University of BRISTOL

DEPARTMENT OF COMPUTER SCIENCE

# Investigating the viability of detecting the toolset used to probe an OT netw

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.

Friday 24th January, 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, Friday 24th January, 2020

# 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 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 with the real world, and encompasses ICS. IT

Draw diagram/table to illustrate device, users, protocols, etc.

OT devices were originally controlled on each machine 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. 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 (add references). 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 compatability 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 emergence of the Industrial Internet of Things (IIoT). Figure 1.1 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.

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. As a result, we must come up with novel 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).

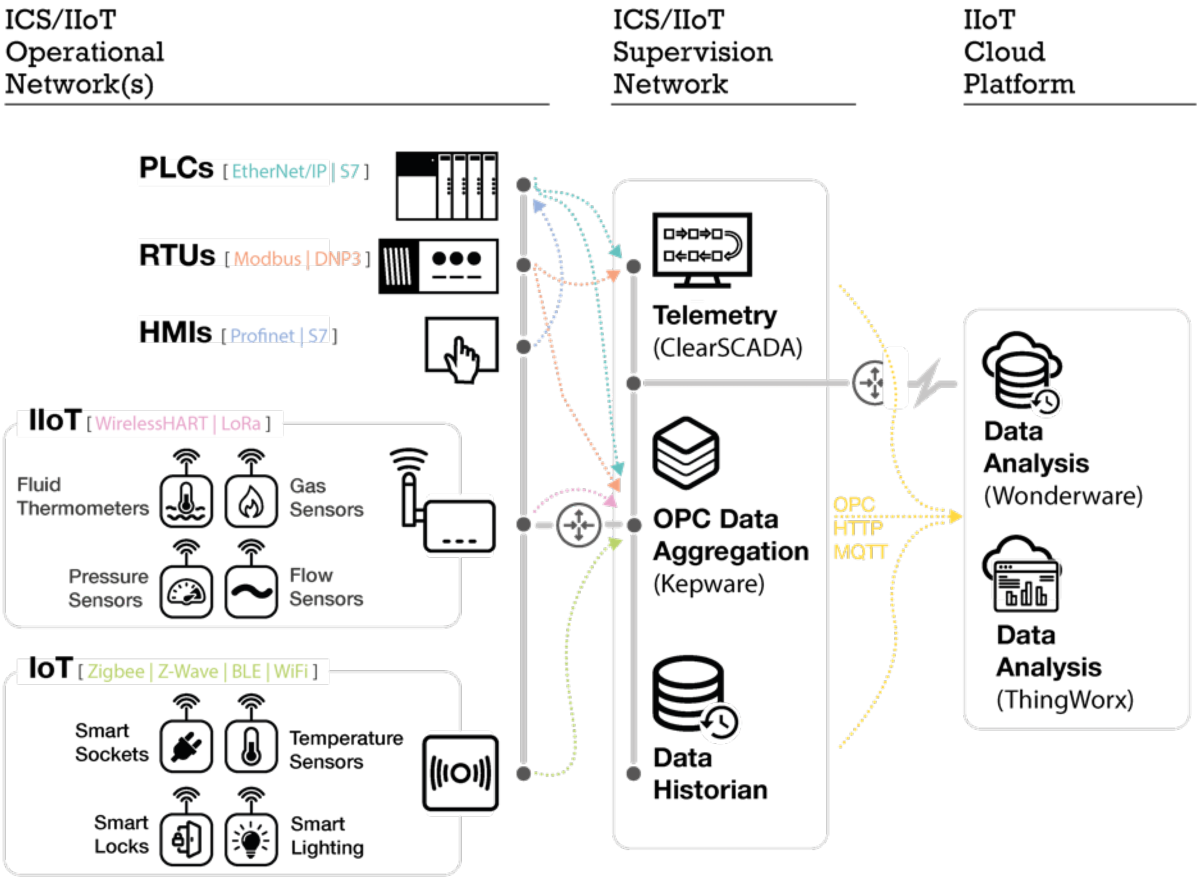
ICS/IIoT Operational Network(s)
ICS/IIoT Supervision Network
IIoT Cloud Platform
PLCs [ EtherNet/IP | S7 ]
RTUs [ Modbus | DNP3 ]
HMIs [ Profinet | S7 ]
IIoT [ WirelessHART | LoRa ]
Fluid Thermometers
Gas Sensors
Pressure Sensors
Flow Sensors
IoT [ Zigbee | Z-Wave | BLE | WiFi ]
Smart Sockets
Temperature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

Figure 1.1: : (DRAW OWN) A typical IIoT environment with a mix of legacy and non-legacy devices and protocols interacting with one another[4].

# Chapter 2

# Background

## 2.1 Operational Technology

We use the term Operational Technology (OT) to describe the devices and protocols used in systems that interact with the real world. Transport, energy and water supply are all areas of critical national infrastructure (CNI) that rely heavily on OT. These systems were originally controlled on each machine 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.

Modern OT systems are digitised. Analogue controls have been replaced with programmable logic computers (PLCs), which communicate between the physical output devices and the command and a delocalized control system, meaning that connections are much easier to manage and scale. Real world settings have hundreds if not thousands of these PLCs that can be spread across many locations.

### 2.1.1 OT Architecture

The operating systems (OS) used by PLCs are designed to carry out operations in real-time since outputs must be carried out in limited time to achieve the desired physical effect. The Typically the OS will be cut down to achieve this, with no need for utilities such as antivirus or application loaders [5]. PLCs are designed to be extremely rugged, operating for long periods of time under the variable vibration, temperature and humidity conditions found in industrial environments. Whilst PLCs are very resilient to physical conditions, if used under the wrong conditions (e.g. a flood of traffic or incorrect protocols) they may fall over or become bricked. This means that care must be taken when working with PLCs, since small errors can be very costly, even in an academic setting. The top vendors of PLCs are Mitsubishi, OMRON, Rockwell Automation, Schneider Electric, and Siemen[6].

Supervisory control and data acquisition (SCADA) is a control system architecture used for large-scale processes over multiple sites, that eliminates the need for human operators to be present at each of the remote locations where the operations take place [7]. Data is collected and transferred from each plc to the central system, where it is analysed, control and logic are implemented and it is then displayed to an operator. Either the operator or some automatic system sends controls back to the PLCs which are then turned into physical actions. There are numerous protocols used for communication between PLCs and their OT networks such as Profbus, CANbus, Modbus, EtherCAT, EtherNET/IP. (Cite these)

## 2.2 A Changing Security Landscape

The focus of the development and use of OT has typically been on availability and reliability, rather than security, which is much more of a primary concern in IT, however security is becoming more and more important now. OT devices are designed to run for a very long time, under tough conditions, meaning that there are many devices in use today that are from 20 (need to check this number, likely longer) years ago, and since patching requires devices to be offline and always runs a risk of altering use, many are unpatched. Security teams have found live devices that have been connected to the internet in real production systems where operators have tried to make their lives easier by letting them work from home. Many devices use their default passwords which easily be found online through system manuals or password databases[8]. A compound of bad design, old devices, little patching and poor security awareness mean that OT is very vulnerable.

The first large scale attack against OT that made itself into mainstream news was Stuxnet. Several zero-days were used in a complex attack targeting the SCADA network of Iran's nuclear program. The worm infected Siemens S7 PLCs which were connected to centrifuges used to separate nuclear material, and caused them to spin at a much faster rate, whilst reporting that they were operating at a normal speed. Since the operators had no way of knowing that they were spinning too fast, the tasks were carried out incorrectly, wasting material and wearing the motors down quickly. Stuxnet reportedly destroyed approximately 2000 centrifuges, roughly one fifth of their total[9]. After seeing the effects of this attack on OT, executives began to consider cyber security as much more of a priority.

Since an attack on IT tends to be far more lucrative in comparison to OT, threat actors incentivised by money such as criminal groups are not typically interested in attacking these areas. Instead, attacks more commonly come from script kiddies who have found a PLC connected to the internet on Shodan and want to have some fun, or from an APT such as state actor wishing to damage a countries CNI. APTs have a large arsenal of resources available to them, including the ability to develop new zero-day exploits for OT. Damage to CNI could cause economic impact, harm to humans and even large-scale loss of life.

Kapersky and ARC Advisory group carried out a study of 282 industrial companies and organizations across the globe in 2019, in which they found that 59% of companies surveyed had experienced a cyber incident in the last 12 months, and 70% consider an attack likely[10]. It is also worth noting that some of the remaining 41% will have had cyber incidents that have so far gone unnoticed [11]. The findings of this report make it clear that more needs to be done in order to keep OT secure.

## 2.3 Attack Paths

Most cyber attacks on IT follow a similar attack path/kill chain[12], composed of different sections which can be broken down into smaller individual tasks: Reconnaissance, weaponization, delivery, exploitation, installation, command control, action on objective. Attacks targeting OT differ in that the final stage – 'action on objective' of the traditional kill chain leads to further stages[13]. The action on objective is to gather information about the victims network and the OT connected to it, and then a second set of stages is started. 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.

## 2.4 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 following a set of rules that blacklist the data flow – in which all packets are allowed apart from those which match some set (or the other way for whitelisting). Rules can be based on IP address, protocol, time, packet data or some combination of them all. Whitelisting 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 follow a set of rules, but instead of just blocking packets, the operators are alerted that an intrusion may be occurring.

- 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[14]

### 2.4.1 Intrusion Detection

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[15] and STAT[16]. 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[17] is an exmaple 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 notices is prolonged.(need to back this up).

## 2.5 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.

## 2.6 Device Scanning

As mentioned earlier, 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. Several scanning tools have been developed that perform this task. Some of these are designed to work across IT and OT (nmap[19]), some across all

OT (RedPoint [https://github.com/digitalbond/Redpoint]), some are vendor specific (PLCScan, but find better) and some have vulnerability scanning built in (SimaticScan).

The tool works by .

Some operators may only ever use one tool, by instruction or out of necessity. If we think of an OT network where all of the devices are provided by a singular vendor e.g. Siemens, then it makes logical sense that the only tool used is scanning tool.

When attackers are conducting reconnaissance or carrying an attack on a network of OT devices, they will need to scan the devices on the network. This may be carried out by a real person but there is a high likelihood that this will be automated – e.g. a worm trying to self replicate onto a specific type of PLC. They may use a scanning tool which is never used by the actual operators. If it is possible to identify which scanning tool is being used, then this could be used as an additional vector in IDS.

# 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] 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.

[5] PanelShop, "Inside machines: Pc vs. plc - comparing control options," Jan 2019.

[6] technavio, *Micro Programmable Logic Controller (PLC) Market by Product, End-users, and Geography - Forecast and Analysis 2020-2024.*

[7] A. Bagri, R. Netto, and D. Jhaveri, "Article: Supervisory control and data acquisition," *International Journal of Computer Applications*, vol. 102, pp. 1–5, September 2014. Full text available.

[8] CRITIFENCE, "Scada default passwords."

[9] J. Rosenberg, "Chapter 6 - security in embedded systems**please visit the companion website http://booksite.elsevier.com/9780128024591 for part two of this chapter which covers the following topics in detail: Important security concepts, security and network architecture, software vulnerability and cyber attacks, security and operating system architecture.," in *Rugged Embedded Systems* (A. Vega, P. Bose, and A. Buyuktosunoglu, eds.), pp. 149 – 205, Boston: Morgan Kaufmann, 2017.

[10] Kapersky, *The State of Industrial CyberSecurity.* 2019 ed.

[11] IBM, *Cost of a Data Breach*, vol. 2019.

[12] 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.

[13] SANS, M. J. Assante, and R. M. Lee, *The Industrial Control System Cyber Kill Chain.* 2020.

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

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

[16] 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.

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

[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. Lyon, "Nmap: The network mapper."