IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

A Survey on Cyber Physical System Security with Deceptive Virtual Host for Industrial Control Networks

Ranjeetha Priya. K[1], Sowmika. S[2], Bharanidharan. A[3]

Department of Computer Science and Engineering, Sri Ramakrishna Engineering College, Coimbatore, India[1, 2, 3]

Abstract: Network security plays a major role in monitoring the intruders in the industrial network and smart grid infrastructure. Industrial network area is suffering seriously with security issues they faced day-to-day. Network administrators should continuously monitor the network traffic to detect intruders in the network. Due to lack of security in the network, network traffic and intruders is becoming a major challenge. This paper presents the effective techniques, tools and approaches such as ettercap, wireshark, SCADA and game theoretic approaches which monitor the intruders in the network and network traffic. Thus the security issues can be improved by below mentioned techniques.

Keywords: SCADA, WAP, DNP3, ICMP.

I. INTRODUCTION

Cyber physical security system is mainly used in industrial complex control systems. Security in this networked system like industries, smart grid infrastructure and SCADA networks is a major concern [1]. Previously, large amount of wireless sensors can be connected to physical systems and report it to one wireless access point (WAP). Now, network monitoring techniques like honeypots [2], intrusion detection systems for SCADA networks [3] and industrial networks is deployed to monitor the intruders and network traffic in the network. Generally control systems have static topologies, regular traffic and simple protocol than any other networks. Several models can be constructed to monitor these abnormalities. Intruders generally follow a pattern, technique to attack the control system. So, using monitoring tools these patterns are identified and intruders are detected. Cyber physical security issues in smart grid infrastructure can be solved using strategies games by introducing test beds in the control system network. The attack done by intruders can be forwarded to virtual host created by any software or hardware. This effectively restricts the access of unauthorized intruders from the network.

These security issues in cyber physical security systems are reduced by means of several tools, techniques and approaches.

II. TOOLS,TECHNIQUES AND APPROACHES

1. Ettercap

Attacks by intruders are not simple and most of them are complex and it is a big challenge in industrial control systems. There are two types of attack, active and passive attack. Active attack alters the system resources and change the data and send it to the users which can be easily identied by doing spoofing or ARP poisoning using ettercap tool[5]. Passive attack simply monitors the network to gain information which can also be identified using this tool by doing port scanning. Spoofing done by this tool is nothing but each computer needs to communicate with other computer needs an IP address. In this technique, fake or virtual host is created originating like real host IP address [4]. This is mainly done to steal the intruder's information by using this virtual host. Ettercap works well with IP-based, MAC-based and ARP-based models to gather many network related information.

Other tools like snort[9],p0f[12],tcpdump[13],tshark[14] and ntop[15].

A) OS fingerprinting:

OS fingerprinting is based on information gathered by tools like p0f and ettercap while requesting for web page or pinging the website. Since usually hacker does not provide any traffic it is very difficult to identify the hackers or intruders because this traffic identies the remote host OS easily. By analysing the packets travelling across the network using ettercap OS can be identified. Sometimes fingerprint act as sniffer which does not put any traffic in the network. Different operating produce different packets which can be identified by ettercap tool. By analysing DHCP request, HTTP request, ICMP request OS fingerprinting can be achieved.

B) ARP poisoning:

ARP poisoning puts the attacker or virtual host in position to intercept communication between two systems. Host A believes that it is communicating with host B but it is actually sending request to virtual host to identify the attributes of the intruders. The first step in ettecap is identifying the list of IP addresses and their MAC addresses then specify the interface. The –t option specifies the particular host to arp poison, if the host is not specified, all host in the LAN will be poisoned. Arpspoof redirects packets from target host to virtual host by forging ARP replies. Ettercap tool is installed in industrial network

control system to monitor the network and identifying the intruders. XML output generated by ettercap is used for creating virtual host and list of IP addresses. Dynamically virtual host is created for OS mapping and for forwarding the intruders request to that emulated host. This virtual host in network control system is updated depending upon the changing environment. Since ettercap runs only in Linux operating system, wireshark is used for windows operating system to identify network entities and intruders in the network.

2. Wireshark

Many industries and smart grid infrastructure [6] uses windows as operating system. So this can be used to analyse the packets transmitted across the network. Wireshark automatically puts the interface into promiscuous mode so that traffic is visible on that network. Since packet analysed using promiscuous mode does not identifies all traffic in the port it has more disadvantage. Wireshark and tshark is used to perform traffic capture. Using this network traffic with high privileges can only be identified for industrial networks. This is provided with list of IP addresses which filters intruders from the network. Apart from these Nmap is an effective tool for port scanning which provides port entities, host discovery and operating system detection and provides MAC addresses. Since it generates traffic on the network which is the major issue in industrial networks it is not chosen for identifying network entities. Thus ettercap is effectively chosen for identifying intruders, network traffic and operating systems of several hosts in network controlled systems.

3. Modbus for SCADA networks

SCADA networks are mainly used in industrial control networks and many smart grid infrastructure. These SCADA systems usually suffer from many damages and malfunction. Modbus[8] is mainly used to communicate between any two intruder monitoring systems. It identifies the amount of traffic present in the network. There are several communication patterns for intruders which is decided by snort rules. These rules are integrated into the control systems and attacks were identified based on the scenario. Snort is a open source network based intrusion detection system used to analyse the traffic in the network using Modbus packets. The rule in snort is also used to detect the attacks. Snort can be operated in three modes in sniffer mode, it reads the packets and just display it, in packet logger mode it log the packets in the disk, in intrusion detection mode the rules monitor the network traffic in the network and identify the possible attacks.

Initially Modbus is connected between human machine interface and PLC (programmable logic controller). This intrusion detection system monitors the modbus packets and the packet pattern, characteristics periodically from PLC devices. Based on the pattern identified the network traffic and attacks were detected. Several model based techniques can also be implemented for Modbus TCP networks. This approach is mainly based on signatures of known attacks. It verifies the signature of an attacker whether they are known attack or unknown attack because unknown attack have different characteristics. The signature is verified by designed models to give access to the services. It it is an attack the modbus does not provide access to get the services from the provider in control systems. Many industrial control networks uses this cyber devices to identify the attackers and network traffic in the network.

A) DNP3 protocol:

Industrial control network is facing a large security issues in analysing the untrusted packets. DNP3 protocol is chosen for analysing and monitoring the untrusted packets based on critical analysis technique. These protocol is also used for identifying attacks in the network systems.DNP3 protocol is more reliable but it is not secure from attacks by hackers that disrupt industrial control systems. In smart grid applications and many physical networks many works and models have been implemented to add secure features to DNP3 protocols. DNP3 protocols can be implemented cyber devices in any network oriented devices because it is interoperable. Since modbus model is a older technique than DNP3 protocol it is selected to identify the network traffic and intruders in industrial control networks by creating virtual host. Virtual host can also be created in DNP3 protocol in many control systems.

These are the various techniques to identify the amount of network traffic and intruders in industrial control networks and smart grid infrastructure.

4. Game theoretic approach

Game theoretic approach is chosen for solving the security issues in wide area networks. It monitors and protects the wide area network. This game theory can be used to detect any kind of attack in control systems. Impacts of various security issues is analysed using its characters and impact of attack is identified.

Using this system defender activity and attacker motivations is characterised. Various probabilities is obtained from this approach and attack cost is evaluated. Using the cost attacker motivation is obtained and their access is denied in the wide area networks. General game theory is formulated to identify the defender strategy to identify attacker actions. Substation is a technique used to protect the security messages transferred between defenders. The messages can be encrypted to protect from attackers in the large area networks. This approach is self updatable and adapt to the changing environment. Based on the model developed by this approach cyber attack scenario is modelled and various information's is gathered from attacker and transferred to the defender.

III. CONCLUSION

Thus in this paper, various tools, techniques and approaches have been discussed to identify the intruders in the network. Ettercap tool is chosen for identifying the man in the middle attack effectively. Wireshark is used for windows operating system. Mainly game theoretic approach identifies character and impact of the attacks. Using these techniques network traffic, attack and intruders are effectively identified.

ACKNOWLEDGEMENT

I would like to express my sense of profound gratitude to all the People who have helped me to gain more knowledge about research papers. I also wish to thank my guide who has helped me to complete the survey paper successfully and also extend my thanks to many of the journals and the websites which has helped to refer many research papers and make it to publish successfully.

REFERENCES

[1] Aditya Ashok, Adam Hahn, Manimaran Govindarasu, "Cyber-physical security of Wide-Area Monitoring, Protection and Control in a smart grid environment," in Journal of Advanced Research, USA, 2014, pp. 481-489.
[2] N. Provos and T. Holz, Virtual Honeypots. Reading, MA, USA: Addison-Wesley, 2007.
[3] Igor Nai Fovino, Alessio Coletta, Andrea Carcano, and Marcelo Masera, "Critical State-Based Filtering System for Securing SCADA Network Protocols," IEEE Transactions on industrial electronics, VOL. 59, NO. 10, OCTOBER 2012.
[4] 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.
[5] Ettercap network sniffer [Online]. Available: http://ettercap.sourforge.net/
[6] O. Linda, T. Vollmer, and M. Manic, "Improving cyber-security of smart grid systems via anomaly detection and linguistic domain knowledge," in Proc. IEEE Symp. Resilience Control Syst., Salt Lake City, UT, USA, Aug. 2012.
[7] G. Lyon, Nmap Network Scanning. Palo Alto, CA, USA: Insecure.org, 2008 [Online]. Available: www.nmap.org
[8] Miami Beach, Florida, "Using Model-based Intrusion Detection for SCADA Networks," Computer Science Laboratory, SRI International, December 2006.
[9] M. Roesch, "Snort: Lightweight intrusion detection for networks," in Proc. 13th Conf. Syst. Admin., Berkeley, CA, USA, Nov. 7–12, 1999, pp. 229–238.
[10] 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
[11] 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.
[12] P0f [Online]. Available: http://lcamtuf.coredump.cx/p0f.shtml
[13] Tshark Network Analyzer [Online]. Available: http://www.wireshark.org/
[14] Tcpdump Packet Analyzer [Online]. Available: http://www.tcpdump.org/
[15] Ntop Network Traffic Probe [Online]. Available: http://www.ntop.org/