ISSN 2395-1621

A Survey on Various Security Models

[#1]Tushar Joshi, [#2]Mohnish Deshpande, [#3]Hare Ram, [#4]Sumesh Dhar,
[#5]Prof. Santosh Darade

[1]tusharjoshi789@gmail.com
[2]deshpandemohnish@gmail.com
[3]Hareram149@gmail.com
[4]umeshdhar1995@gmail.com
[5]daradesantosh@gmail.com

[#12345]Department of Computer Engineering

Sinhgad Institute of Technology and Science, Narhe, Pune.

ABSTRACT

A comprised control system can have security, public safety, industrial and economic consequences coupled with human induced failures risk the entire network infrastructure. Network monitoring systems play a significant part in protecting control systems. Honeypots are classic examples of deception, a strategy in warfare used to intentionally mislead the opponent into doing actions in one's favour. They can be physical or virtual devices that provide heavy monitoring and activity logging, which can help to waste attacker's time and resource but helping the defender to study and device various counter measures. Deploying honeypots in systems, the defender can lure attackers into these targets meanwhile allowing to study the type of attacks used and intercept them. Honeypots not only monitor normal accesses but also website accesses by search engine crawlers. Therefore, it becomes important to classify the types of attacks from all these different sources but in doing so, it is becoming increasingly difficult with the growth in network traffic. So, it usually requires a mode of automation to identify malicious intrusions. So, dynamic virtual honeypots are effective tools to observe and attract network intrusion activity. This type of system has the benefit of little human input but can readily adapt to changes in operational network environment.

ARTICLE INFO

Article History

Received: 3rd January 2017

Received in revised form :

3rd January 2017

Accepted: 9th January 2017

Published online :

9th January 2017

Keywords: **virtual honeypot, intrusion detection, network monitoring**

I. INTRODUCTION

Many modern complex control systems are interconnected via Ethernet networks. A compromised control system could have security, public safety, industrial or economic consequences [1],[2]. Network security monitoring systems are a significant part of a solution to protecting control systems. In most contexts, they are rarely capable of providing perfect intrusion detection [7], [8]. It is difficult to list the definitive attributes of a network host necessary to attract an attacker's attention .Prevention of web-based attacks is a challenging and essential task for realizing secure network systems. . In other words, detecting attacks using known vulnerabilities is insufficient for preventing all web-based attacks. Honeypots monitor not only malicious accesses but also normal accesses such as crawler accesses by search engines.

Nowadays, with the exception of the big values that the IoT brings, there also are growing considerations regarding security risks that accompany it, particularly the threats of cyber-attacks. Another recent article [4] reportable that a quest Protea cynaroides designed to collect knowledge regarding attacks on industrial management systems had fully fledged 4000 attacks in just three days. Scientific theory provides an appropriate framework to check the higher than attack and defense drawback. it's long been applied to network security [9], [10]. Whereas most of the same works targeted on the deceptive ways of defenders, specifically the way to minimize the likelihood of getting a true system vulnerable, attackers usually were shapely as having fixed, simple actions like generic attacks, probes and withdraw.

Low-interaction honeynet [1] represents a solution where several interconnected systems serve as a lure for attackers. Each honeypot is located in a specific network (and connected via the network to the Internet) and shares

the data on attacks that it records to a central server (e.g. via XMPP protocol). The centrally gathered data is stored in a database and later subjected to an analysis.

Dionaea honeypot, i.e. medium-interaction honeypot emulating Windows services, has been used for this study. The following protocols were emulated for this research: TFTP protocol on port 69, FTP – A simple FTP server is provided on port 21 with file download and upload functions, Server Message Block (SMB)1 protocol on the port 445, MSSQL – Tabular Data Stream protocol that is used by Microsoft SQL Server was active on port 1433, MySQL – Dionaea emulates the MySQL wire stream protocol on port 3306, SIP – VoIP emulation is done via SIP protocol and Connections on other ports were recorded using NFQ module.

Although private and scientific information have an enormous value for an attacker, the user privacy for legal and ethical reasons must be respected by the Chief Security Officer (CSO). Scientific networks are a special and interesting case; in one hand there is a strong demand of security in the network and the resources and services which are listening. Although private and scientific information have an enormous value for an attacker, the user privacy for legal and ethical reasons must be respected by the Chief Security Officer (CSO). Scientific networks are a special and interesting case; in one hand there is a strong demand of security in the network and the resources and services which are listening.

II. LITERATURE SURVEY

Buvaneswari and Subha [7] have proposed an approach called IHoneycol to effectively mitigate the distributed DoS efficiently. By utilising firecol-IPS system and honeypot-IDS, IHoneycol provides a collaborative solution for the early detection of flooding DDoS attacks. It protects the subscribed customers and saves the valuable network resources by preventing the attack closer to the source and farther from destination. However, deployment of firecol routers becomes highly expensive and the honeypot server needs protection from various attacks. Our work eliminates the use of any external systems apart from roaming honeypots and provides complete protection to attacks against honeypots.

Xuxian Jianga et al. [9] have presented Collapsar, a virtual machine-based architecture for network attack capture and detention. A Collapsar center accomplishes the role of hosting and managing a large number of high-interaction virtual honeypots in a local dedicated network. A wide diverse view of network attacks was provided by decentralised logical presence of honeypots. The centralised operation eliminates the honeypot necessity in every production network by enabling the dedicated administration and convenient event correlation. Collapsar realised the traditional honey farm vision and a new reverse honey farm vision, where the honeypots act as the vulnerable clients exploited by real-world malicious servers. However, tracking or tracing the attackers from the external domain is a challenging task. Hence, our work provides a complete tracking mechanism for intruders.

Sherif Khattab et al. [9] have proposed an efficient hop-by-hop trace back mechanism called honeypot back propagation with a novel leverage of the roaming honeypots scheme to obtain accurate attack signatures. On receiving the attack packets, the honeypot triggers the activation of a tree of honeypot sessions rooted at the honeypot under attack toward attack sources. The tree formation is hierarchical with autonomous system level and router level. Honeypot back propagation supports the incremental deployment by providing incentives for ISPs even with partial deployment. Progressive back propagation was also proposed to cope with low-rate attackers like on–off attacks with short bursts since more time is taken by most of the trace back schemes against low-rate attackers for collecting the needed number of packets. However, there is no security system to protect the honeypots from unknown attacks, false negatives, false positives and so on. If an attacker breaks into honeypot, it will break honeypot connections. Our work provides complete protection to attacks against honeypots.

Anoosha Prathapani et al. [10] have proposed an intelligent honeypot-based detection system (IHBD) to identify the black hole attackers in WMNs. The honeypot-based detection model helps in throughput enhancement in case of WMN with black hole MRs. It has a high detection rate and low false positive rate. However, this work focus on detecting only black hole attacks rather than other type of DoS attacks. However, our work considers more DDoS attacks apart from traditional attacks like black hole and worm holes.

Prof. Smita Jawale et al. [11] have designed an architecture for intrusion detection using honeypot. The honeypot being a component coordinate with IDS to increase its flexibility, configurability and security. By enabling the user attempt to intrude the system, a honeypot notices the intruder's activity and generate intruder's signature. The absence of tools detecting honeypots is a major drawback in honeypot technologies. In addition, virtual honeypots based on virtualisation technology was proposed to hide honeypots. However, tracking or tracing the intrusive behaviours of attackers remain as a challenge. Hence, in our work, a complete tracking mechanism for intruders is provided.

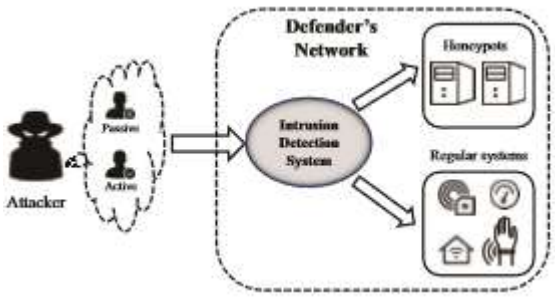

Fig 1 : Attacker and defender in the network

Fig. 1 [1] depicts the attack-and-defence scenario. The networks in the IoT paradigm very often consists of numerous smart, Internet-connected but potentially vulnerable objects. Among the chief candidates are smart household devices, electric meters, medical wearable devices and remote sensors. They are also running some

critical operations such as data collection and real-time monitoring, which makes them attractive targets to malicious attackers. To provide protection against potential attacks, multi-layer security measures are proposed for systems with IoT-based applications [5]; in which honeypot-enabled intrusion detection component adds extra depth to the defence. One such intrusion detection framework is documented in [6], where the system analyzes the incoming traffic flow according to some pre-defined scripts. Suspicious traffic will be rerouted to the honeypots to be logged and further analyzed. The rest of the traffics' are directed to the regular destinations, among which are the attacker's targets.

III. LIMITATIONS

Bayesian Game theory doesn't gives guarantee of complete defence against new attack .To overcome this, Classification of the Attacks on Honeypot proposed, but limitation of this, difficulty in classifying all threats. One more limitations can't automatically generate signatures for new malware and difficult to identify MIMT attacks in wireless network.

IV. CONCLUSION AND FUTURE SCOPE

Since the rapid growth of web services, it is becoming increasingly difficult to monitor and classify a large number of logs using only some distinctive features manually. The defender must mix up their strategy and try various combinations of different counter measures in order to make the attacker stay engaged while capturing the details. Automatically deployed honeypots must be able to attract and should possibly try to delay the intruder. Dynamic virtual honeypots are simpler to implement than hardware based system but requires complex management of services to be provided while also configuring according to the needs required dynamically.

REFRENCES

[1] Quang Duy La, Tony Q. S. Quek and Jemin Lee , "A Game Theoretic Model for enabling Honeypots in IoT Networks ,"IEEE ICC 2016 SAC Internet of Things.

[2] Naomi Kuze, Shu Ishikura, Takeshi Yagi, Daiki Chiba and Masayuki Murata,"Detection of Vulnerability Scanning using features of Collective Access based on Information Collected from Multiple Honeypots,"IEEE/IFIP NOMS 2016 Workshop: International Workshop on Analytics for Network and Service Management pg. no. 1067-1072

[3] Michele Bombardieri, Salvatore Castano` , Fabrizio Curcio, Angelo Furfaro and Helen D. Karatza, "Honeypot Powered Malware Reverse Engineering," 2016 IEEE International Conference on Cloud Engineering Workshops, pages 65-69

[4] Roman Banakh, Andrian Piskozub, Yaroslav Stefinko, "External Elements of Honeypot for Wireless Networks," TCSET'2016 February 23-26 2016, Lviv Slavsake, Ukraine, pg. no. 280-282.

[5] Tomas Sochor, Matej Zuzcak, Petr Bujok, "Analysis of Attackers Against Windows Emulating Honeypots in various types of Networks and Regions,"978-1- 4673-9991-3/16/$31.00 ©2016 IEEE, pages 863-868.

[6] Todd Vollmer and Milos Manic, "Cyber-Physical Systems Security with Descriptive Virtual Hosts for Industrial Control Networks," IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 10, NO. 2, MAY 2014 pages 1337-1347.

[7] Buvaneswari, M., Subha, T.: 'IHONEYCOL: a distributed collaborative approach for mitigation of DDoS attack'. Int. Conf. on Information Communication and Embedded Systems (ICICES), Chennai, 2013

[8] Jianga, X., Xua, D., Wang, Y.-M.: 'Collapsar: AVM-based honeyfarm and reverse honeyfarm architecture for network attack capture and detention', J. Parallel Distrib. Comput., 2006, 66, pp. 1165–1180

[9] Khattab, S., Melhem, R., Mossé, D., et al.: 'Honeypot back-propagation for mitigating spoofing distributed denial-of-service attacks'. 20th Int. Parallel and Distributed Processing Symp., IPDPS, Rhodes Island, 2006

[10] Prathapani, A., Santhananr, L., Agrawal, D.P.: 'Intelligent honeypot agent for blackhole attack detection in wireless mesh networks'. IEEE 6th Int. Conf. on Mobile Adhoc and Sensor Systems (MASS), Macau, 2009

[11] Jawale, S., Mehta, R., Mahalingam, V., et al.: 'Intrusion detection system using virtual honeypots'. Int. J. of Engineering Research and Applications (IJERA), National Conf. on Emerging Trends in Engineering & Technology, March 2012

[12] Bedi, H.S., Roy, S., Shiva, S.: 'Game theory-based defense mechanisms against DDoS attacks on TCP/TCP-friendly flows'. IEEE Symp. on Computational Intelligence in Cyber Security (CICS), Paris, 2011.

