Security Systems For Smart Grid Networks With Virtual Host

K. Ranjeethapriya[1], A. Bharanidharan[2]
[1, 2] Department of Computer Science and Engineering
[1, 2] Sri Ramakrishna Engineering College

Abstract- *Industrial control networks have large number of connected networks which are facing many security issues like intruders passing through the network and network traffic. There are many tools identified to monitor the intruders and network traffic in the network out of which ettercap is used to scan the port, MAC address and IP address for all hosts. Raspberrypi is a embedded hardware through which many softwares and tools can be installed and hosts in the network can be monitored. Raspberry pi can be updated regularly using system configuration. This hardware is controlled by administrators through individual PC's.*

I. INTRODUCTION

Network security deals with various techniques to identify real members taking part in communication sytems. Industrial control networks have many secret information that to be preserved from unauthorized users. Many industries and small grid infrastructure are taking prevention techniques to detect the intruders passing through the network. Raspberrypi hardware is connected to the physical devices in the industries and monitored through the PC.A single PI can scan large number of host and network entities connected through the network. To overcome the security issues faced by industrial networks ettercap is installed in raspberrypi and hosts were scanned. Ethernet cable is used for connecting PC, raspberrypi and network. Access point can be used to connect large number of raspberrypi in the industries. In this mechanism network entities(i.e) source, destination and port activity which is helpful for creating virtual networks using raspberrypi. This virtual host is created in the raspberrypi to divert the intruders activity. Hardware is already assigned with list of IP addresses that to be blocked or be diverted.

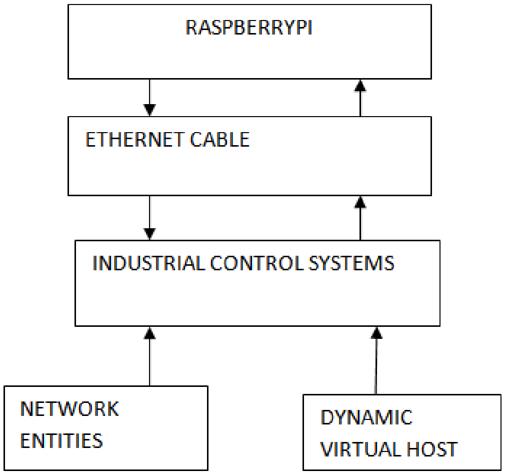


Fig 1: A Common ICS system connected with raspberrypi

The fig 1 shows the common industrial control sytem which is connected with hardware to obtain the information and for the creation of virtual host.

II. RELATED WORKS

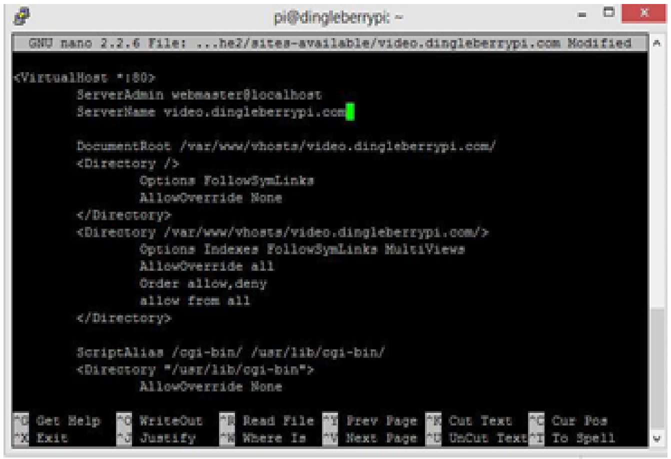
The Autonomic Intelligent Cyber Sensor to Support Industrial Control Network Awareness were discussed in[1]. When there comes the purpose of honeypots, informations can be gathered using active and passive scanning tools.Lightweight intrusion detection for networks is carried out using snort tool[2]. In which snort resembles the rule based intrusion detection system but only limited amount of information can cleaned by passive scanning tool was restricted in collecting the information from captured stream. The suitable tool that identify passive information is Ettercap[3]. Nmap is one of the active scanning tool that gives successful result in interrogating hosts on a network[4].Active scanning tool suffers from the problem of service request interruption on hosts especially in most of the industrial network control systems that may leads to damages. Dynamic host configuration and virtual honeypots for detecting intruders[5].DHP solutions were discussed in [6][7]. In the literature review the identification tools are used for providing network host identification are P0f [8], Tshark [9], Tcpdump [10], SinFP [11] and Ntop [12].

III. EXISTING SYSTEM

Automatic configuration in honeyd has a great advantage in solving the security issues. It differs from honeypot and honeynet which connects number of networks. These honeypots or honeynet is implemented in system to connect large number of hosts in a network. But low interaction honeypots can only gather basic informations. Ettercap is an effective tool for gathering network entities. A four step process is carried out for creating XML output, using this output honeyd is created automatically and updated. This honeyd enables one to connect large number of host on a network, so that attackers can be identified easily.The fig 2 shows the honeyd configuration which monitors unused ip addresses in the network. If an attacker uses it which is identified by virtual host with the help of ip spoofing.

IV. PROPOSED SYTEM

In this paper honeyd configuration is done using raspberrypi so that this device acts as a virtual honeypot. Ettercap tool is also implemented in raspberrypi to gather the network entity information and list of IP address to be restricted is marked. A log file is created using ettercap and list of IP address to be restricted is written in that hardware. This is the base for the creation of virtual host. A session is created in the system which is already connected with raspberrypi. Administrator can control the hardware manually using this session. Virtual host Apache is installed using python, mysql etc. This virtual host monitors the intruder activity and that particular IP can be redirected to this virtual host. This virtual host can then provide access or deny them based on their performance.



```
GNU nano 2.2.6 File: ...he2/sites-available/video.dingleberrypi.com Modified

<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        ServerName video.dingleberrypi.com

        DocumentRoot /var/www/vhosts/video.dingleberrypi.com/
        <Directory />
                Options FollowSymLinks
                AllowOverride None
        </Directory>
        <Directory /var/www/vhosts/video.dingleberrypi.com/>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride all
                Order allow,deny
                allow from all
        </Directory>

        ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
        <Directory "/usr/lib/cgi-bin">
                AllowOverride None

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

FIG 2:SAMPLE LOG FILE

V. IMPLEMENTATION AND DESIGN

The above proposed system is implemented by means of python and essential software's to obtain the required result.The steps are as follows:

- The hardware is connected to the control system with preinstalled ipscanner,putty and xming software.
- Using ettercap monitor the intruders activity using sniffing process and create a log file.
- Virtual host is created in the hardware to divert the intruders process.
- IP classification and IP extraction is done based on the log file.
- All the intruders is redirected to virtual host created and their activity is monitored

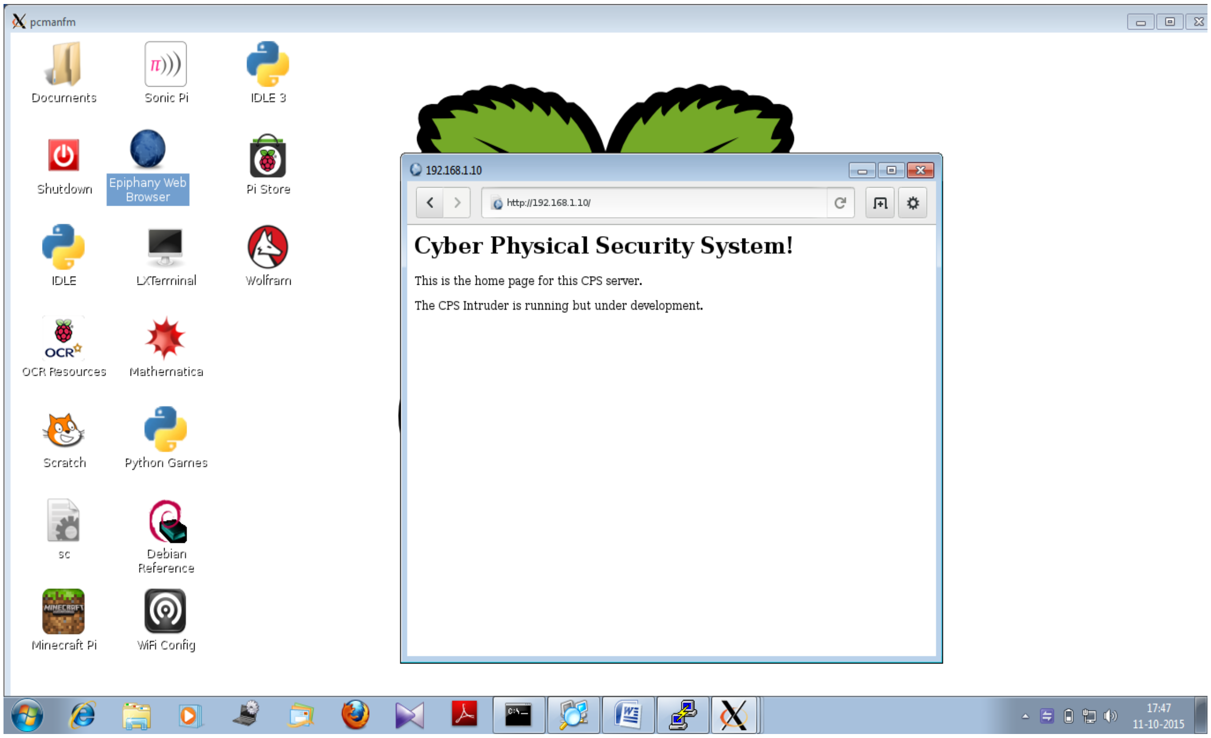
Initially the system should be installed with software like putty,xming and ipscanner. Raspberrypi to be connected with the system is installed with ettercap software for running in linux platform and wireshark for windows operating system. This software provides the network entities like source,port and MAC address. Using DNS server one end of LAN cable is connected to the laptop and other end to the hardware. Now, the IP address of hardware is identified through system using IP scanner and Putty software is used for creating new session and ssh forwarding that is done using x11 forwarding.

VI. ETTERCAP TOOL

The session is created in the system for controlling the hardware directly. Ettercap is made to run using terminal and number of host in the network is scanned. Network entities like source, port and MAC address is also displayed by this tool. Since there is large number of hosts target is fixed for any two host. Sniffing process is started to monitor the activity of that particular host. If any intruder continuously tries to steal the information from the organizations that intruders IP is displayed using Ettercap. ARP poisoning is also achieved through this tool. Finally a log file is created and given to the hardware. Using this file each host operating system is displayed using raspberrypi terminal.

Intruders tries to attack the sytem is identified and their activity is monitored simultaneously. Finally a virtual host is created in that hardware using terminal. Here apache is chosen as a virtual host or server to monitor the intruder's activity. Once the intruder is fixed its IP is diverted the virtual host which is similar to the real host. Intruder will think the emulated host as real host and request the services from that server,so that their activity is monitored. Once the intruder is fixed their access is restricted in the network. This virtual host is updated manually using the hardware terminal.

VII. RESULTS AND DISCUSSION

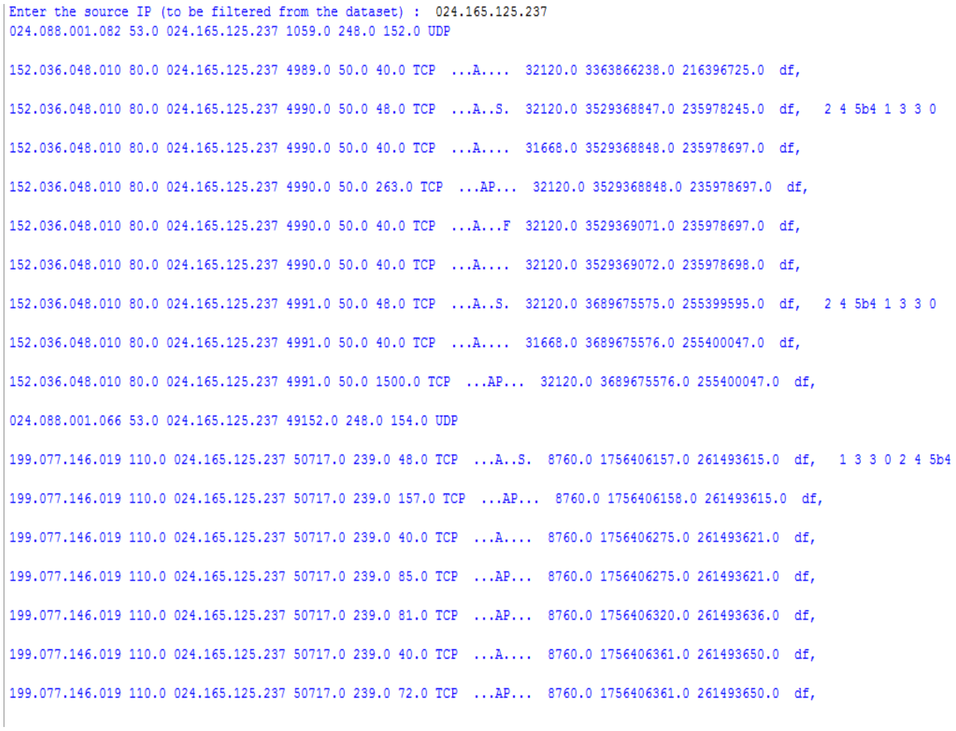


Cyber Physical Security System!

This is the home page for this CPS server.

The CPS Intruder is running but under development.

Fig 3: Virtual host



```
Enter the source IP (to be filtered from the dataset) :  024.165.125.237
024.088.001.082 53.0 024.165.125.237 1059.0 248.0 152.0 UDP

152.036.048.010 80.0 024.165.125.237 4989.0 50.0 40.0 TCP  ...A....  32120.0 3363866238.0 216396725.0  df,

152.036.048.010 80.0 024.165.125.237 4990.0 50.0 48.0 TCP  ...A..S.  32120.0 3529368847.0 235978245.0  df,   2 4 5b4 1 3 3 0

152.036.048.010 80.0 024.165.125.237 4990.0 50.0 40.0 TCP  ...A....  31668.0 3529368848.0 235978697.0  df,

152.036.048.010 80.0 024.165.125.237 4990.0 50.0 263.0 TCP  ...AP...  32120.0 3529368848.0 235978697.0  df,

152.036.048.010 80.0 024.165.125.237 4990.0 50.0 40.0 TCP  ...A...F  32120.0 3529369071.0 235978697.0  df,

152.036.048.010 80.0 024.165.125.237 4990.0 50.0 40.0 TCP  ...A....  32120.0 3529369072.0 235978698.0  df,

152.036.048.010 80.0 024.165.125.237 4991.0 50.0 48.0 TCP  ...A..S.  32120.0 3689675575.0 255399595.0  df,   2 4 5b4 1 3 3 0

152.036.048.010 80.0 024.165.125.237 4991.0 50.0 40.0 TCP  ...A....  31668.0 3689675576.0 255400047.0  df,

152.036.048.010 80.0 024.165.125.237 4991.0 50.0 1500.0 TCP  ...AP...  32120.0 3689675576.0 255400047.0  df,

024.088.001.066 53.0 024.165.125.237 49152.0 248.0 154.0 UDP

199.077.146.019 110.0 024.165.125.237 50717.0 239.0 48.0 TCP  ...A..S.  8760.0 1756406157.0 261493615.0  df,   1 3 3 0 2 4 5b4

199.077.146.019 110.0 024.165.125.237 50717.0 239.0 157.0 TCP  ...AP...  8760.0 1756406158.0 261493615.0  df,

199.077.146.019 110.0 024.165.125.237 50717.0 239.0 40.0 TCP  ...A....  8760.0 1756406275.0 261493621.0  df,

199.077.146.019 110.0 024.165.125.237 50717.0 239.0 85.0 TCP  ...AP...  8760.0 1756406275.0 261493621.0  df,

199.077.146.019 110.0 024.165.125.237 50717.0 239.0 81.0 TCP  ...AP...  8760.0 1756406320.0 261493636.0  df,

199.077.146.019 110.0 024.165.125.237 50717.0 239.0 40.0 TCP  ...A....  8760.0 1756406361.0 261493650.0  df,

199.077.146.019 110.0 024.165.125.237 50717.0 239.0 72.0 TCP  ...AP...  8760.0 1756406361.0 261493650.0  df,
```

Fig 4: IP extraction

VIII. CONCLUSION AND FUTURE ENHANCEMENT

In this paper we discussed some of the drawbacks faced by the existing system regarding virtual host configuration and updating process. This is effectively handled by our proposed system which updates the virtual system and usage of hardware for connecting large number of networks and host.

REFERENCES

[1] Todd Vollmer, Milos Manic, "Autonomic Intelligent Cyber Sensor to Support Industrial Control Network Awareness," IEEE Transactions on industrial informatics, VOL. 10, NO. 2, May 2014

[2] M. Roesch, "Snort: Lightweight intrusion detection for networks," in Proc. 13th Conf. Syst. Admin., Berkeley, CA, USA, Nov. 7–12, 1999, pp. 229–238.

[3] Ettercap network sniffer [Online]. Available: http://ettercap.sourforge.net/

[4] G. Lyon, Nmap Network Scanning. Palo Alto, CA, USA: Insecure.org, 2008 [Online]. Available: www.nmap.org

[5] N. Provos and T. Holz, Virtual Honeypots. Reading, MA, USA: Addison-Wesley, 2007.

[6] L. Chao, M. Sumiko, and K. Hirotsugu, "Dynamic hybrid system of honeypot and IDS for network security analysis," IPSJ SIG Notes, vol. 2013,no. 26, pp. 1–5, Dec. 2013

[7] C. Hecker, K. L. Nance, and B. Hay, "Dynamic honeypot construction," in Proc. 10th Coll. Inf. Syst. Secur. Educ., Adelphi, MD, USA, 2006, pp. 4880–4889.

[8] P0f [Online]. Available: http://lcamtuf.coredump.cx /p0f.shtml

[9] Tshark Network Analyzer [Online]. Available: http://www.wireshark.org/

[10] Tcpdump Packet Analyzer [Online]. Available: http://www.tcpdump.org/

[11] P. Auffret, "SinFP, unification of active and passive operating system fingerprinting," J. Comput. Virol., vol. 6, no. 3, pp. 197–205, Aug. 2010

[12] Ntop Network Traffic Probe [Online]. Available: http://www.ntop.org/