Implementation of a Honey Pot Security mechanism on a Raspberry Pi

Ayush R1, M. Baskar2 and M. Sri Vishnu Vardhan3

1,2,3 Department of Information Technology, KCG College of Technology, Chennai, India

Abstract—In the modern day, most of the enterprises have decided to move their services to a web based system which is more convenient and easily accessible to all the customers. With the advent of Internet of Things, several thousand more devices transmit data through the internet to perform various tasks that optimize our issues. These devices can provide a possible security loophole for unauthorized or illegal access. These peripheral devices that transmit data over a network and this security loophole is what we plan to address by implementing a honey pot mechanism on these very devices and neutralize any intrusion attempts through these access points. This paper in essence discusses a possible mechanism to deal with the security threats that are evolving due to the internet of things.

Index Terms—Honey pot; raspberry pi; security; unauthorized access; low interaction;

I. INTRODUCTION

Today, most of the enterprises have decided to move their services to a web based system which is more convenient and easily accessible to all the customers. With the advent of Internet of Things, several thousand more devices transmit data through the internet to perform various tasks that optimize our issues. These devices can provide a possible security loophole for unauthorized or illegal access. These peripheral devices that transmit data over a network and this security loophole is what we plan to address by implementing a honey pot mechanism on these very devices and neutralize any intrusion attempts through these access points. This paper in essence discusses a possible mechanism to deal with the security threats that are evolving due to the internet of things.

Introduction: In the rapidly advancing world of technology, we are dynamically evolving to efficiently improve our day to day lives by innovating around our handheld devices and utilize the internet to facilitate the same. One of the most important emerging trends and the way forward in the future of technology is the Internet of Things where we have several devices that can communicate with each other by transmitting data over a network. This communication by these peripheral devices over the network offer an access point for the attacker to target and exploit the loophole in the network, resulting in them gaining access to these devices and open up an intrusion pathway into the network and obtain access to the data and information present on the network.

In order to secure our networks from this possible security loophole when all households adapt to the concept and trend of internet of things, the suggested method or mechanism to tackle the threat would be to create a facility to secure the peripheral devices (Raspberry Pi or Arduino) like our conventional Personal computers have inbuilt defence systems. This will ensure end to end security for our networks.

II. CASE STUDY

A. Home automation systems

The case study that we will be using as an example for the understanding of the need for this process is a simple home automation system that works with the mechanism of remotely operating devices from your phone by sending the required text message that is predetermined during encoding to switch on or off the device. A simple text message can ensure that your air conditioner at home is switched on by a text message and thereby ensure cooling of your room by the time you get home on a hot day. This mechanism can be exploited by attackers to inject their scripts and access the private network which also provides access to these peripheral devices (like raspberry pi) to communicate with the master computer and optimize device usage.

In order to prevent the network from being compromised via this access point, we need to close this security loophole which is what this paper discusses.
B. Intelligent systems
Intelligent systems are an upcoming trend used in both smart homes and medical facilities to monitor the various aspects of the environment such as temperature, moisture content etc. and instruct various devices to react as and when the scales deem fit. In these systems, small peripheral devices communicate with each other and take the necessary action. These devices generally use the same private network that we use to store our data and hence are a potential pathway for intrusion. Tackling this threat can be done by using our suggested method.

III. RELATED WORKS
The previous and related work with respect to both honey pots and the Raspberry Pi implementation in security mechanisms is discussed below:
A. Use of a Honey Pot in a Local Area Network(LAN)
In today’s world, the growing threat of cyber attacks is something that we are not dealing with in an effective/efficient manner. Attacks are becoming more and more dynamic in nature and defence mechanisms need to adopt an equal measure of dynamism. Most network administrators are focussed on repelling any attacks or intrusions and hence they fail to study the method or patterns of attacks. Hackers attempting to access information stored on the network or the server constantly keep bombarding the target with new variations of attacks.
As a result, sometimes the hacker can penetrate the system without the knowledge of the network administrators or users resulting in loss of data which is probably not noticed by the network security engineers.
The role or the use of a honey-pot is extremely simple yet valuable. We use a honey pot setup to actively monitor and defend the network from illegal access. If there is a network breach which is not noticed by the security mechanisms, the honey pot will do its job of attempting to lure the attackers towards it and thereby protect the important information. In addition, the methods used by the attacker to access the network are stored in the logs as evidence and can be retrieved for future study of the attack patterns.
This can also be used to map and predict possible future attacks by decoding the mechanism used by the attacker and progressively identifying the tools utilised for the same. This is essentially a mechanism of evolution for network defence and security systems [1].

B. Using a honey pot as a proxy server
The system architecture proposed by Supeno Djanali, FX Arunanto, Baskoro Adi Pratomo, Hudan Studiawan, Satrio Gita Nugraha [2] is essentially a system that uses a proxy server, combined with the actual server carrying the information and a honey pot. The proxy server receives the web requests and does analysis of the request and decides to forward it either to the honeypot or to the server. Here the server cannot be accessed directly over the internet as it is the proxy server that is connected to the internet. The actual server is connected to the proxy server via a private network. The honey pot is also linked up with the proxy server and can be accessed via the internet itself. Basically, the proxy server and the honeypot work in tandem and can be considered as one unit.
The proxy server serves as a detector and analyser for SQL injections and any such malicious requests are dealt by the honey pot

C. Performance of honey pots
The performance analysis is done on the various types of honey pots that are in implementation today. Classifying them into two broad categories, we have high interaction and low interaction honey pots. Both have their own pros and cons. For instance if we consider the high interaction type honey pot, it is a much more efficient mechanism on implementation and provides all the sufficient attacker information and is extremely detailed. It is also quite prompt in displaying the alerts. On the flip side, in a high interaction honey pot, we run the risk of more interaction with the attacker and enabling the attacker to gain access into the real system and the real operating system and the system is used as bait.
Low interaction honey pots meanwhile, are not as effective as the other type when it comes to information collection and the data collected is usually not in-depth. But in the system that employs low interaction honey pots, the attacker cannot interact much with the system and the integrity will not be compromised. This type of honey pot can also be simulated across various network topologies without a problem [3].
IV. PROPOSED SYSTEM

The proposed approach is in line with the internet of Things (IoT) trend where we have several smaller devices that communicate over the internet to share information and enhance efficient processing of our systems. We consider the Raspberry Pi (or any other smaller computer) that acts as the peripheral device to be the access point for a possible intrusion attack into the network. Our conventional computers are loaded with different mechanisms to counter such threats. The idea is to do the same for these peripheral devices, hence leaving them equipped enough to deal with the intrusion attempt. Ideally, the Honey pot proposed will be a low interaction honey pot that will be able to safely collect attack information that can be used for our analysis of attack patterns and enable us to consistently evolve in the field of network security as we see new threats rising each and every day. Adapting to these new threats is the challenge and accurate attack information if obtained can go a long way in curbing the menace of intrusion attacks by making the network immune to such attacks by adapting as required based on the pattern.

V. CONCLUSION

This proposed method emulates a simple mechanism to tackle an overlooked loophole and possible path of security compromise by attackers onto private networks by means of using the peripheral devices in the internet of things trend. The honey pot mechanism implemented will also collect the attack logs of attackers and will provide the required data collected to the network security administrator to take action that is necessary to prevent any further attempts at infiltration.

FUTURE SCOPE

Since the trend of internet of things (IoT) is just taking off, there is an ample amount of scope for this project as there is no security mechanism envisioned to deal with threats at the said access points. This proposed method guarantees end to end network security.

ACKNOWLEDGMENTS

We would like to thank the Head of the department of Information Technology, Dr. Frank Vijay for providing his constant support. We would also like to thank Ms. Subbulakshmi for being a source of encouragement in our work. Finally, we would like to whole heartedly thank our families and friends in this venture.

REFERENCES