# Proposed Title

The viability of toolset identification as a vector for operational technology intrusion detection.

# Supervisor

Dr Barney Craggs

# Project Area

Cyber Security

# Problem Statement

There are many tools available to inspect and analyse Operational Technology (OT) assets. Some of these tools such as ModScan (Bristow, 2008) and PLCScan (SCADAStrangeLove, 2012) are used to simply identify the device, whereas others go further and even find vulnerabilities - SimaticScan (Antrobus, et al., 2016). Attackers use these tools during reconnaissance before they begin attacking. Detection of a malicious scan can be used to stop an attack in its early stages. There are several vectors which may indicate that a scan is malicious, including time, intensity and source address. Alone, each of these parts in isolation would not provide sufficient and sound intrusion detection.

Proposed Research

To investigate the viability of augmenting the existing known indicative vectors used in IDS with intelligence as to the toolset being used to probe an OT network. Thus providing another method by which mitigation can be achieved.

# Background

Operational Technology is used to monitor and control changes in industrial equipment, for example water pumps in a sewage plant or the motor in a uranium centrifuge. OT devices are found primarily in Critical National Infrastructure, on which our daily life depends.

OT devices are being connected to the internet more and more in order to improve communication, analyse date for business intelligence, and allow operators to work remotely. One only needs to perform a few searches on Shodan to see just how many OT devices like PLCs are connected to the internet.

Global research from Ponemon shows that nearly 70 percent of critical infrastructure managers reported at least one security breach that led to the loss of confidential information or disruption of operations in the past 12 months. In addition, 78 percent said a successful attack on their organization’s ICS or SCADA systems is at least ‘somewhat likely’ within the next 24 months. Yet only one in six respondents described their organization’s IT security program or activities as ‘mature.’”  
NTT Security, 2018. Securing Operational Technology: How vulnerable is our national critical infrastructure? <https://www.nttsecurity.com/docs/librariesprovider3/resources/gbl_thought_leadership_operational_technology_uea.pdf?sfvrsn=4dd3b469_6>

### What makes OT so vulnerable?

Login credentials are often left as default, which can be looked up online if one knows the product number. Devices are meant to be deployed for a long time under tough conditions, and were not intended to be connected to the internet, so the focus for design of these devices has traditionally been on availability and robustness rather than security. Since these devices last a long time there is a lot of legacy equipment from 15+ years ago. Many operators are not trained or do not view security as a high priority, so won’t change the login credentials or update the devices to patch vulnerabilities out of a reluctance to take the devices offline. It is also worth noting that it is often very easy to make OT devices fall over simply by flooding the network, for example with a high intensity scan.

### Current Intrusion Detection Systems (IDS)

Most IDS can be broken down into two categories:

Signature Based – Matches packets on the network against a database of ‘bad’ signatures of known threats. Ineffective against novel attacks. Wouldn’t pick out scanning of OT devices as an intrusion because this is normal behaviour.

Anomaly Based – Compares network traffic to ‘normal’ traffic in order to provide a likelihood that malicious activity is occurring. Effective against high intensity attacks, but a ‘low and slow’ attack would not be detected.

Both types are primarily used for detecting intrusions and exploitations, but do not provide good detection against the reconnaissance part of the kill chain.

An example of an IDS used in OT is SENAMI (Jardine, et al., 2016).

Another challenge in the world of OT is that operators and managers are often reluctant to make changes to their networks, as any kind of accidental fault or failure could potentially have huge financial repercussions – e.g. an oil rig going offline for a day due to a network fault, would cost tens if not hundreds of thousands.

# Proposed Workplan

The aim of this project is to analyse the packets received by an ICS device during a scan, and identify which tool is being used. This would aid in the detection of malicious scans, and potentially prevent future attacks.

### Steps Needed:

1. Identify which tools are used to scan OT devices by real operators and by attackers
2. Understand how these tools work
   * Read the source code
   * Analyse packet captures
   * Understand any relevant technologies (e.g. Modbus)
3. Obtain a real PLC, and carry scans with different tools
   * Analyse the results and come up with a prototype classifier
4. Carry out the scans on a different PLC, and see if the results are the same
5. Build classifier, test different tools on different PLCs
   * Build a table of results to improve the classifier
6. Iteratively improve the classifier
7. Work out what could be done to confuse/obfuscate the detection
8. If our investigation finds that it is impossible to differentiate between tools, then we will have shown that toolset analysis is not a viable technique for intrusion detection

# Potential Outcomes

This project will provide a technique to differentiate between the tools used to scan OT devices, which could be used to strengthen intrusion detection in OT networks. This would have a positive impact, reducing the risk of a successful attack, saving money and possibly even lives.

# Glossary of Terms

OT – Operational Technology

PLC – Programmable Logic Controller

IDS – Intrusion Detection System

# Bibliography

Antrobus, R., Frey, S., Green, B. & Rashid, A., 2016. *SimaticScan: Towards A Specialised Vulnerability Scanner for Industrial Control Systems.* Belfast, BCS.

Bristow, M., 2008. *ModScan - A SCADA MODBUS Network Scanner.* [Online]   
Available at: https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-bristow.pdf  
[Accessed 25 Oct 2019].

Jardine, W., Frey, S., Green, B. & Rashid, A., 2016. *SENAMI: Selective Non-Invasive Active Monitoring for ICS Intrusion Detection.* New York, ACM.

SCADAStrangeLove, 2012. *PLCScan the Internet.* [Online]   
Available at: http://www.scada.sl/2012/11/plcscan.html  
[Accessed 25 October 2019].