by deploying a honeypot system which is capable of handling DDoS attacks using botnets, since the verification system for this model might prove incapable there. Moreover, the use of honeypot could be extended for other types of attacks as a research based honeypot to collect details.

REFERENCES

[1] Sherif M. Khattab, Chatree Sangpachatanaruk, Daniel Moss´e, Rami Melhem and Taieb Znati "Roaming Honeypots for Mitigating Service level Denial-of-Service Attacks" in 24th International Conference on Distributed Computing Systems, Mar. 2004, pp. 328–337.

[2] Theodor Richardson "Preventing Attacks on Back-End Servers using Masquerading/Honeypots" in Seventh ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, Jun. 2006, pp. 381–388.

[3] Sherif Khattab, Rami Melhem, Daniel Moss´e, and Taieb Znati "Honeypot Back-propagation for Mitigating Spoofing Distributed Denial-of-Service Attacks" in 20th IEEE International Parallel & Distributed Processing Symposium, Apr. 2006, pp. 8-8.

[4] Sudip Misra, P. Venkata Krishna, Harshit Agarwal, Antriksh Saxena and Mohammad S. Obaidat "A Learning Automata Based Solution for Preventing Distributed Denial of Service in Internet of Things" in 4th IEEE International Conference on Cyber, Physical and Social Computings, Oct. 2011, pp. 114-122.

[5] Quang Duy La, Tony Q. S. Quek, Jemin Lee, Shi Jin, and Hongbo Zhu "Deceptive Attack and Defense Game in Honeypot-enabled Networks for the Internet of Things" in IEEE Internet of Things Journal, vol. 3, no. 9, Feb. 2016, pp. 1-1.

[6] Quang Duy La, Tony Q. S. Quek, Jemin Lee, Shi Jin, and Hongbo Zhu "Deceptive Attack and Defense Game in Honeypot-enabled Networks for the Internet of Things" in IEEE Internet of Things Journal, vol. 3, no. 9, Feb. 2016, pp. 1-1.

[7] Quang Duy La, Tony Q. S. Quek, Jemin Lee, Shi Jin, and Hongbo Zhu "Deceptive Attack and Defense Game in Honeypot-enabled Networks for the Internet of Things" in IEEE Internet of Things Journal, vol. 3, no. 9, Feb. 2016, pp. 1-1.

[8] W. Zhang and B. Qu, "Security architecture of the Internet of Things oriented to perceptual layer" in Int. J. Comput. Consum. Control, vol. 2, no. 2, Jun. 2013, pp. 37–45.

[9] N. Garg and D. Grosu, "Deception in honeynets: A game-theoretic analysis" in Proc. IEEE Workshop on Information Assurance, Jun. 2007, pp. 107–113.

[10] "The Honeynet Project, Know Your Enemy: Learning about Security Threats", 2nd ed. Addison-Wesley Professional, May 2004.

[11] C. Kwon, W. Li, and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception attacks" in Proc. American Control Conference, Jun. 2013, pp. 3350–3355.

[10] C. Scott, "Designing and implementing a honeypot for a SCADA network" in SANS Institute Reading Room May.2014[Online].Available:http://www.sans.org/readingroom/whitepapers/detection/designing-implementing-honeypot-scadanetwork-35252.

978-1-5090-3716-2/17/$31.00 ©2017 IEEE