A Mobile Honeypot for Industrial Control Systems

Master-Thesis von Shreyas Srinivasa aus Bangalore, India

Tag der Einreichung:

Gutachten: Emmanouil Vasilomanolakis

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Fachbereich Informatik
Telekooperation
Prof. Dr. Max Mühlhäuser

A Mobile Honeypot for Industrial Control Systems

Vorgelegte Master-Thesis von Shreyas Srinivasa aus Bangalore, India

Gutachten: Emmanouil Vasilomanolakis

Tag der Einreichung:

1 Introduction

Mobile devices today have better communication capabilities. They enable dynamic and faster communication. Users are able to access internet and web applications through their smart phones anywhere, anytime. Smarter applications offer better social interaction and online presence to the users. This creates an urge to stay connected and be online seamlessly to be updated.Public infrastructures like airports, coffee shops, shopping malls provide free access to their networks to its customers to facilitate their connectivity and of course, for some information exchange. With free access to networks, attackers are now concentrating on the possibility of exploiting users in the same network. Securing open networks is very challenging and complex. It is however possible to detect these attacks. A pro-active approach is a better way for detecting the attacks.

Huge industries like nuclear power plants, water treatment and distribution plants, manufacturing plants have many complex critical machines and require constant monitoring. They rely on process automation on these machines and are dependent on sensors for making this automation possible. This sensor-to-machine-to-human communication and automation is achieved with the help of PLCs[14] or Programmable Logic Controllers. This communication is usually not secure and is open to attacks. As this hardware has limited computing resources, encryption of data is an expensive option. There have been many attacks detected over the years on SCADA[1] ICS, most notable being STUXNET[5]. Securing and detecting attacks in these networks is necessary as it is responsible for communication in critical machines. Failure of such machines could cause a devastation to the environment and human life because of the wide spread use of PLCs in infrastructures like airports, coffee shops and also in prisons.

There are two approaches for detection of attacks. One is by using a NIDS[10] (Network Intrusion Detection System) and the other is by using Honeypot[9] . NIDS are installed on the server machines or hosts. The requests are scanned and analyzed for exploit-forged packets before they are sent to the server. NIDS are suitable for systems with high resources. The Honeypot approach, rather could be used where there are lesser resources. The idea behind Honeypot, is to pose as vulnerable hosts connected to the network, which could be tempting for exploits, thereby trapping the attacker by collecting as much information possible to backtrack, or good enough to detect that the network is under attack.

1.1 Motivation

The applicability of a Honeypot in a mobile environment is prodigious, considering the public network infrastructure services offered. Network connectivity has become more of a necessity than a luxury, as technology is continuously evolving. Better services, data management and accessibility draw a lot of users having online space and in the need to stay connected. This need is rendered by some businesses and public infrastructure like airports, malls and cafeterias. With smart phones, people have the power to stay connected and do the majority of the tasks efficiently at their fingertips. Mobile devices today are considered personal devices because of the capability to store, share and process private data. This data is valuable and private to a user and has to be secured. Connecting to public networks can result in lot of vulnerabilities, as there is not always security considered in public networks. With the help of scripts crafted to exploit these vulnerabilities, an attacker can exploit users personal data.

Attacks are not limited to the above protocols. Airports, malls, enterprise hotels and huge industries use PLCs[14] (Programmable Logic Controllers) as for many applications such as conveyor belts, elevators, lighting control systems, fire and safety detection systems in order to automate the tasks quickly without human intervention. PLCs can be programmed logically to specify the methods to be called, based on inputs provided by sensors. SCADA (Supervisory Control and Data Acquisition) is a system operating with coded signals over the communication channels so as to provide control of remote equipment like PLCs.

A study made by DELL[2] showed that the attacks on Industrial components like PLCs doubled over the years, and even more dangerously, such incidents going unreported. The research found a 100 percent increase in attacks against industrial control systems like SCADA.

Figure 1 gives an understanding of the Key SCADA Attack Methods. It shows that about half of the total attacks were based on improper assignment on bounds of a memory buffer, improper input invalidation, vulnerabilities in credentials management. These vulnerabilities pose as a huge threat to ICS. Figure 2 represents the number of attacks performed over the months. There is a steep increase in the number of attacks performed over the months, expressing the need to safeguard ICS systems and also detect these attacks.

The majority of industrial systems today use SCADA for controlling and automating their processes. Securing these devices is as much important like any other hosts in the network because these devices are programmable and could affect the normal automatized working. STUXNET[5], a computer worm discovered in 2010 was designed to attack industrial programmable logic controllers (PLCs). STUXNET reportedly compromised PLCs in power plant at Iran. The design and architecture of STUXNET is not domain-specific and it could be forged for exploiting modern SCADA and PLC systems.

[1] http://www.schneider-electric.com/solutions/ww/en/med/20340568/application/pdf/1485se-whitepaper-letter-scadaoverview-v005.pdf

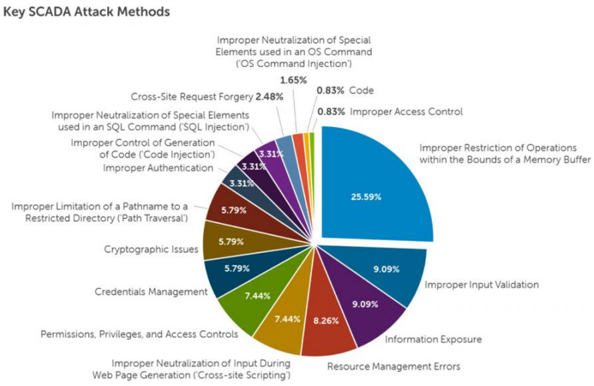

Abbildung 1: SCADA attack methods[2]

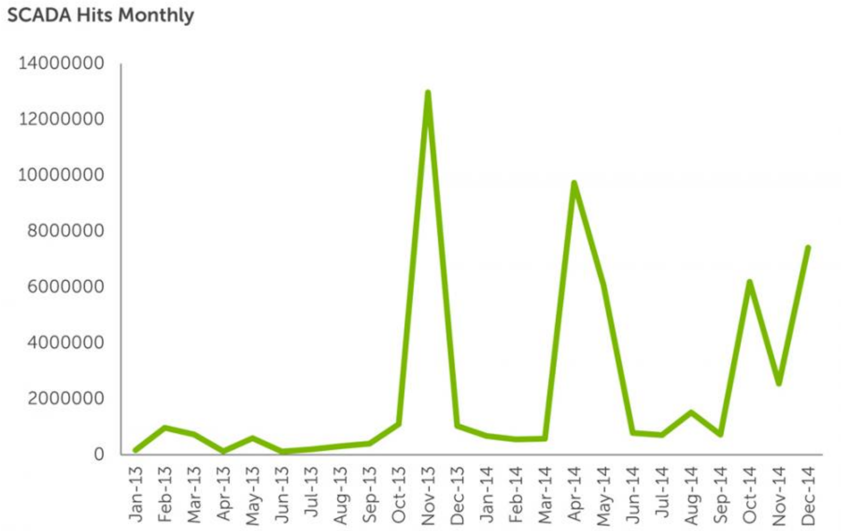

Abbildung 2: SCADA hits on a monthly basis.[2]

1.2 Contribution

This theses aims at identifying and detecting the SCADA attacks using a low interaction mobile Honeypot platform using which a industrial master and slave profiiles will be simualted. An analysis of the communication paradigm and the security loopholes in a SCADA ICS system is made, to simulate the services offered by the system. The thesis also concentrates on contributing to many security related research questions of SCADA ICS systems like identifying the targets, analyzing the malware, assessing the consequences and defending ICS systems.

1.3 Outline

This thesis topic also aims at adding more capabilities to detect attacks through different malware, mainly focussing on simulating industrial level SCADA PLC to determine malware attacks on them. The rest of the expose is structured as follows. Section 2 will specify the requirements to develop the protocol emulation for mobile Honeypot. In Section 3, related work in the area of mobile Honeypot and SCADA Honeypot are discussed. Section 4 describes a proposed system for a mobile Honeypot for ICS systems and Section 5 concludes with a time plan for the thesis.

2 Background - ICS SCADA and Mobile Honeypots

ICS (Industrial Control Systems) form a dominant portion in present day industries. Strange, yet astonishing, the fact that ICS is also a part of everyday life is also true. ICS components include actuators, sensors, networking devices, controlling systems and PLC's . The sensors form a major part of ICS as they provide continuous feed of critical information which is used to automate and control other systems. The other important component is the PLC. This interface allows a programmer to implement a logic to automate the systems based on the data received from sensors. There are a few different kinds of ICS. One of the major types is SCADA (Supervisory control and data acquisition) which is deployed on geographically widespread and controlled using a central location. Examples to this type include nuclear power plants, water distribution , power distribution where there is a need constant monitoring and critical automation. SCADA systems are mainly deployed where is a need for alarm systems. The other kind of ICS system is the Distributed Control Systems (DCS). On the contrary these systems are not centralized, but distributed across a network. We shall focus more on SCADA ICS systems as they are being deployed in major infrastructures today.

Infrastructures discussed above have a lot of components and devices which need constant communication between them.

2.1 ICS SCADA

SCADA is an industrial automation control system at the core of many indutries today including Energy, Oil and Gas, power, Water and Recycling , Manufacturing and many more. They are used by both private sector industries and the public sector service providers. It provides the benefit of simple configuration and usability.

The basic architecture of SCADA involves communication of information from sensors or manual inputs to PLCs or RTUs. These PLCs process the information as per the logic deployed in them and then forward this information to workstations/servers running SCADA applications. Figure 3 describes the basic architecture of a SCADA system.

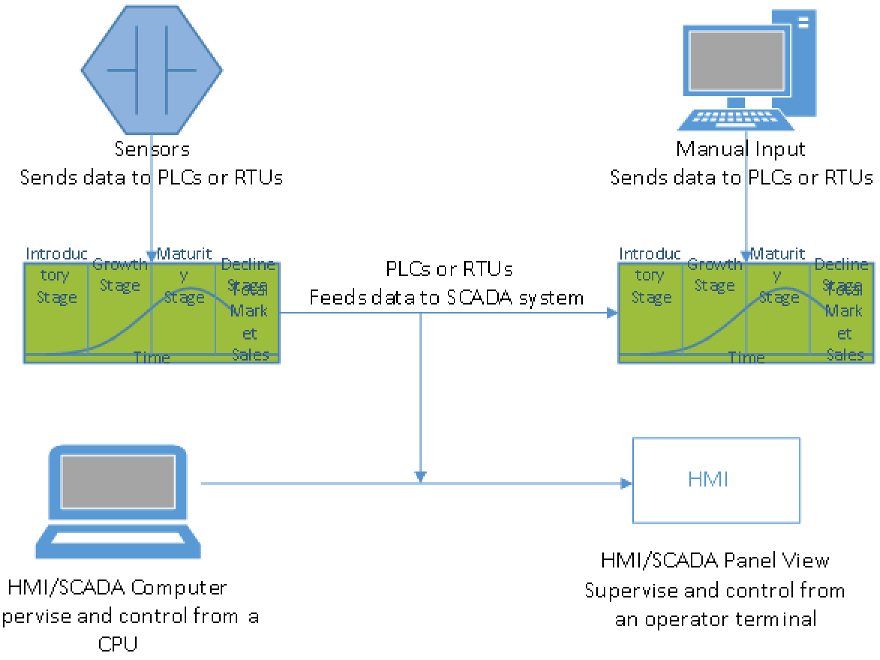

Abbildung 3: SCADA Architecture

SCADA systems involve control components and network components. The following is a list of control components in SCADA:

- **Remote Terminal Units (RTU):**These units connect to sensors in the process and convert sensor signals to digital data. They have telemetry hardware capable of sending digital data to the supervisory system, as well as receiving digital commands from the supervisory system. RTUs often have embedded control capabilities in order to accomplish boolean logic operations.

- **Programmable logic controller (PLCs):** These devices connect to sensors in the process and convert sensor signals to digital data. PLCs have more sophisticated embedded control capabilities than RTUs. PLCs do not have telemetry hardware, although this functionality is typically installed alongside them. PLCs are sometimes used in place of RTUs as field devices because they are more economical, versatile, flexible, and configurable.

- **Telemetry system:** It is typically used to connect PLCs and RTUs with control centers, data warehouses, and the enterprise. Examples of wired telemetry media used in SCADA systems include leased telephone lines and WAN circuits. Examples of wireless telemetry media used in SCADA systems include satellite (VSAT), licensed and unlicensed radio, cellular and microwave.

- **Data and Control Server:**A data acquisition server is a software service which uses industrial protocols to connect software services, via telemetry, with field devices such as RTUs and PLCs. It allows clients to access data from these field devices using standard protocols.
- **Human Machine Interface (HMI):** It is the apparatus or device which presents processed data to a human operator, and through this, the human operator monitors and interacts with the process. The HMI is a client that requests data from a data acquisition server.
- **Historian software:** A software service which accumulates time-stamped data, boolean events, and boolean alarms in a database which can be queried or used to populate graphic trends in the HMI. The historian is a client that requests data from a data acquisition server.

Different network characteristics exist for every layer within the control systems. The network topologies vary by vendors or manufacturers and also on different implementations. Modern day SCADA systems are open to Internet communication and enterprise integration can be achieved. The control networks work in hand with the corporate enterprise networks to better manage and control the systems from outside networks. The following are the major network components of an ICS network:

- **Fieldbus Network:** The fieldbus network links sensors and other devices to a PLC or other controller. Use of fieldbus technologies eliminates the need for point-to-point wiring between the controller and each device. The devices communicate with the fieldbus controller using a variety of protocols. The messages sent between the sensors and the controller uniquely identify each of the sensors.
- **Control Network:** The control network connects the supervisory control level to lower-level control modules.
- **Communications Routers:** A router is a communication device that transfers messages between two networks. Common uses for routers include connecting a LAN to a WAN, and connecting MTUs and RTUs to a long-distance network medium for SCADA communication.

SCADA applications help in monitoring, analysing the data to help the device controllers and operators work efficiently. Modern SCADA systems allow real time data from the plants to be accessed from anywhere in the world. This also means that it provides attackers an opportunity to exploit this data and availability. Exploiting SCADA systems can cause catastrophic as it may result in huge damage to the environment and people in the plant. We try to identify the attacks and exploits that could be made and detect them using a mobile Honeypot.

2.2 Security Perspective of SCADA ICS

ICS SCADA systems are highly distributed. They are used to control and manage geographically dispersed plants, often scattered over thousands of kilometers. In these areas centralized data acquisition and control are critical to system operation. They are applicable in distribution systems such as water distribution and wastewater collection systems, oil and natural gas pipelines and electrical power grids.on systems. A SCADA control center provides centralized monitoring and control for field sites over long-distance communications networks, including monitoring alarms and processing status data. Based on information received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station control devices, which are often referred to as field devices. Field devices control local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions.

The control center is responsible for managing and controlling the devices at the field site and thus there is a need to have a critical communication network between them. This is usually established through the MODBUS TCP/IP over the Ethernet. It is usually advised to place the SCADA devices on a network that is not physically connected to any other networks (cite http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf).

// Refer to paper Plausible Solution to SCADA security for more info

2.3 Honeypots

A Honeypot is a decoy server or a system in a network which is closely monitored for adversaries. It is also defined as: *A Honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource*. (//cite https://www.acsac.org/2003/papers/spitzner.pdf). They are mostly deployed inside firewalls, but they could be deployed in any part of the network. It is designed to be a system with vulnerabilities and services that are offered by a real target system. Any attempt to connect to these systems could be considered as an attack. All the activities are logged and further traced. The general idea is that once an adversary detects a vulnerable system and tries to attack it, he would come back with more sophisticated attacks. The initial part of discovery and knowing the general services and loopholes is called system social engineering. Honeypots provide are active monitoring components that wait for attacks and respond to the attacks by luring the attacker to pursue more.

There are certain main functionalities that the Honeypots must possess in order to perform their main functionality.

1. Honeypots must simulate the system that they are intend to focus on. This gives the attacker a feeling of approaching a real system. The Honeypot may simulate the complete functionality of the system or just the services offered by the system.

2. A proper response mechanism which keeps the attacker engaged to the Honeypot. This makes better logging of the attack and also provides more data to analyze the attacks.

3. It mainly has three perspectives. Firstly, an attacker perspective, by posing as a vulnerable system; second an administrator who can log identify and log the attacks made by the attacker and third, being able to present and analyse the attacks logged by the administrator.

4. Honeypots must not induce additional load on the infrastructure. Honeypots must be designed to be lightweight and having no influence on the production systems.

5. Honeypots are basically exposed to exploits, threats and malware. It is very important to see that this data is not leaked through the network which can later infect other systems in the network.

6. Based on the previous condition, Honeypots must be robust to withstand the attacks and exploits and not fail.

It is very clear are valued because of the interaction mechanism that they provide for any communication request. They can be used to study and gather exploits, malware and threats in an early attack phase. There are many advantages that one could consider for using Honeypots as an additional security monitor. There are various advantages of Honeypots:

- **Effective Data Sets:** Honeypot collects data only when there is a communication requested with it. The data collected at Honeypots may not be immense but is good enough to analyze and detect attacks. The logs provide information about the attacker IP, time of attack and protocol used to carry out the attack. This makes lesser false positives.

- **Reduced False Positives:** Among other security approaches like IDS and firewalls, false positives are quite common. The biggest challenge is to reduce false positives. Honeypots reduce false positives or could be designed to reduce false positives. Any communication with the Honeypot is unauthorized. This makes Honeypots efficient in detecting attacks.

- **Catching False Negatives:** Honeypots have advantages over signature based detection systems. Signature based systems do not categorize unknown attacks. They rely on a signature system to be updated on their local database to identify and detect uknown attacks. The probability of a detecting a new exploit is low. Honeypots detect all attacks irrespective of their signatures, hereby increasing the possibility of detecting new attacks.

- **Encrypted Communication:** The current standards in Transport layer includes using encrypted TLS communiction between nodes. Some attacks fail to detect because of the encrypted data and communication. All enterprise employ secure protocols like SSH,IPSec, HTTPS, TLS in their infrastructure. This may cause problems in detecting exploits and analyzing the attacks later. Honeypots solve this issue as they are end points in the communication. The hosts directly interact with the node and hence all the traffic and data can be decrypted and analysed later.

- **Compatibility to new architecture:** Technology evolves every moment. It is very essential to consider future compatibility with newer standards and technology. Most of modern day IDS or firewalls are not compatible with IPv6 which promises to be the next standard on Internet addressing. Honeypots can be made compatible to newer standards and technology as they are not mediators or devices but act as end points. However, devices could be simulated by Honeypots.

- **Flexibility:** Honeypots can be deployed locally or open to the external network. Honeypots could be deployed on any environments based on the requirements. Honeypots could be used to simulate any software, hardware, servers, workstations and devices.

- **Minimal Resource Consumption:** Honeypots can run on low resource machines as they are just simulations and are may not depict full functionality of the system simulated. Honeypots today can run on smartphones as they possess the required resources which are good enough to run a Honeypot.

There has been extensive research going on in the field of Honeypots. This section describes related works on Honeypots.

2.3.1 Types of Honeypots

Honeypots can be classified into two types based on the ability of the attacker to interact with the application or services. They can be categorized to High-Interaction Honeypots and Low-Interaction Honeypots. This classification is mainly based on the Honeypot's interaction with the attackers. Highn Interaction Honeypots typically composed of the actual device, its operating system and all the applications that run on that device. In short, the exact machine is used as a Honeypot with all its services. This provides better interaction as we are using the device itself as a Honeypot. There are also better chances that based on the vulnerability known, all the exploits work on the device. The main advantage of such Honeypots is that it is the machine itself that is being exposed and has greater chances of attracting attackers. The disadvantage would be that if the Honeypot is completely compromised, then it has to be rebuilt in order to log other attacks. The validity of such Honeypots is not guaranteed. A low interaction honeypot on the other hand is a software based or simulation based Honeypot approach. The system to be subjected to attack is simulated by the Honeypot along with its main services. The Honeypot can run on any system, for example it can run on a Linux machine and simulate a Honeypot for a Windows IIS server. It can simulate or mimic the network stack and the operating system of the targetted system. All connections and communication with this device is logged. The advantage of low interaction Honeypots is that they are completely flexible and easy to maintain. Low interaction Honeypots are also likely not to get compromised as they just mimic the services or in short the basic communication mechanism. It is on the researcher to design these Honeypots accurately to get productive results.

2.3.2 Honeynets

Honeynets are a networked collection of honeypots that look like common network services and servers. (Provos and Holz, Virtual Honeypots: From Botnet Tracking to Intrusion Detection , 2008). It could be a collection of Honeypots depicting as a Domain Controller, web server, application server, file server and so on which provide a facade of a enterprise network. Honeynets usually consist of high -interaction honeypots, low - interaction honeypots, or a combination of both. Using high interaction Honeypots only for this approach would be more expensive. Honeynets are placed behind a Honeywall , which acts as a bridge to the honeynet. It includes network monitoring, packet capture, and IDS capabilities.

2.3.3 Mobile Honeypots

Modern day smart phones are context sensitive and collect a lot of data from the users perspective. This data is both private and critical to the user. There is a need to protect this data. The phones also have enormous computing resources in terms of hardware and also efficiently built software kernels that are capable of processing huge data. We are also able to stay online every moment and can connect to various hotspots providing us Internet facilities to stay connected. This also is huge security concern as the networks and the apps that are deployed on our phones may not be secure and leak sensitive data with respect to the user.

The power of mobility, computing resources, usability and flexibility make Mobile devices a good platform to host low interaction Honeypots. Such capabilities make it possible to host a low interaction Honeypot on the devices.Some researchers believe that Mobile Honeypots are still not well defined and could be used to define either a probe deployed on a mobile device or on a mobile operating system. It can also be defined for a system that is controlled in the network of mobile devices. (http://conferences.sigcomm.org/sigcomm/2012/paper/sigcomm/p305.pdf)

Early research on Mobile Honeypots focused only on Bluetooth communications[5,17]. The continuous advances in the field of smartphone technology has enabled better opportunities towards Honeypot research on smart phones.

//Write about Mobile Honeypots There has been existing work that focused on detection of mobile specific malware. The first to discuss the idea of a Honeypot for smartphones were Mulliner et al., by providing the initial ideas, challenges and an architecture for their proposed system[8]. Nomadic Honeypots[7] concentrates on mobile specific malware and also trades off with a lot of personal information.

- **HoneyDroid**(cite HoneyDroid) HoneyDroid is a smartphone Honeypot for Android operating system which claims to be the first ever Honeypot in the Mobile Honeypots category which makes use of smart phone hardware to host the Honeypot.It is built on a Linux micro-kernel and is customized to impose restrictions on the Android operating system for monitoring its activities. The architecture is comprised of a Event Monitor, to monitor active connection requests and also system calls in the kernel level; Filters to mitigate any attempts of malware trying to affect the system and a log software to log all the activities. This Honeypot is also focused on detecting attacks from apps installed in the device which try to infiltrate the kernel for gaining unauthorized access. The system also involves virtualization which enables simulation of various services. This could also result in an overhead, hereby causing a signature which can be detected by attackers and malware. However, the direction of HoneyDroid was to introduce the concept of Mobile Honeypots.

- **Cellpot:** (cite Cellpot) Cellpot concentrates on detection and defence of attacks in the cellular network. It comprises of a collection of Honeypots, or Honeynets that are deployed on mobile phones. Cellpot consists of applications like SMS spam prevention, mobile phone theft and malware protection. The Honeypot mainly is concentrated towards Small Cells(cite from paper), wireless infrastructure deployed in customers site and operated in licensed bands. The main use of Small cells is to support the need of coverage and capacity. These points are a good place to deploy the Honeypots to detect malware and other intrusion attacks. Denial Of Service is the most common category of attack in the area of cellular networks, and with the help of few devices,this attack can be executed successfully. Introducing a Honeypot approach for detecting such attacks at small cells is a feasible solution.The concept of Cellpot is to detect, collect intelligence and mitigate threats against the cellular network directly on the base stations. Further, it has the ability to deploy countermeasures against detected threats, and enables a wide area of applications. It provides a good platform for mobile network operators to deploy and run additional applications to reduce signaling.

- **Nomadic Honeypots:**
- **HosTaGe:**[12],[13] is an Android App which acts as a Mobile Honeypot, determined to detect malicious networks and probe for attacks. It is user centric and aims at creating security awareness to its users. The results obtained in this process are synchronised with a global repository and also can be shared locally through bluetooth. The current version has capabilities of emulating as Windows, Unix, Apache Server, SQL and Paranoid host. Attacks through HTTP, SMB, SSH, HTTPS, Telnet and FTP can be identified.

2.4 SCADA Honeypots

Analysing the security concerns of ICS SCADA systems and the advantages of Honeypots, a solution could be implemented to combine the needs and features. SCADA Honeypots could be deployed in ICS Networks for monitoring and analysis. They act as an additional line of defense providing warnings and notifications for attacks. Designing a SCADA Honeypot involves studying the architecture of the SCADA systems and the components, protocols involved in communication and processing of data. Further, as discussed before, SCADA networks comprise of hardware devices like PLCs and RTUs which play a very critical role in processing and communication of data. SCADA systems rely on PLCs for data processing. If PLCs are targeted by attackers to compromise their working, it could bring down the entire plant, hereby resulting in a huge catastrophe. Modern day PLCs offer TCP/IP communication which can used to control and manage the data flow between other PLCs and control servers. On investigating attacks that have occured in the past, STUXNET a malware, was found to be injected in a Nuclear Enrichment Facility in Iran. STUXNET was found to be injected into the network using a USB drive to one of the host control systems. The malware spread from that system to other systems through intranet and remained hidden from operators. STUXNET was able to interfere with the working of a PLC that controlled centrifuges and managed to compromise the conditions on which the PLC depends. It was only by the observation of an operator that the PLC was causing the centrifuges to run more fast than usual was detected. But nobody could determine what caused the centrifuges run abnormally.

Detecting such kinds of attacks is not only complex but also very necessary. Such kind of attacks cannot be detected neither by signature based systems, nor by firewalls. Some organisations took initiative to design Honeypots for SCADA systems. They are elaborated in futher secctions.

2.4.1 SCADA Honeynet

SCADA Honeynet Project[3] is a project aimed at building Honeypots for industrial networks. It was the theb first of the type. SCADA Honeynet was designed to simulate the PLCs and detect attacks performed on them.The short-term goal of the project was to determine the feasibility of building a software-based framework to simulate a variety of industrial networks such as SCADA, DCS, and PLC architectures. It provided scriptable industrial protocol simulators to test actual protocol implementation. The design was a ingration of stack level, protocol level, application level and hardware level. The Honeypot was carefully designed to cover all the services offered by the SCADA systems, including the networking devices like routers and a direct serial device.

2.4.2 Trend Micro SCADA Honeypot

Trend Micro a global security software company conducted an experiment[2] to detect attacks on SCADA by setting up 12 Honeypots in 8 countries. The Honeypots camouflaged a municipal water control system based on SCADA that was connected to the internet. Attacks were basically focussed on meddling with the pump system. The objective of this experiment is to assess who/what is attacking Internet-facing ICS/SCADA(Industrial Control Systems) devices and why. In addition, the research set out to identify if the attacks performed on these systems were targeted, by whom, and for what purpose.

[2] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-whos-really-attacking-your-ics-equipment.pdf

The Honeypot architecture design used a combination of high-interaction and pure-production Honeypots. A total of three Honeypots were created to ensure as much of the target surface as possible. All three Honeypots were Internet facing and used three different static Internet IP addresses in different subnets scattered throughout the United States.

2.4.3 Digital Bond

Digital Bond is a security research and consulting firm created a Honeypott system that comprised of two virtual machines. It is open source. One of the virtual machine acts as a PLC Honeypot and the other is a monitoring engine that logs all the traffic information. This system is also called a Honeywall. Honeywalls can also be used to monitor High Interaction PLC Honeypots. The Honeywall comprises of Snort IDS and signatures with respect to PLC. The services that are simulated are FTP, TELNET, HTTP, SNMP and MODBUS TCP.

2.4.4 Conpot

Conpot[3] is a low interactive server side ICS Honeypot designed to be easy to deploy, modify and extend. It provides a range of common industrial control protocols capable of emulating complex infrastructures to convince an adversary that he just found a huge industrial complex.To improve the deceptive capabilities it also provides the possibility to server a custom human machine interface to increase the Honeypots attack surface. The default configuration of Conpot simulates a basic Siemens SIMATIC S7-200 PLC with an input/output module.

2.5 MODBUS

MODBUS denoted IETF RFC 2026 is a serial communications protocol published by Modicon for using in its PLCs. It is now a standard that connects industrial devices together. The basic configuration involves connecting a SCADA supervisory control system to a PLC or RTU. Many of the data types are named from its use in driving relays: a single-bit physical output is called a coil, and a single-bit physical input is called a discrete input or a contact. The device requesting the information is called the Modbus Master and the devices supplying information are Modbus Slaves. In a standard Modbus network, there is one Master and up to 247 Slaves, each with a unique Slave Address from 1 to 247. The Master can also write information to the Slaves. MODBUS TCP/IP specification was introduced to MODBUS to integrate corporate intranet with PLC systems. This made the network better manageable, scalable and also cost-effective.MODBUS TCP/IP offers many advantages:

- **Simplicity:** The TCP is wrapped with MODBUS instruction set. The setup involves simple driver initialization at end devices to communicate. Low development cost, hardware and compatibility with many OS makes it simple.
- **Standard Ethernet:** Ethernet ingrates easily into simple chipsets and boards. The cost of implementing Ethernet to MODBUS is low and also provides ample resources as there are many developers are working on optimizing the technology. Ethernet port 502 is used by the MODBUS TCP/IP protocol.
- **Open:** The MODBUS protocol has been open source since 2004 and a dedicated organization working towards develpoment,optimization and maintenance.
- **Compatibility:** MODBUS provides interoperability among various vendors and also compatibilty with devices of other manufacturers.

MODBUS TCP/IP is an Internet protocol. This makes the devices open to the Internet. This was a particular feature that was incorporated to facilitate better control and making device maintenance through remote systems over the internet. MODBUS is also industrial networks protocol and the industries are geographically separated. MODBUS TCP/IP helps in better management of distributed industrial systems throughout the world.

3 Proposed System

In this work, a low interaction Mobile Honeypot mechanism to simulate industrial PLC will be designed and implemented. The design also aims at detecting attacks and making inferences about the attackers and attacks. The final version will be integrated to the HosTaGe app along with the other advanced mechanisms that HosTaGe already provides to its users. As the proposed system deals with implementing a low interaction Honeypot, the challenge involves implementing only the essential components or services, that satisfy the discovery and vulnerability to attack them, for example, the network stack. Along with basic attack detection, the system must also have a short response time, robust design to withstand the attacks and also maintain a log of the exploit for further analysis and backtracking. An attempt will be made to detect attacks forged with popular identified worms like STUXNET. The conclusions on the attacks made will be pushed on to a central repository where the details of the attack are made public for users worldwide. The overlay of the proposed system, mechanisms and the evaluation are followed below.

[3] http://conpot.org/

4 System Design

HosTaGe has implemented mechanisms to emulate different kind of hosts like a windows host, linux host, webserver, FTP server, SSH server and more. The simulation of industrial level SCADA based PLC will be added to the the existing list of simulated hosts and services. To simulate PLCs it is important to understand their communication and control infrastructure. PLCs have network interfaces that support Ethernet, TCP/IP, MODBUS[4], DeviceNet[6], ControlNet[6], Foundation Fieldbus[11]. The manufacturers have their own in built shells to support FTP commands. The Ethernet communication module of the PLC typically runs an embedded operating system that includes standard network protocol as well as implementations of industrial network protocols such as Modbus/TCP or EtherNet/IP. Telnet and FTP servers are common and have identifying information which can be used to determine the vendor and version of software. The network components that need to be simulated in a PLC are the TCP/IP stack, Modbus/TCP server, FTP server, Telnetd server and a HTTP web server which provides an interface to manage the functioning and control of PLC.

The discovery and identification of the PLC in the network can be through a network nmap scan that reveals information about the host name, ports 21, 80 and 502(Modbus) open.

The main objective is to detect attacks made using the protocols offered by the Siemens Simati S7 200 PLC . A logging mechanism logs the information about the attacker in pursuit.

4.1 Siemens SIMATIC s7 200 - Overview

The Siemens S7 200 is a micro-programmable logic controller which can control a wide variety of devices to support various automation needs. The S7-200 monitors, inputs and changes outputs as controlled by the user program, which can include Boolean logic, counting, timing, complex math operations, and communications with other intelligent devices. It can control and communicate with devices like automatic pressure controllers, centrifuge pumps, water cooling systems. The STEP 7–Micro/WIN programming package provides a user-friendly environment to develop, edit, and monitor the logic needed to control the application that monitor devices. The Siemens Simatic S7 PLC's use PROFINET which is based on Ethernet for communication. There are over 3 million PROFINET devices deployed worldwide.

Siemens S7 200 PLCs boasts of a compact design, powerful performance, optimum modularity and open communications. This Micro PLC has been in successful use in millions of applications around the world âĂŞ in both stand-alone and net-worked solutions.

This PLC uses communication protocols such as PROFINET, an advanced version of MODBUS communication protocol. This protocol is also based on Ethernet. It also supports TELNET, HTTP, FTP, SNMP, MODBUS and S7 Comm protocols. Though this PLC is designed to be used to control critical systems, security was not a part of its design. The above mentioned protocols were not customized to facilitate secure communication. The standards were defined to create an interconnected environment between industrial automation devices and common networking protocols.Security was either ignored or rather was thought to be expensive on these devices. This makes it an easier target for attackers.

The S7 200 is also widely used for various applications because of its flexibility, usablilty and comptibility.

- **Open Communications**
- **:**
- **:**

Open Communication

4.2 Protocols

4.3 Design of HosTaGe ICS Honeypot

4.4 Perspective

Make points of Adversary Perspective and Administrator Perspective

5 Implementation

5.1 SCADA PLC Profiles

5.2 Protocol Implementation

5.3 Vulnerabilities

5.4 Attacks Log

5.5 Challenges

5.6 Detection of Multistage Attack Approach

5.7 Detecting malware

6 Evaluation and Results

6.1 Attack Data analysis

6.2 Conpot and HosTaGe attack comparison

6.3 Vulnerabilities of Siemens S7200

6.4 HosTaGe ICS - Performance Evaluation as an Android App

6.5 Observation and Analysis

7 conclusion and Future Work

Literatur

[1] NATIONAL CYBERSECURITY and US Dept. Of Homeland Security COMMUNICATIONS INTEGRATION CENTER. Ics-cert monitor. 2015.

[2] DELL. Dell security annual threat report 2015. 2015.

[3] A. Galante, A. Kokos, and S. Zanero. Bluebat: Towards practical bluetooth honeypots. In *Communications, 2009. ICC '09. IEEE International Conference on*, pages 1–6, June 2009.

[4] Dao gang Peng, Hao Zhang, Li Yang, and Hui Li. Design and realization of modbus protocol based on embedded linux system. In *Embedded Software and Systems Symposia, 2008. ICESS Symposia '08. International Conference on*, pages 275–280, July 2008.

[5] Ralph Langner. Stuxnet: Dissecting a cyberwarfare weapon. pages 49–51, May 2011.

[6] Feng-Li Lian, James R. Moyne, and D.M. Tilbury. Performance evaluation of control networks: Ethernet, controlnet, and devicenet. *Control Systems, IEEE*, 21(1):66–83, Feb 2001.

[7] Steffen Liebergeld, Matthias Lange, and Collin Mulliner. Nomadic honeypots: A novel concept for smartphone honeypots.

[8] Collin Mulliner, Steffen Liebergeld, and Matthias Lange. Poster: Honeydroid-creating a smartphone honeypot. *IEEE Symposium on Security and Privacy (S&P)*, 2011.

[9] Niels Provos. A virtual honeypot framework. In *Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13*, SSYM'04, pages 1–1, Berkeley, CA, USA, 2004. USENIX Association.

[10] S. Rubin, S. Jha, and B.P. Miller. Automatic generation and analysis of nids attacks. In *Computer Security Applications Conference, 2004. 20th Annual*, pages 28–38, Dec 2004.

[11] J.-P. Thomesse. Fieldbus technology in industrial automation. *Proceedings of the IEEE*, 93(6):1073–1101, June 2005.

[12] Emmanouil Vasilomanolakis, Shankar Karuppayah, Mathias Fischer, Max Mühlhäuser, Mihai Plasoianu, Lars Pandikow, and Wulf Pfeiffer. This network is infected: Hostage - a low-interaction honeypot for mobile devices. In *Proceedings of the Third ACM Workshop on Security and Privacy in Smartphones &#38; Mobile Devices*, pages 43–48. ACM, 2013.

[13] Emmanouil Vasilomanolakis, Shankar Karuppayah, Max Mühlhäuser, and Mathias Fischer. Hostage: A mobile honeypot for collaborative defense. In *Proceedings of the 7th International Conference on Security of Information and Networks*, pages 330:330–330:333. ACM, 2014.

[14] John W. Webb and Ronald A. Reis. *Programmable Logic Controllers: Principles and Applications*. Prentice Hall PTR, Upper Saddle River, NJ, USA, 4th edition, 1998.