University of BRISTOL

DEPARTMENT OF COMPUTER SCIENCE

Viability of probe-toolset detection within an OT network, providing another indicative vector to use in IDS.

Zack Dove

A dissertation submitted to the University of Bristol in accordance with the requirements of the degree of Bachelor of Science in the Faculty of Engineering.

Sunday 9th February, 2020

Declaration

This dissertation is submitted to the University of Bristol in accordance with the requirements of the degree of BSc in the Faculty of Engineering. It has not been submitted for any other degree or diploma of any examining body. Except where specifically acknowledged, it is all the work of the Author.

Zack Dove, Sunday 9th February, 2020

Contents

Chapter 1

Introduction

The societal services that form critical national infrastructure (CNI) such as water and waste treatment, electricity generation, and public transport all rely upon industrial control systems (ICS). The frequency of attacks on CNI has been increasing over the years, with recent examples of Stuxnet[1], Triton[2] and the 2015 Ukrainian Power Outage attack[3] reaching news headlines across the world.

CNI is traditionally composed of two parts, information technology (IT) and operational technology (OT). The former relates to technology involved in the processing and communication of information, whilst the latter relates to the technology used in systems that interact physically with the real world. Industrial control systems (ICS) are just one example of OT.

	IT	**OT**
Users	Companywide, from HR, to CEO	Engineers
Priority	Confidentiality, Integrity, Availablity	Safety, Availability, Integrity, Confidentiality
Devices	Laptops, Servers, Databases	PLCs, HMIs, Industrial Equipment, SCADA Control
Scope	General	Specialised
Protocols	HTTP, HTTPS, RDP	Modbus, Profinet, EtherNet/IP
Device Lifespan	3-5 years	15+ years

OT appliances such as valves were originally controlled individually and manually, until we began to centralise command by transmitting individual analogue controls to a control room. Whilst this was a great improvement, the analogue connections and interfaces were inflexible, short ranged, physical malfunctions were commonplace and needed to be manually rewired each time a device was added or changed, and so we digitized them. Analogue controls were replaced with programmable logic controllers (PLCs), which communicate between the physical output devices and the control system, meaning that connections are much easier to manage and scale. PLCs are at level 1 in the Purdue model shown in Figure 1.1. Real world settings have hundreds if not thousands of these PLCs that can be spread across many locations.

PLCs are designed to be extremely rugged, lasting for 20 to 30 years and operating under the variable vibration, temperature and humidity conditions found in industrial environments. Many OT components were never designed to be connected to a network meaning that security was not a design consideration, and there are many well known vulnerabilities[4][5][6]. Vulnerabilities are addressed through security patches, but many operators choose not to patch since they cannot afford their devices to go offline and are worried about updates causing compatibility issues with the other legacy equipment.

Recently, we have seen the introduction of the Internet of Things (IoT) - a system of interconnected devices, machines and objects that communicate together without human interaction. Smart thermometers, lights and even toasters can be found in many households. OT environments can benefit greatly from the enhanced levels of visibility and automation provided IoT devices and systems, leading to the use of IoT devices in layers 0-3 of the Purdue model in Figure 1.1. This has bee termed the Industrial Internet of Things (IIoT). Figure 1.2 shows how IIoT causes a convergence of IoT and OT, leading to systems using a mixture of traditional ICS devices and modern IoT devices. The move to convergent networks also means a move to large attack spaces, and the research into this field is very young.

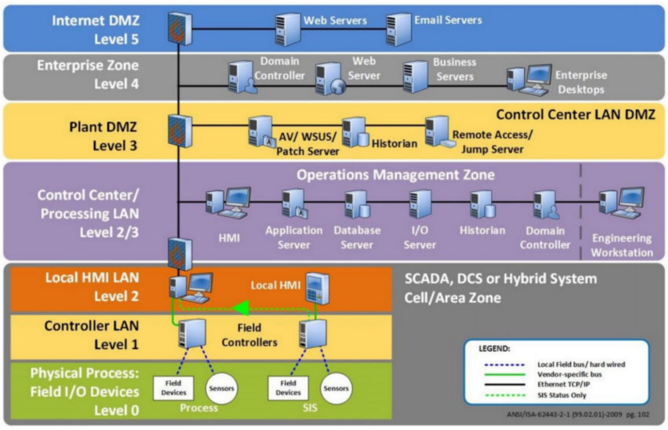

Figure 1.1: The Purdue model showing a typical OT architecture[7][8]

Interconnected networks of IT devices have been around for a long time, meaning that both sides of attack and defence in IT are sophisticated. We cannot use all of the same techniques and technologies used to prevent/mitigate attacks on IT for OT, since the protocols used for communication are different and many legacy ICS devices are very sensitive and can be bricked by something as simple as a port scan[9]. As a result, we must come up with novel security solutions.

This project/report/thesis investigates whether we can detect which toolset is being used to probe an OT network, thus providing another indicative vector to use in intrusion detection, strengthening OT security. First we discuss background information and related work (Section 2), then we lay out our methodology for the experiment (Section 3), following that we analyse the results (Section 4) and provide a conclusion (Section 5).

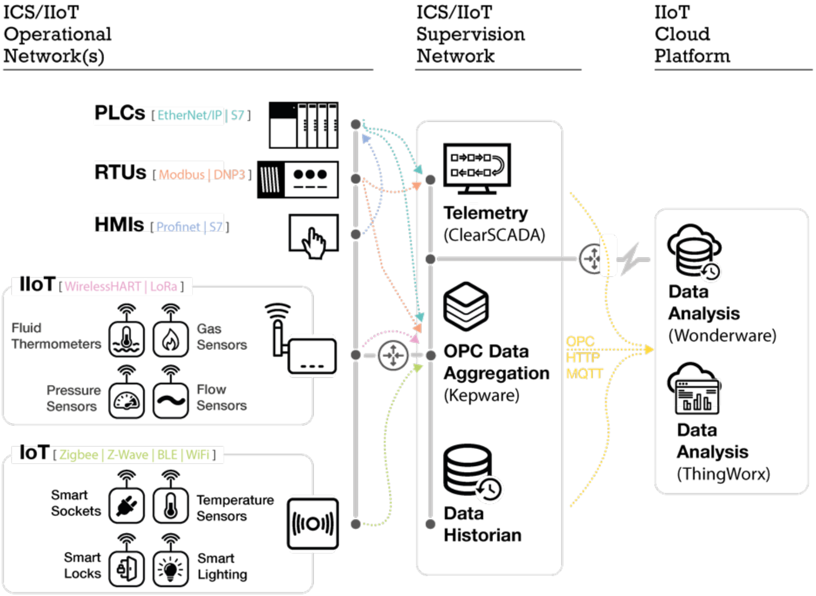
ICS/IIoT Operational Network(s)
ICS/IIoT Supervision Network
IIoT Cloud Platform
PLCs [EtherNet/IP | S7]
RTUs [Modbus | DNP3]
HMIs [Profinet | S7]
IIoT [WirelessHART | LoRa]
Fluid Thermometers
Gas Sensors
Pressure Sensors
Flow Sensors
IoT [Zigbee | Z-Wave | BLE | WiFi]
Smart Sockets
Temperature Sensors
Smart Locks
Smart Lighting
Telemetry (ClearSCADA)
OPC Data Aggregation (Kepware)
Data Historian
OPC
HTTP
MQTT
Data Analysis (Wonderware)
Data Analysis (ThingWorx)

Figure 1.2: A typical IIoT environment with a mix of legacy and non-legacy devices and protocols interacting with one another[10].

Chapter 2

Background

2.1 Attack Paths

Hutchins et al. [11] describe the traditional cyber kill chain, composed of different sections which can be broken down into smaller individual tasks: Reconnaissance, weaponization, delivery, exploitation, installation, command control, action on objective. Assante & Lee explain that attacks targeting OT differ in that the final stage – 'action on objective' of the traditional kill chain leads to further stages[12]. The purpose of 'action on objective' is to gather information about the victims network and the OT connected to it, and then instigate a second kind of kill chain. The sensitivity of the equipment mentioned earlier means that host discovery and network exploration may cause unintended effects such as devices malfunctioning. Armed with command and control the in the victims network and a knowledge of the OT connected, attackers can weaponize or develop a new exploit targeting the ICS. If the attack is to be successful, it should be tested first – this limits the scope to governments or well resourced organisations, since the equipment required to mimic the victims network is extremely costly. Lastly, the attack is launched, which may intend to cause: loss of view, denial of view, manipulation of view, denial of control, loss of control, manipulation of control, activation of safety, denial of safety, manipulation of safety or manipulation of sensors and instruments.

2.2 Techniques To Prevent Attacks

There are a number of techniques used to mitigate and prevent against attacks.

- Separation is used to stop attackers moving from moving easily from one part of a network to another. It is common practice that the devices on corporate networks are kept separate from the internet, and connection is managed through the DMZ. This can easily be breached by connecting an ethernet cable or connecting a device over wireless communications.

- Patch management aims to remove vulnerabilities on individual devices by fixing erroneous software through updates, however this is slow, and many operators worry that security updates will break devices or lead to more vulnerabilities. Patch management is also ineffective against zero day attacks.

- Firewalls work by analysing each individual packet flowing through – packets are dropped if they meet some rule. Rules can be based on IP address, protocol, time, packet data or some combination of them all. Whitelisting is where we specify a small set of conditions that packets must meet if they are to pass, and is often a very secure solution, however runs the risk of affecting ease of use. Firewalls are often placed at intersections throughout the network, and so we can give different areas different rules.

- Intrusion detection systems (IDS) will be discussed in the next section.

- Honeypots are devices put on the network that mimic real devices, but have no valuable data or physical connections. Honeypots can be used to gather intelligence about attackers or can tie in with IDS[13]

2.2.1 Intrusion Detection

IDS works by analysing packets in a similar way to Firewalls, but instead of just dropping packets, an alert is raised to notify the system that an intrusion may be occuring. Most IDS can be broken down into two categories:

- Signature Based – Packets on the network are matched against a database of 'bad' signatures of known threats such as malware. Ineffective against novel attacks. Examples include IDIOT[14] and STAT[15].

- Anomaly Based – Compares network traffic to 'normal' traffic using statistics or machine learning in order to provide a likelihood that malicious activity is occurring. Very effective against high intensity attacks such as brute forcing a password, but much less effective against 'low and slow' attacks. IDES[16] is an example of an anomaly based IDS.

In a large network with thousands of devices and users it becomes very difficult to accurately detect attacks, so having a good model and thresholding for anomaly-based detection is very important. IDSs like SNORT give a huge number of false positives, and so operators must be trained to decide which alarms are real and are false, meaning that the amount of time before a real attack is noticed is prolonged[17].

SENAMI

Most IDS for industrial use are just modified IDS that are typically used in IT, rather than tailored to OT. Selective Non-Invasive Active Monitoring for ICS Intrusion Detection (SENAMI)[18] is an IDS built specifically for OT. The approach involves passively observing PLC data packets on the network to spot suspicious behaviour and specific attacks, as well as actively monitoring a select number of PLC variables.

The vectors used in SENAMI detection include:

- Timing - both frequency and difference to legitimate timing

- IP addresses

- Packet content

- Values in the PLCs themselves

The upload of PLC logic code is easily detected through packet content analysis, but is not enough to indicate an attack since it is a valid operation that an operator may carry out. When detected and combined with some information about timing and IP addresses, are stronger indicator is formed. Thus each vector used in SENAMI is combined together in order to detect an intrusion.

2.3 Techniques for Device Scanning

There are often thousands of PLCs and other devices connected on an OT network. This means that when operators are configuring and interacting with a network, they require some method of digitally requesting information from the devices. Asset discovery and detection is also an essential part of the reconnaissance phase of the ICS kill chain that we mentioned earlier. Many tools have been developed to perform this task. For the purpose of this report, we will focus only on tools that work with OT. We can categorise ICS scanning tools into two methodologies - active and passive which we will discuss next.

2.3.1 Passive Scanning

Bartlett et al.[19] describe passive scanning as "[finding] services on a network by observing traffic generated by servers and clients as it passes an observation point and is generally invisible to the hosts running the services." Gonzalez and Pappa[20] provide a passive technique that extracts Modbus traffic in order to gain information about the devices and transactions occurring on the network. Since passive scanning techniques do not create any traffic, we are unable to analyse the output, thus our work will focus on the analysis of active scanning techniques.

2.3.2 Active Scanning

In active scanning techniques, packets are sent to the hosts, and the responses returned are analysed. Talk about drawbacks (ie damaging). A large number of active scanning tools are available, the work of Coffey et al.[9] focuses on Nmap[21] and Nessus. We outline these along with other available tools in Table 2.1. In the next chapter we will discuss the methodology used to carry out the project.

Tool	Protocols/Services	Proprietary	Purpose
PLCScan	s7comm, Modbus		PLC device Scaner
Nmap-	s7comm, EtherNet/IP, Modbus		General port scanner with many extra plugins
Nessus	Many		Generalised vulnerability scanner
Redpoint	BACnet, CoDeSys V2, EtherNet/IP, Niagara Fox, Modbus, Omron FINS, PC Worx, ProConOS, s7comm		ICS device enumeration
Industrial Control System Exploitation Framework	Profinet DCP, Vxworks 6.x, S7comm, EtherNet/IP		ICS exploitation framework
smod	Modbus		Modbus penetration testing framework
Industrial Security Exploitation Framework	Modbus, S7comm		ICS exploitation framework, based on NSA tools
Modscan	Modbus		Modbus device scanner
SCADAShutdownTool	?		PLC exploitation framework with GUI
Sixnet-tools	Sixnet Universal		Sixnet device exlpoitation framework
s7scan	s7comm		Improvemet of PLCscan
scada-tools	Profinet		Contains scripts for enumerating Siemens devices over Profinet.
modbus-scanner	Modbus		Modbus registry scanner
Shodan	?		Search engine for IoT
masscan	-		Internet-scale port scanner
modbus-discover	Modbus		Improvement on Modscan
PLCScanner	s7comm		Enumerates Siemens S7 PLCs with GUI.
SimaticScan	s7comm		Vulnerability scanner specialised to Siemens SIMATIC PLCs. (ACADEMIC) uses plcscan
PiVOTScan	s7comm, modbus		OT vulnerability scanner (ACADEMIC)
Simatic Manager	?	X	Siemens proprietary software for managing Siemens PLCs.
FactoryTalk	?	X	Rockwell's proprietary software for managing Rockwell PLCs.
Zmap	-		Internet scale port scanner, similar to masscan

Table 2.1: Available scanning tools

Chapter 3

Methodology

Chapter 4

Results and Analysis

Chapter 5

Conclusion

Bibliography

[1] D. Kushner, "The real story of stuxnet," *IEEE Spectrum*, vol. 50, pp. 48–53, 2013.

[2] FireEye, B. Johnson, D. Caban, M. Krotofil, D. Scali, N. Brubaker, and C. Glyer, *Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure.* 2017.

[3] CISA, *Cyber-Attack Against Ukrainian Critical Infrastructure.* 2016.

[4] D. Beresford, "Exploiting siemens simatic s7 plcs," *Black Hat USA*, vol. 16, no. 2, pp. 723–733, 2011.

[5] H. K. Hui and K. McLaughlin, "Investigating current plc security issues regarding siemens s7 communications and tia portal," 2018.

[6] B. Lim, D. Chen, Y. An, Z. Kalbarczyk, and R. Iyer, "Attack induced common-mode failures on plc-based safety system in a nuclear power plant: Practical experience report," in *2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC)*, pp. 205–210, Jan 2017.

[7] D. Peterson, "Purdue model diagram," Feb 2019.

[8] T. J. Williams, "The purdue enterprise reference architecture," *Computers in industry*, vol. 24, no. 2-3, pp. 141–158, 1994.

[9] K. Coffey, R. Smith, L. A. Maglaras, and H. Janicke, "Vulnerability analysis of network scanning on scada systems," *Security and Communication Networks*, vol. 2018, pp. 3794603:1–3794603:21, 2018.

[10] B. Craggs, A. Rashid, C. Hankin, R. Antrobus, O. Serban, and N. Thapen, "A reference architecture for iiot and industrial control systems testbeds," in *2nd Conference on Living in the Internet of Things 2019*, (United Kingdom), Institution of Engineering and Technology (IET), 2019.

[11] L. M. Corporation, E. M. Hutchins, M. J. Cloppert, and R. M. Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.* 2015.

[12] SANS, M. J. Assante, and R. M. Lee, *The Industrial Control System Cyber Kill Chain.* 2015.

[13] D. I. Buffey, D. R. Piggin, and Atkins, *Active defence using an operational technology honeypot.*

[14] M. Crosbie, B. Dole, T. M. Ellis, I. Krsul, and E. H. Spafford, "Idiot - users guide," 1996.

[15] K. Ilgun, R. A. Kemmerer, and P. A. Porras, "State transition analysis: A rule-based intrusion detection approach," *IEEE Trans. Software Eng.*, vol. 21, pp. 181–199, 1995.

[16] T. F. Lunt, "A real-time intrusion detection expert system (ides)-final report," 1992.

[17] T. Pietraszek, "Using adaptive alert classification to reduce false positives in intrusion detection," in *Recent Advances in Intrusion Detection* (E. Jonsson, A. Valdes, and M. Almgren, eds.), (Berlin, Heidelberg), pp. 102–124, Springer Berlin Heidelberg, 2004.

[18] W. Jardine, S. Frey, B. Green, and A. Rashid, "Senami: Selective non-invasive active monitoring for ics intrusion detection," in *CPS-SPC '16*, 2016.

[19] G. Bartlett, J. Heidemann, and C. Papadopoulos, "Understanding passive and active service discovery," in *Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement*, IMC '07, (New York, NY, USA), p. 57–70, Association for Computing Machinery, 2007.

[20] J. Gonzalez and M. Papa, “Passive scanning in modbus networks,” in *Critical Infrastructure Protection* (E. Goetz and S. Shenoi, eds.), (Boston, MA), pp. 175–187, Springer US, 2008.

[21] G. Lyon, “Nmap: The network mapper.”