ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 3, March 2017

A Honeypot based Attack Detection and Prevention System for Smart Cities Networks

[1]Rohit Kumar, [2]Surbhi Khare, [3]Deepa Kale
[1][2][3] Priyadarshini Institute of Engineering and Technology, Nagpur

***Abstract* - In today's world, technology is changing almost every second day. This rapidly changing technology offers lots of benefits but also put some great challenges. Smart city is a concept that merges various Information and Communication Technology (ICT) and Internet of Things(IoT) based service solutions, together. Thus, the concept of smart cities uses all possible technologies in the state-of-the-art form. Hence, there is a need to make sure that the no one could use our networks for their own benefits. Malicious users always wait for the perfect opportunities and attack on the most vulnerable part of the network. A strong defense mechanism is needed to defend against them, otherwise the concept of smart cities would only be a chaos. In this paper, we will explain the different types of possible attacks, analyze them and will propose a mechanism to defend against them, based on Honeypot based services.**

***Index Terms* — ICT, IoT, Honeypot, Security Attacks, IDS/IPS.**

I. INTRODUCTION

In today's world technology is changing with rapid pace. Smart cities are just an example of that. Smart cities have incorporated the idea of IoT and ICT based services to provide the supreme form of services. Besides the growing facilities, there also increases the base of exploits.

II. RELATED WORK

Smart Cities

Smart cities have come up with new definitions and challenges. They use the ICT and IoT services and put a glamorous city in front of you. The definition has changed from the Connected Cities to Smart Cities. As the concept behind everything is changing in smart cities, there is a lot of scope in research in smart cities architecture [1]. The smart cities will support the concept of E-commerce more strongly than even before [2]. There would be a number of different privacy preserving and security guaranteeing tools and techniques working in it [3]. Different new approaches would be employed in different fields like public key distribution, etc. [4] and the overall framework would be very useful in different industries, like in healthcare, etc [5].

Attacks

Attacks are the unwanted traffic or activities in the network that slow down the network performance by consuming the resources or disrupting the normal functioning. Attacks mainly can be of two types: 1. Passive- It is called so because the attacker wants to remain passive (active in background) to capture more information, and 2. Active- In this, the attacker attacks explicitly and reveals its presence. There are a number of surveys done in past [6][7] and it is found that the different attacks combinedly can defeat the secure considered approach[8]. The different types of attacks are listed below-.

Spoofing: *In this, the attacker uses someone else's identity to* impersonate some authentic user or the device on the network.

Modification: The main motive of this attack is to increase delay in the communication process. The attacker will alter the messages in the normal routing route and obviously, upon detection, the sender will change the route of delivery.

Wormhole: In this attack, the attacker uses the 'Tunnel Effect' to implement the attack. The attacker forwards the packets to other attacking nodes just to give the impression of fast delivery.

Fabrication: In this, the attacker generates the false routing alerts to give misguide the delivery between sender and receiver.

Denial of services*:* The main motive of this type of attacks is to consume the resources (bandwidth, etc.) of the authentic node so that it could not get the time to process the actual data. This could be achieved by generating the false data to keep the actual node busy.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 3, March 2017

Sinkhole: It is a popular attack that can also be used to launch various other types of attacks. In this, the attacker modifies the information coming from the neighbors of the authentic node.

Sybil: The motive of this attack is to disrupt the services by increasing the chances of attack through various copies of the malicious code. The more malicious nodes get into the network, the more possibility of failure gets into the picture.

Traffic Analysis Attack: This is a kind of passive attack in which the attacker just wants to know the amount of traffic data that has been flown between the sender ans receiver. Many useful information could be deduced by the total amount of data. Later on, the attacker use this information to carry on with some new attacks.

Eavesdropping: It is also a kind of passive attack in which the attacker tries to capture or listen the information, being communicated between the authentic parties. This information might be anything of any importance.

Monitoring: In this type of attack, the attacker might be able to interpret the data through the visualization of the traffic. Many information might be obtained through a visual depiction of the traffic.

Black hole attack: It is a quite advance form of attack, in which the attacker claims that it has the shortest possible path to the destination of the message. The sender considers this claim if it didn't get any other more promising claim from any other node.

Rushing attack : This is also a very different type of attack in which the attacker keeps the receiver busy by sending the false duplicated messages. Initially the attacker copies the original message and later on deliver its copies to receiver, just to keep it busy.

Replay attack: In this, the attacker may capture the original message once and later on may use it to gain some advantages.

Byzantine attack: In this attack, a number of attacking nodes work together to degrade the performance of the network by looing effect, etc.

Location disclosure attack: In this the attacker tries to discover the location of the authentic node. In addition to this information, it uses many other information pieces and later on plans the attack.

BOTNET Attack: The botnet is a group of malicious or the attacking nodes that can be human or the automatic robots. The motive of the group remains to deisrupt the functioning of the normal network, using sensitive information in its favor, launching DDoS attacks, etc.

Relay Chat (IRC) networks: Many times, it might be possible that your system might also be working as a bot. This might happen because of a malware, hiding inside your computer and continuously sending your sensitive information outside. The motive of the Relay Chat Network is to organize all the bits and perform the combined attack as per the schedule.

Distributed Denial-of- service attack : It is very popular and most discussed type of attack in industries. In this a network of attacking nodes attack on the target system together just to suspend it, making it down temporarily or permanently. The locations of the bots might be different. Each bot uses a different IP and attacks on the system with a shared purpose.

Watering hole attacks: This is a advance form of attack in which the attacker tries to infect the one or more machines and later on could use them against the network. This type of attack is commonly performed when there is a large lot that uses the target group.

Spear phishing attacks: This is a targeted form of a phishing attack, in which the particular group or the audience is targeted to infect or suffer. The online social sites are mainly affected with such attacks, in which the one user's information is used to infect others.

Zero-day attacks: This is a very dangerous type of attack. In this, the attack is launched when still there is no information in the market about such event. That's why the attacks may go undetected for many months even after their launch. Later on, when they get revealed, still the spread goes on because it takes time to develop the control measures.

Counter-Measures of Attacks

There are a number of challenges in the countermeasures of the attacks [9]. The traditional security measures that work on the signature based approach are useless in-front of the advanced attacks, being used now-a-days. Some special features that need to be employed to deal with the today's attacks and to confirm the sense of security against the attacks are-

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 3, March 2017

Signature-less malware detection: The value os signature based approached has gone down over the period of last some years. The pattern matching approach many times goes in failure and leaves the employer with loss and sense of insecurity. So there must be a concept of signature-less malware detection that could leave no malware undetected. The need is to work without relying only on pattern matching and consider the new attacking approaches.

Multi-stage protection architecture: Today's networks have become so sophisticated that a single layer approach of security can't defend the system against the modern attacks. The need is to employ the multilayer approach so that we could deal with the different layers challenges in a separate and effective way. A multi-channel of multi-layer security approach is the need.

Use of existing solutions for next generation solutions: It is a fact that no technology or solution can work itself without any support from the past technologies. The need is same in case of security solutions. We need to develop the future safety solutions by combining the best of the features of the today's available solutions.

Honeypot

A Honeypot is a fake replica of the actual resources that lure the malicious users. Its main motive is to defeat the false purposes of the rogue users. It directs the user in a normal way as the actual system does but it does not offers anything critical to him/her. At the end, user finds out the reality but till then his/her profile gets recorded by the monitoring devices and the System Administrator may take the suitable actions to safeguard its resources.

Types of Honeypots

There are a number of honeypots and the categorization might be done on different parameters. According to [10], the honeypots can be divided into two categories based on the level of involvement with the attacker or the user - a) Low Interaction Honeypots and b) High Interaction Honeypots. The more administrator opens his system architecture for the attacker with the help of Honeypot, more we shift from the low interaction honeypots to high interaction honeypots. That's why, high interaction honeypots offer you a detailed picture of a particular attack but with a greater risk probability. The Honeypot itself might be compromised to attack the actual network, existing behind it. Besides this, honeypots can also be divided based on the level of deployment - a) Production Honeypots b) Research Honeypots. The production honeypots are designed to address the basic requirement of industries or organizations i.e. Security from current attacks. But the Research Honeypot focuses on the future possibilities and that's why doesn't only study the activities of the attackers but also records them properly to help a better design for future. This is a long-term investment. The design of a research honeypot becomes heavy and that's why this types of honeypots are complex to design.

III. PROPOSAL

A Honeypot system is deployed like a normal server. Usually it exists behind the firewall/IPS of any network. A general scenario looks like [11]:

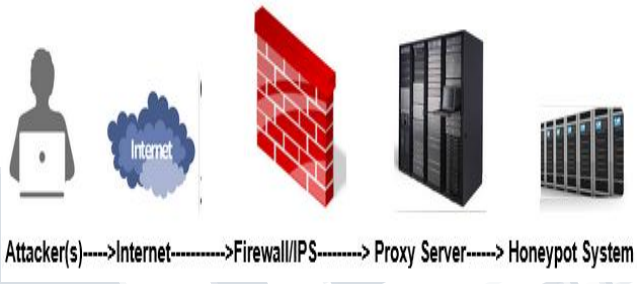

Fig. 1: A general Honeypot Deployment Scenario

The attackers might be known, so to filter them out, the firewall is necessary. The Proxy server maintains the log record of each session and the finally the honeypot system tries to bait the attackers. The log files remain safe even in case of the complete takeover of the honeypot system by the attackers. These log files will later help to analyze the attack and that would help to design more robust system in future. The honeypot system runs at-least one real service and the HIDS(Host Intrusion Detection System). The running service(s) lures the attackers and the honeypot keeps a check on the service(s). The safekeeping of the log files and the proper mining on them is a must. We may use online or the offline services to mine the log files. The Proposed approach is to apply the Honeypot at the random location, independent of the user's information. Put it in safe and hidden location, so that even the internal users could not get the presence of Honeypot. The unawareness about the honeypot is the key to its success. The location of honeypot might be changed time to time to create ambiguity about its location (even if the user/attacker is aware about the presence of honeypot) and to increase its success rate. In case of wireless networks, the accesspoints can also simulate the honeypot.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 3, March 2017

IV. COMPARATIVE ANALYSIS

The question about the true utility of the honeypot has always been prominent. There are a number of methods and logs are available to store the network activities. Still, the honeypot has maintained its status and that's due to its usefulness with its unique way of functioning. According to [12], the honeypots are designed to capture very less amount of data but only meaningful, in terms of network attacks. The other logs maintained at firewall, etc. just capture all the data and hence sometimes it becomes almost impossible to trace a single network attack activity. In this way, honeypots save the log processing time and fasten the response activities. Besides this, the resource exhaustion problem is also not a part of honeypot and that's why the honeypots may be a popular choice in network-centric applications. The cost factor is also in favor of honeypot. No special hardware is needed to deploy a honeypot in your network. Any moderately configured system might serve the purpose of a honeypot. As there is no special algorithm or concept working behind the honeypot, so it has always been a simple and straightforward method to deploy the honeypot. Honeypots show their significance by recording the attack activities and in this way they never become a victim of their own success like firewall, IDS/IPS, Authentication, Encryption, host-based armoring, etc. The Table -1 lists the advantages of the Honeypot based design over the Non-Honeypot based designs, based on some parameters:

TABLE – 1 (Advantages Table)

Parameters	**Hoenypot Based Network Designs**	**Non-Honeypot (Firewall/IDS/IPS) Based Designs**
Amount of Data, stored for analysis	Less	More
Efforts needed to find a particular attack activity	Less	More
Response to attacks	Fast	Slow
Resource Exhaustion Problem	Not Possible	Possible
Cost Factor	Low	High
Suitability for Centralized Systems	High	Low
Design Complexity	Less	More
Possibility of being a victim of their own success	None	Much
Expert Knowledge Required	Less	More
Return on Investment	High	Low

As the TABLE-1 states there are a number of reasons to go with a Honeypot based design but still there are some drawbacks. The Table - 2 lists the disadvantages of the Honeypot based design in comparison to the Non-Honeypot based designs, based on some parameters:

TABLE – 2 (Dis-Advantages Table)

Parameters	**Hoenypot Based Network Designs**	**Non-Honeypot (Firewall/IDS/IPS) Based Designs**
FOV (Field Of View)	Narrow	Wide
Fingerprint Problem	Yes	No
Risk of becoming an attack launch-pad	Yes	No

According to [13], the experts believe that the Honeypots are still in their infancy stage. Although, the progress has been made but still most of the honeypot users are the academicians or the researchers. Even then, a Honeypot is a promising solution for different types of attacks. It can effectively handle insider attacks also [14]. Using IoT, a number of applications can be automated [15], and their safety can also be implemented using effective means against attacks like sybil [16]. More has been written on the security and the concept is also linked to the Cyber-security [17]. But, the common beliefs and surveys emphasis that the Honeypot is the need of the hour [18].

V. CONCLUSION AND FUTURE WORK

In future, the further research should be done to reduce the complexity of Research Honeypots and to improve the Field of View. The paper presents a study work. This may be used to explore some other aspects of the Honeypot and their deployment at different levels. And perhaps, the coming world will witness the scalability of

Honeypots, giving a boost to the network security. As we have seen that a Honeypot based design offers a number of benefits, so its use should be promoted in industries as well as in other institutions. Honeypots might be a great tool in the security learning process. So, in academics/training also, they have a good scope. Besides, it is very clear that Honeypots alone can't defend the system but they may be a very good complement to the existing IDSs (Intrusion Detection Systems).

REFERENCES

[1] R. Khatoun and S. Zeadally, " Smart Cities: Basic Concepts, Architectural Issues, and Research Opportunities," Commun. ACM , vol. 59, no. 8, Aug. 2016, pp. 46–57.

[2] UN E - Government Survey 2014, "E-Government for the Future We Want," http://www.un.org/desaB. David et al ., " Unconditionally Secure, Universally Composable Privacy Preserving Linear Algebra," IEEE Trans. Info. Forensics Security , vol. 11, no. 1, Jan. 2016, pp. 59–73.

[3] J. H. Cheon and J. Kim, "A Hybrid Scheme of Public Key Encryption and Somewhat Homomorphic Encryption," IEEE Trans. Info. Forensics Security , vol. 10, no. 5, May 2015, pp. 1052–63.

[4] H. Demirkan, "A Smart Healthcare Systems Framework," IT Professional , vol. 15, no. 5, Sept.–Oct. 2013, pp. 38–45.

[5] Y. Zou, J. Zhu, X. Wang and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," in *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727-1765, Sept. 2016.

[6] D. Kapetanovic, G. Zheng and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," in *IEEE Communications Magazine*, vol. 53, no. 6, pp. 21-27, June 2015.

[7] C. Clavier, B. Feix, G. Gagnerot and M. Roussellet, "Passive and Active Combined Attacks on AES Combining Fault Attacks and Side Channel Analysis," *2010 Workshop on Fault Diagnosis and Tolerance in Cryptography*, Santa Barbara, CA, 2010, pp. 10-19.

[8] M. A. Chaqfeh, N. Mohamed, "Challenges in middleware solutions for the Internet of Things", *Proc. Int. Conf. CTS*, pp. 21-26, 2012.

[9] OmniSecu.com http://www.omnisecu.com/security/infrastructure-and-email-security/low-interaction-honeypots-and-high-interaction-honeypots.php

[10] P. Diebold, A. Hess, G. Schafer "A Honeypot Architecture for Detecting and Analyzing Unknown Network Attacks", In Proc. Of 14th Kommounikation in Verteilten Systemen 2005 (KiVS05), Kaiserslautern, Germany, February, 2005. http://www2.tkn.tus-berlin.de/publications/papers/kivs05.pdf

[11] InformIT.com http://www.informit.com/articles/article.aspx?p=30489

Tech-target.com http://searchsecurity.techtarget.com/feature/Honeypot-technology-How-honeypots-work-in-the-enterprise

K. Padayachee, "Aspectising honeytokens to contain the insider threat", *IET Information Security*, vol. 9, no. 4, pp. 240-247, 2015.

A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, "Internet of things: A survey on enabling technologies protocols and applications", *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347-2376, 2015.

K. Zhang, X. Liang, R. Lu, X. Shen, "Sybil attacks and their defenses in the internet of things", *IEEE Internet Things J.*, vol. 1, no. 5, pp. 372-383, 2014.

"Cybersecurity and The Internet of Things", *EY. global*, 2015.

N. Kambow, L. Passi, "Honeypots: The need of network security", *International Journal of Computer Scienceand Information Technologies*, vol. 5, 2014.