ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

INTRUSION DETECTION IN INDUSTRIAL CONTROL SYSTEM BY PACKET BEHAVIOUR BASED ANALYSIS

[1] G Elavarasan, [2] Y Suresh,
[1] PG Scholar, [2] Assistant professor,
[1, 2] Department Of Information technology,
[1, 2] Sona College of Technology,
[1, 2] India.

ABSTRACT: Nowadays the production, business and entertainment environment uses Industrial Control Systems (ICSs), which are designed, implemented, and deployed in these environment. First priority is giving to safety, while dealing with the physical devices. ICSs are commonly split into two subsystems - Programmable Logic Controllers (PLCs) and Supervisory Control and Data Acquisition (SCADA) systems. Use to achieve high safety, allow engineers to observe states of an ICS, and perform various configuration updates. The proposed System describes the Packet Behavior based analysis which examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service attacks, certain forms of malware, and policy violations. This approach recognizes attacks based on what they do, rather than whether their code matches strings used in a specific past incident.

Keywords: [Industrial Control Systems (ICSs), Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition (SCADA), Intrusion Detection System (IDS), Local Area Network (LAN), Expected Chance of Successful Attack (ECSA).]

INTRODUCTION

Safety is a number one priority when dealing with physical devices. ICSs are commonly split into two subsystems – PLCs and SCADA systems - to achieve high safety, allow engineers to observe states of an ICS, and perform various configuration updates. PLCs are small processing systems which are able to modify the behaviour of the controlled devices and receive input from the system's sensors. SCADA systems allow engineers to monitor the ICS state and modify its parameters as needed.

As the price of networking devices fell, and the Internet received global adoption, the benefits of attaching ICSs to wide and global area networks became evident. Engineers gained an ability to monitor and fix critical problems remotely, eliminating travel times to the ICS, which gave them more time to work on problem solving when the system malfunctioned. The price of implementing geographically dispersed ICSs, where PLCs and SCADA systems may be miles away from each other, decreased with the spread of the Internet. The critical infrastructure Smart Power Grid is one such ICS where each house has its own controller - a smart meter – that transmits usage information to the power company and may turn off the house’s power for maintenance or lack of payment.

One of the approaches to securing the communication of network attached ICSs is a network telemetry-based Intrusion Detection System (IDS). Such a system operates by measuring and verifying data that is transmitted through the network but is not inherently the data used by the transmission protocol. Network telemetry may include temporal data of packet arrival, packet sizes, session times and sizes, amount of dropped packets and more. To achieve this, telemetry-based IDSs need to monitor all packets traversing the ICS network, have a running average of the telemetry data, and be able to alert system engineers when anomalies in traffic are detected.For this infrastructure is very important but only few systems are supporting the critical infrastructure like air-gapped. Another challenge in ICS to be discussed is procurement, installation and maintenance because the controlling equipments using which to be installed, configured and run by plant engineers on site in an effective manner. To overcome the security threats in the modern world an advanced security system should develop to overcome the critical cyber-physical system drawbacks. It was connected by means of Ethernet network and for protecting the control system the network monitoring system is the major one in providing a fine solution from network intruders.

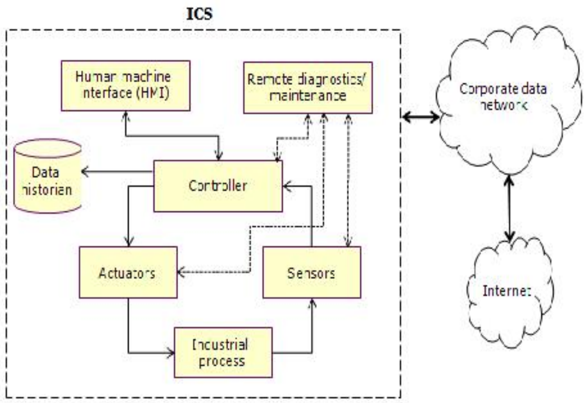


Figure - 1 A common ICS System

The fig 1 shows the industrial control system and the overall process are monitored by the network monitor system through internet. In this mechanism the configuring devices are huge in number and also high in deployment. For example consider a AMI system advanced metering infrastructure in which moreover 1500wireless sensors are to be connected to a multiple wireless access point (WAP). In this case a monitoring system should be effective in detecting the accuracy and precision rates. In this mechanism NEI (network identity information) plays a vital role in monitoring the traffics in the network, by means of gathering the information from source, destination, and port activity. That information’s are useful in creating a representative virtual network.

PLCs are small processing systems which are able to modify the behavior of the controlled devices and receive input from the system’s sensors. SCADA systems allow engineers to monitor the ICS state and modify its parameters as needed. Existing system uses a telemetry based IDS. The goal of Network Telemetry based IDSs is to protect PLCs and the underlying physical plant from malicious activity unauthorized access and control of PLC hardware. To achieve classification, the IDS must receive the entire network packets sent to the PLCs. Telemetry is an automated communications process by which measurements are made and other data collected at remote or inaccessible points and transmitted to receiving equipment for monitoring.

Intrusion Detection System (IDS) are software or hardware systems that automate the process of monitoring and analyzing the events that occur in a computer network, to detect malicious activity. Stuxnet was one of the largest and most complicated attacks deployed that targeted an industrial control system. Stuxnet was a worm, a malicious application that is capable of replicating and spreading itself over a network. The proposed System describes the Packet Behavior based analysis which examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service attacks, certain forms of malware, and policy violations. This approach recognizes attacks based on what they do, rather than whether their code matches strings used in a specific past incident.

RELATED WORK

For an effective control system various researchers were discussed about complex control system and their working strategies in which a compromised control system was discussed about the security, public safety, and industrial consequences [1] [2]. In which [3] [4] were discussed about the critical cyber physical system and their security threats globally. On discussing about network monitoring system a protective control system is analyzed in [5] [6]. A deceptive system for monitoring solution with enhanced approach in accuracy and precision rates were considered in [7] [8]. According to John ousterhout in a faithful honeypot automation construction there are four common factors are involved in order to turn the deployment of enemy into a friend [9]. In a network system it is difficult list the definitive attributes of a network host which are required to grab the attacker attentions. When the propose of honeypot raise there are primary aspects in gathering the information one is active scanning and another term is passive scanning. Most of the previous work were discussed about the passive scanning in which was implemented with P0f and occasionally Snort [10] [11]. A

suitable tool which is commonly used for gathering passive information is Ettercap[12]. In which snort resembles the rule based introduction system but only limited amount of information can gleaned by passive scanning as the tool was restricted in collecting the information from captured stream [12]. On dealing these situations active scanning is more powerful and successful. In which Nmap is one of the active scanning tool that proved successful in interrogating hosts on a network [13]. But active scanning is also suffers from the problem of service interruption on hosts especially in most of the control systems. That pings on older system which may leads to physical damages [14]. On this Lance Spitzner has introduced a dynamic honeypot in 2004 (DHP) that is a concept of automatic configuring based on the gleaned information from the network traffic. The DHP requires two factors such as network information gathering and deploying honeypot configuration. More about DHP solution were discussed in [15] [16]. On discussed about the previous works supervisory control and data acquisition (SCADA) Honeynet project by Matthew Franz and Venkat Pothamsetty of the Cisco Critical Infrastructure Assurance Group (CIAG) were remarkable one in simulating a set of services for a PLC [17]. According to digital bond Inc is a research group for consulting the control systems which utilizes two machines one as monitoring tool such as snort and another one is for simulating the PLC [18].

In the literature review the tools which are used for providing network host identification are P0f [19], Tshark [20], Ettercap, Snort [21], Tcpdump [22], SinFP [23] and Ntop [24]. But these tools are not effective in accurate execution on the test sensor systems. In the Anomaly behavior (AB) its implementation and works are discussed by the author in [25] which configure the virtual honeypot IP addresses and send alerts based on any activity. But this approach was not effective according to the real time situations.

EXISTING SYSTEM

PLCs are small processing systems which are able to modify the behavior of the controlled devices and receive input from the system’s sensors. SCADA systems allow engineers to monitor the ICS state and modify its parameters as needed. Existing system uses a telemetry based IDS. The goal of Network Telemetry based IDSs is to protect PLCs and the underlying physical plant from malicious activity unauthorized access and control of PLC hardware. To achieve classification, the IDS must receive the entire network packets sent to the PLCs. Telemetry is an automated communications process by which measurements are made and other data collected at remote or inaccessible points and transmitted to receiving equipment for monitoring.

PROPOSED SYSTEM

Intrusion Detection System (IDS) are software or hardware systems that automate the process of monitoring and analyzing the events that occur in a computer network, to detect malicious activity. Stuxnet was one of the largest and most complicated attacks deployed that targeted an industrial control system. Stuxnet was a worm, a malicious application that is capable of replicating and spreading itself over a network. The proposed System describes the Packet Behavior based analysis which examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service attacks, certain forms of malware, and policy violations. This approach recognizes attacks based on what they do, rather than whether their code matches strings used in a specific past incident.

PACKET BEHAVIOUR BASED ANALYSIS

Newly implemented Packet Behaviour based analysis is efficient and provide fast result. In future we can enhance the accuracy of the session classifier may be improved by different methods. We can able to differentiate between the delays introduced by networking hardware, such as routers, and delays introduced by the client machine’s hardware and software should increase the accuracy of the classifier. Future work includes acquiring an accuracy curve for attacks initiated from different hops from the target, determining the importance of software changes for detection accuracy In this analysis source and destination are set at larger distance, the source transmits the data packets to destination through the intermediate hop nodes using TCP/IP user State Full protocol.

ALGORITHM AND EXPLANATION

By defining, implementing, and experimenting with a new probabilistic quantification model that we combine with our novel optimization problem as described. Our probabilistic quantification model, referred to as success measurement model, quantifies the vulnerabilities of networked components and resources, by computing the expected chance of successful attack (ECSA) at every attack step, which is represented by an attack graph node.The computation in the success measurement model requires three sets of inputs, which are a set of attack steps, a set of network configuration and potential vulnerabilities, and a set of ground facts. The first set includes the steps necessary to execute a targeted attack in a network. These steps represent intermediate attack goals such as compromising a machine that has an internal connectivity with a targeted server. In addition, the attack steps also describe the various parallel choices available to an attack when achieving a specific target. The second set includes the network configurations and vulnerability data that collectively provide host software installations, inter host connectivity, running services and connections, and known or potential software vulnerabilities. The third set contains the ground fact values that describe the vulnerability, availability, and connectivity of various network configurations. In our implementation, the first two sets of inputs (i.e., the attack steps and the network configuration data) are taken from dependency attack graphs.

The system administrators use vulnerability assessment tools (such as OVAL) to explore the configurations and vulnerability data in their networks. The output of such assessment is provided as an input to attack graph generation tools. Attack graph generation tools (such as MulVAL) often include customized predefined attack step rules that are applied to the configurations and vulnerability data of a network and produce a plain (that is, not quantified) attack graph. The additional step required by our model is to develop a set of ground fact values. The values bootstrap the computation of success probabilities throughout an attack graph.The output of the computation based on our success measurement model is the input to the security optimization model .Using the security improvement model, we transform the quantified attack graph from the success measurement model into a mathematical program. The resulting mathematical program includes an additional set of data that represent various network security defense strategies. In the tool that we developed, the security administrators simply feed this information as logical predicates such as ips_installed(T, E), which describes a potential installation of an intrusion prevention system of type T and security effectiveness E. The effectiveness value E is a score estimated by the system administrator based on prior experiences and available effectiveness data.

MODULE DESCRIPTION

REGISTRATION PHASE

The mobile nodes are designed and configured dynamically, designed to employ across the network, the nodes are set according to the X, Y, Z dimension, which the nodes have the direct transmission range to all other nodes.

PATH IDENTIFICATION

The source and destination are set at larger distance, the source transmits the data packets to destination through the intermediate hop nodes using TCP/IP user State Full protocol,

MOBILE AGENT SYSTEM

MDP scheduling the delay is high because of allocating a time slot the data delivery from transmitter to receiver takes a long time thus results in delay constraint. So MA (mobile agent) concept is proposed to reduce the time delay and also serve as a ACK acknowledgement for secure data delivery from transmitter to receiver.

SECURITY ANALYSIS

To achieve more secure and privacy in multicast routing, RSA cryptocraphy is implemented for data authentication and privacy protection. By above process the adversary nodes are in in active state, the false injection packets does not affects the receiver in any constraint.

GRAPH EXAMINATION

The performance analysis of the existing and proposed work is examined through graphical analysis. IV. SIMULATION AND RESULT We are constructing attack graphs for sensor placement [14].Attack graphs predict the various possible ways of penetrating a network to reach critical assets.

Then place IDS sensor to cover all these paths, using the fewest numbers of sensor. We characterize expected monitoring costs for the network. We restrict the costs to a range of values 1 to 10 to express relative monitoring costs for different locations on a network. Router nodes 1 and 2 are assigned a cost of 8,router nodes 3,4,5 and 9 are assigned cost of 7,router nodes 8 and 10 are assigned cost of 6,router nodes 6,11,15 are assigned cost of 5.We assign a flat cost of 4 for all the other subnet router nodes.

They are designed different. tcl script through NS2 simulator (For here showing v3.tcl,v4.tcl,v5.tcl,normal1.tcl).For attack Simulation Denial of Service(DOS) attack(eg.Normal1.tcl) is simulated for attack penetration. For probing of attack Worm attack (eg.Worm.tcl) is simulated

A. Attack Graphs

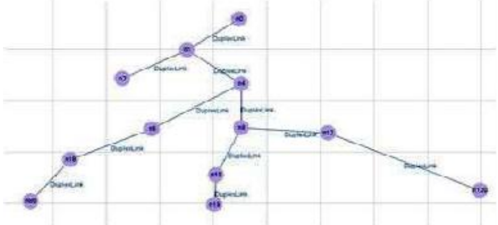
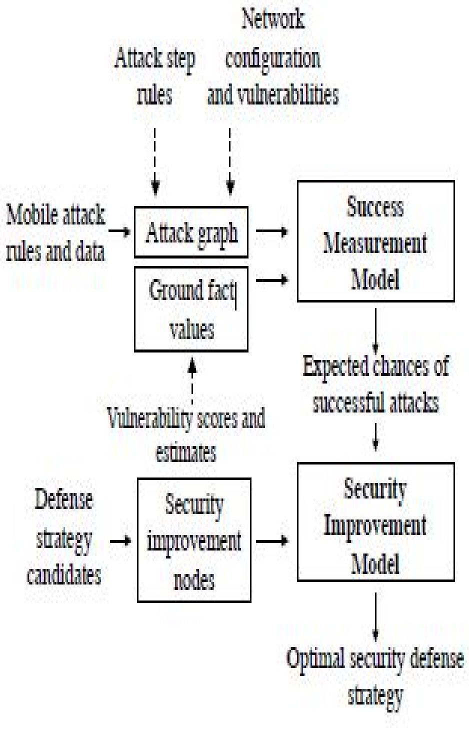


Figure – 2 V5. tcl Attacker Node `26, 40, 5`

IMPLEMENTATION DESIGN

Our models work based on three input sets from attack graph generators as well as initial belief values associated with potential vulnerabilities and network configuration data.Our security improvement model uses the computed probabilities from the success. The above explained proposed system is implemented by means of tcl with supporting software's to obtain the expected results.


Network configuration and vulnerabilities
Attack step rules
Mobile attack rules and data
Attack graph
Ground fact values
Success Measurement Model
Expected chances of successful attacks
Vulnerability scores and estimates
Defense strategy candidates
Security improvement nodes
Security Improvement Model
Optimal security defense strategy

CONCLUSIONS

The developed intrusion detection system can identify communication of different machines by analyzing telemetry data of the network. The classification is done at two different server-client separation stages which allows the IDS to differentiate between the inside and outside originating traffic. The IDS was able to achieve accuracy with no false negatives and false positives. While these values are, on average, near accuracies of other IDS, the use of network telemetry data as features results in a harder-to-obfuscate IDS. The IDS should notify system engineers of all detected intrusions and let them decide on further actions.

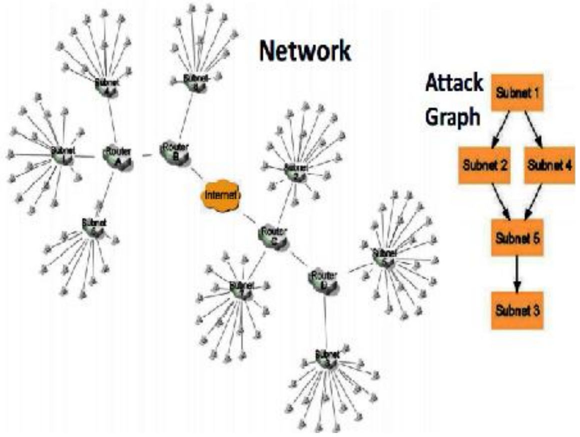


Figure - 3 Attack Graph Diagram

REFERENCES

[1] "Recommended practice: Improving industrial control systems cybersecurity with defense-in-depth strategies," Department of Homeland Security, Tech. Rep., 2009.

[2] J. Gao, J. Liu, B. Rajan, R. Nori, B. Fu, Y. Xiao, W. Liang, and C. Philip Chen, "Scada communication and security issues," Security and Communication Networks, vol. 7, no. 1, pp. 175–194, 2014.

[3] L. T. Heberlein and M. Bishop, "Attack class: Address spoofing," in Proceedings of the 19th National Information Systems Security Conference, 1996, pp. 371–377.

[4] S. Ponomarev, N. Wallace, and T. Atkison, "Detection of ssh host spoofing in control systems through network telemetry analysis," in Proceedings of the CIRSC conference, 2014, pp. 1–12.

[5] N. Falliere, L. O. Murchu, and E. Chien, "W32. stuxnet dossier," White paper, Symantec Corp., Security Response, 2011.

[6] B. Schneier, “The story behind the stuxnet virus,” Forbes. com, 2010.

[7] A. Matrosov, E. Rodionov, D. Harley, and J. Malcho, “Stuxnet under the microscope,” ESET LLC (September 2010), 2010.

[8] S. Ponomarev, N. Wallace, and T. Atkison, “Detection of ssh host spoofing in control systems through network telemetry analysis,” in Proceedings of the CIRSC conference, 2014, pp. 1–12.

[9] N. Wallace, S. Ponomarev, and T. Atkison, “A dimensional transformation scheme for power grid cyber event detection,” in Proceedings of the CIRSC conference, 2014, pp. 1–12.

[10] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. N. Fovino, and A. Trombetta, “A multidimensional critical state analysis for detecting intrusions in scada systems,” Industrial Informatics, IEEE Transactions on, vol. 7, no. 2, pp. 179–186, 2011.