DOI: http://dx.doi.org/10.14236/ewic/ICS2015.8

Automated Asset Discovery in Industrial Control Systems - Exploring the Problem

Adam Wedgbury and Kevin Jones
Airbus Group Innovations
Quadrant House
Celtic Springs
Newport, NP10 8FZ
UK
adam.wedgbury, kevin.jones@airbus.com

Vulnerabilities within Industrial Control Systems (ICS) and Critical National Infrastructure (CNI) represent a significant safety, ecological and economical risk to owners, operators and nation states. Numerous examples from recent years are available to demonstrate that these vulnerabilities are being exploited by threat actors. One of the first steps required when securing legacy infrastructures is to obtain a complete asset (device) inventory, as is it impossible to protect a system without first understanding its content and connectivity. ICS environments offer significant challenges to the automated and safe discovery of network connected devices. Legacy ICS-based network services are often very fragile and networks are often sensitive to increased traffic, latency or interference, precluding the use of active scanning technologies. The decentralised nature of ICS traffic flows alongside the lack of capability of legacy network equipment make the use of standard passive scanning technologies difficult. This paper presents an overview and understanding of passive ICS discovery and provides the results of an experiment to show how existing passive scanning tools fare in an ICS environment in which port mirroring technologies are not ubiquitously supported.

Keywords: SCADA, ICS, automated device discovery, passive, active, safety

1. INTRODUCTION

Supervisory Control and Data Acquisition (SCADA) systems are specialised computer networks containing devices and applications to monitor and control physical processes. These processes often consist of distributed networks with interconnected sensors and actuators. The SCADA element provides central command and control oversight to a collection these localised processes.

Historically, SCADA systems were isolated networks with no external connection. As the world became increasingly interconnected, benefits were seen in integrating control systems, providing standardisation of connections, utilising global communications infrastructures, and integrating with business IT systems in order to facilitate activities such as remote access and monitoring. Therefore, such systems are entirely reliant on interconnected network infrastructures, including the Internet, and become vulnerable to inherent security concerns Nicholson et al. (2012).

In 2013, the number of Industrial Control System (ICS) security incidents reported to US ICS-CERT rose to a total of 257. This is a rise from 197 in 2012 and 140 in 2011. In-step with this trend, the number of vulnerabilities found and reported to ICS-CERT rose to 187 in 2013, up from 137 in 2012 ICS-CERT (2014).

There are many challenges facing the process of securing ICS environments, including; the accountability of actions when changes are made. It is often difficult to determine who, or what, was responsible for a change. An auditing and thus, authentication and authorisation, facility is required to alleviate this issue, however this is a feature commonly lacking from the embedded devices used within ICS environments. In addition, preventative defence is of the utmost importance due to the safety critical real-time nature of these devices and their interaction with the physical world.

The degradation of air gaps between Industrial Control networks and other infrastructures such as

the Internet either directly or indirectly has become a priority in the security considerations of the environments Byres (2012). Search engines such as SHODAN[1], in which the headers of Internet facing servers are indexed and made searchable, has highlighted the scale of the Internet exposure of components of many SCADA systems.

In order to properly secure an existing ICS installation, a thorough understanding of the system is paramount Dumont (2014). Without this understanding the risk cannot be quantified, defence cannot be complete, the perimeter cannot be established Valladares (2012), and patching is not feasible Pauna and Moulinos (2013). Gathering a complete inventory of the system is the first step to developing an understanding of it. There are a number of questions that must be answered in order to develop this understanding; one of which is: What devices and components is the system made up of? The answer to this question should include as a minimum; device vendor and model, hardware, software and firmware versions, and configuration.

In a traditional IT environment, a large proportion of this inventory intelligence can be gained using network-based scanning techniques, most commonly requiring active polling of devices. Such active polling scans the IP address space, and thus the devices listening on those addresses, for as much information as possible Oliva and Crowe (2003). Many ICS components found in legacy systems were not designed to be a part of a large, crowded and distributed network, therefore their network services were not robustly designed. As a result many legacy ICS components, and indeed some modern components, can be forcibly taken off-line upon receipt of even the simplest unsupported packet of data. The fragility found in these ICS components and the requirements for safety principles in network connectivity and latency mean that active scanning techniques cannot currently be safely used in an assured manner. Therefore an alternative passive approach must be used to gain the required system knowledge.

These issues are further compounded by the presence of non-IP-based components, such as RS232 serial and RF-based links, that are unsupported by existing tools and techniques.

This report aims to fully explore the problem space, identifying what tools are currently available and where they lack the required capability. A test scenario will be presented, highlighting the specific problems with representative equipment. Finally, areas of future research will be laid out, providing a roadmap for overcoming the problem.

[1] http://www.shodanhq.com

2. RELATED WORK

Former work of Liu and Neufeld (2009) discusses configuration within the control network of the Large Hadron Collider (LHC), maintained and operated in Switzerland by CERN in which the Link Layer Discovery Protocol (LLDP) is used to maintain awareness of the network topology and connected devices. LLDP is a vendor neutral Layer-2 protocol that is used for the advertisement of identity, capability and neighbours of network devices. In this context, the term 'network devices' refers to components directly supporting network infrastructure such as switches, routers and access points. An LLDP cascade approach is used at the LHC to incrementally discover each active network device. Simple Network Management Protocol (SNMP) is then used to query the discovered LLDP network devices to obtain a list of hosts stored in its MAC address table. Address Resolution Protocol (ARP) can then be used to translate the recovered MAC address into IP addresses. This process works at the LHC because all network devices are known to support LLDP and they know the level of generated traffic will not impact operations.

Wiberg (2006) goes some way to developing an ICS specific network reconnaissance tool set and discusses a range of techniques for the identification of network connected hosts including; MAC Address Identification, TCP/UDP port number identification, service interrogation and equipment profiling. Only passing reference is made to the safety issues introduced by using active scanning techniques in this work, with testing in a non-production environment being offered as the main mitigation.

3. THE NEED FOR ASSET DISCOVERY AND MANAGEMENT

Proper asset management processes allows an owner/operator to maintain good visibility of their computing infrastructure to support business, financial, safety, and security requirements. According to Mohan (2013), good asset management allows for an in-depth understanding of:

- What systems and equipment exist
- Where components reside
- How they are used
- What they cost
- When were they added to the inventory

- Whether they have an expiry date
- How they impact IT and business services

The benefits of asset management are equally applicable to both traditional IT and ICS environments, although the challenges of establishing and maintaining the management process differs significantly between the two. Whilst good asset management processes offer benefits to many parts of a business, such as planning refresh cycles or account auditing, the focus of this paper is for asset management as a cyber security tool either pro-actively or reactively to support a SCADA forensics investigation Wu T. et al. (2013); van der Knijff (2014); Stirland (2014).

Good asset management, and in particular a comprehensive asset inventory, is vital to appropriate defence of a network and infrastructure. It must be known what devices are on the network, to whom they communicate and how, characteristics of the devices and the presence of any known vulnerabilities. Only once this information is known can the perimeter be established and secured, and proper anomaly detection put in place.

4. FACETS OF NETWORK DISCOVERY

The topic of network discovery can be segregated into a number of discrete topics, largely due to the range of capabilities offered by many software tools Zhu et al. (2002). The two broadest areas are:

- Device Discovery - Is there a device present?
- Device Classification - What is the device?

Device classification is the act of confidently identifying a device, usually including such parameters as; vendor, model, version, location, network address, patch level and vulnerability status. Whilst device classification is a challenge, it is generally a matter extensive device and protocol support being used as an input to existing technology.

Device discovery is the process of confirming the mere existence of a device. In many cases the information used to confirm the existence of a device is also fed into a detailed classification process. The initial network and device discovery exercise is often the phase that can prove most difficult, especially in challenging environments such as ICS in which there are bespoke technologies, legacy devices, and safety considerations. Currently there is no tangible solution to this problem in such an ICS and it is an under researched field, but one that is the vital first step in understanding and securing these critical environments.

Often, device discovery products are bundled along with vulnerability scanning engines in order to provide additional information and risk profiles. As with the detection products themselves, these engines also either work passively, listing to network traffic, or actively, where they poll the devices to find vulnerabilities. However, as the primary problem is asset discovery as a precursor to vulnerability scanning and the field of vulnerability scanning for ICS brings additional considerations it is out of scope for this paper. That said, vulnerability scanning vendors and operators have previously approached the subject of ICS/SCADA scanning Permann and Rohde (2005); Peterson (2006).

5. THE PROBLEM WITH TRADITIONAL METHODS

The requirement of building an asset inventory used to inform the defence strategy is equally applicable to traditional enterprise IT environments as it is those containing ICS equipment. The nature of a traditional IT environment makes this an easier task for a number of reasons. Firstly, all IT hardware is generally refreshed every 3 to 5 years (Archstone Consulting White Paper 2015) meaning that a typical installation will have been commissioned using modern security and business practices and so likely to have at least a minimal asset management system in place. Secondly IT equipment is often subject to regular interactive use, be it a user's workstation or configuration management of service equipment, meaning that a human is likely to be at least aware of the existence of the equipment. Further, IT equipment is designed to operate in a relatively hostile network environment, leaving them with very robust network services and finally the scanning tools are designed specifically to operate within such environments. This means that active detection and polling techniques are considered safe to use in such environments.

In contrast, the presence of legacy components in ICS environments is commonplace due to the general lack of regular equipment refresh cycles. Once an installation has been commissioned, it is often left untouched unless a failure occurs or a modification is necessary. This means that many currently in-service systems were commissioned before the advent of modern security and system maintenance best practices. This, coupled with often ad-hoc modifications and extensions, leaves these systems without thorough asset registers.

5.1. Component Fragility

ICS components, particularly legacy components were designed to operate in a controlled and

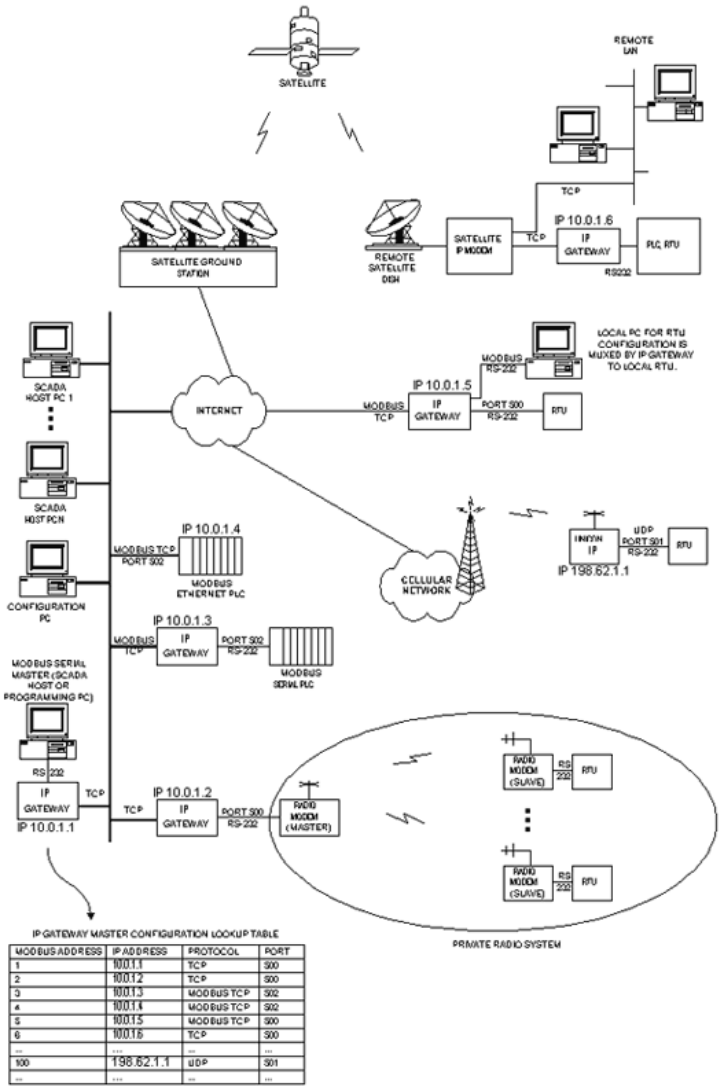

Figure 1: *An example of various types of data links present in an ICS network*

isolated network environment where traffic and interactions could be predicted. This has led to services being designed and implemented with regard to functionality and safety, with little attention being paid to operational characteristics outside of design parameters. Therefore, many components commonly found in ICS environments today have very poor network robustness, leaving them unable to process requests that they are not specifically designed for. Whilst performing traditional network discovery techniques on a network containing such fragile components, such as PLCs and RTUs, it is quite likely that the affected devices will become unstable or crash, effectively resulting in a denial of service effect and pose a direct risk to safety, both of human and environmental.

5.2. Network Constraints

ICS networks operate with constraints different to those of traditional IT environments. In many scenarios an ICS network must guarantee a highly deterministic, low latency service in support of a real-time process Galloway and Hancke (2013); Nicholson et al. (2014). Such constraints mean that traffic must be carefully controlled in order to ensure that the network is not congested with superfluous data, delaying or affecting mission-critical data. Further, data links within an ICS environment may be very low-bandwidth such as dial-up, radio or RS232/485 serial. Such low-bandwidth data links require data traversing the network to be very carefully controlled as to not cause congestion and adversely affect the process. Figure 1 as adapted

from Bentek Systems[2] depicts a how different types of data link can be dispersed within an ICS network.

6. ACTIVE SCANNING

For the reasons discussed in this section, active scanning techniques cannot be universally and safely used within an ICS network. Instability within the ICS component may cause undefined effects upon receipt of unsupported network data, and violation of network constraints by the introduction of extra traffic could have a detrimental effect on the process. The effect of these risks being realised could either be financial, in the case of the process simply being interrupted, or in more extreme cases safety controls could be compromised leading to risk of injury or damage to the environment.

Peterson and Hilt of Digital Bond outline a case where a PLC was observed to irrecoverably crash following a simple port scan Peterson (2012). The PLC in question would attempt to load new firmware upon detecting any activity on a certain port, regardless of the lack of parameters or authentication. With no new firmware present the device fell into an irrecoverable state until it was completely reset and reloaded with new firmware.

Various attempts have been made to develop an ICS safe active discovery tool, however they should always be used with great caution. As an example, 'plcscan'[3] is an open source project to actively discover ICS devices safely using native ICS protocols (supporting Siemens s7comm and Modbus) for discovery, with the knowledge that the fragile devices should be able to safely handle a native protocol. However, not all ICS devices support all ICS protocols and risk still remains when sending unsupported network traffic to a device.

6.1. Shodan

Shodan is an Internet search engine that indexes devices and services connected to the Internet, as opposed to a traditional search engine indexing only websites, and has been used to identify internet facing ICS components Williams (2014). To accomplish this Shodan first randomly selects a public IP address from the IPv4 range along with a randomly selected port from its limited range of supported services. Shodan will then attempt a TCP connection to the socket with a TCP-ACK packet. If no response is received, a new socket will be randomly selected and the process will start again. If a SYN-ACK response is received however, the connection will be completed and a banner grab initiated, with the results being stored in a database. The database is then searchable on the Shodan website Bodenheim (2014).

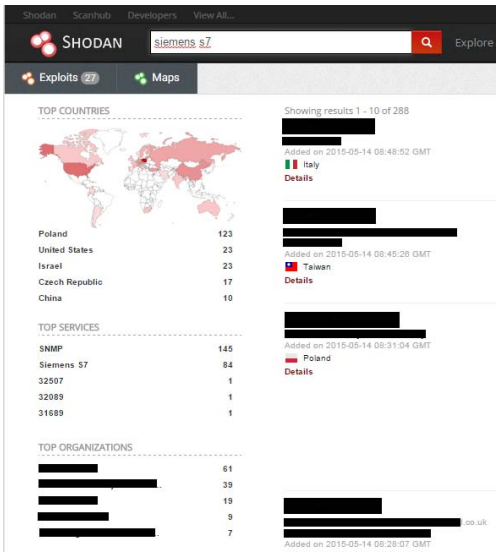

Figure 2: *Sample of results returned from the Shodan search engine.*

At the time of writing, a Shodan search query of '*siemens s7*' returned 288 results from across the globe (see Figure 2). To date, there has been no publicly reported incidents of Shodan scans interfering with the normal operation of ICS equipment. The reason for this is unclear - it is possible that Shodan scans its targets in a safe manner, or that it hasn't yet found any such unstable devices exposed to the Internet. It may also be possible that any incidents simply haven't been reported and as outlined by Peterson (2012) there remains a danger with the approach.

6.2. ARP Scanning

If actively scanning a network segment was deemed necessary, Address Resolution Protocol (ARP) scanning would likely be the safest approach. ARP is the protocol that resolves IP addresses to local, physical MAC addresses within a subnet. Because of its function, ARP is ubiquitous to almost all Ethernet and IP-based devices. Performing an ARP scan does not use the protocol in any other way that its specification dictates, giving it a minimal risk of adversely affecting any device. ARP is limited in scope to the local subnet however, resulting in hosts on separate subnets being undetectable.

Even if using ARP requests to actively scan a network range is deemed to not pose a risk to the stability of network devices in a particular installation, great care must still be taken to not flood the network

[2]http://www.scadalink.com/products/legacy-products/ip-gateway-modbus-multiplexer-mux-multiport-modbus-serial-tcp-gateway-terminal-server/
[3]https://code.google.com/p/plcscan/

with scan-related traffic, causing a denial of service effect.

7. PASSIVE SCANNING

As an alternative, passive scanning does not actively poll network connected devices. Instead passive scanners transparently intercept and listen to traffic already traversing the network. Merely the receipt of traffic to or from a host will be adequate to inform the scanner of the presence of a device. Introspection analysis of the traffic may additionally allow the scanner to determine more information about the device, such as type, version and location.

Existing tools are available to passively discover network attached devices, such as Sophia[4] and Tenables Passive Vulnerability Scanner[5]. However, the inherent disadvantage of passive scanners is that they can only be aware of the presence of a device on the network if traffic destined to, or originating from, the device reaches the scanner's listening interface. This means that any device who's network communications do not traverse the passive discovery sensor will remain undetected.

In a modern traditional IT environment this limitation often isn't a problem due to good documentation and the widespread use of managed network equipment with centralised pinch-points allowing the replication or introspection of network traffic. Thus such network traffic can easily be fed into the passive listener, giving the scanner visibility of all, or at least a significant portion of the network. A legacy ICS environment however, is unlikely to have such a well managed environment and will not necessarily have a centralised network interface for large data collection. It is common to see many switches, direct connections, or alternative communications (e.g. radio links, modems, etc.) Choi (2013) which would significantly reduce the effectiveness of a deployed passive scanner.

7.1. Hybrid Approach

There is an approach that combines both active and passive methods, using active techniques as an enabler for passive techniques. An example of this would be to use ARP Spoofing techniques Trabelsi and El-Hajj (2010) to force all traffic on a network through a central host, allowing it to be detected and classified by a passive sensor. This retains the same flaws inherent to active scanning as described in Section 6, further compounded by the aggressiveness of techniques such as ARP Spoofing.

[4]http://nexdefense.com/about-sophia/how-does-it-work/
[5]http://www.tenable.com/products/passive-vulnerability-scanner

8. PASSIVE ASSET DISCOVERY TOOL KITS

In the implementation of passive discovery it is useful to understand the existing tools and capabilities that are able to support the operation. Examples include:

- **Tenable Network Security Passive Vulnerability Scanner**[6]: isn't purely an asset detection tool kit, it passively monitors the network to identify vulnerable systems, inappropriate activity and misuse, and detecting the flow of sensitive data
- **Passive Asset Detection System (PADS)**[7]: is a lightweight, open-source, signature-based passive detection engine. It is designed to sit alongside an Intrusion Detection System (IDS) and provide context to the IDS alerts.
- **Alien Vault Unified Security Management (USM)**[8]: is a comprehensive suite of tools designed to help security visibility within a large network and provides vulnerability discovery, intrusion detection and behavioural monitoring alongside its asset discovery capability. USM also has active scanning capabilities for use in a permissive environment and contains plugins to enable classification and enumeration of ICS related devices.
- **Netdiscover**[9]: a lightweight, open source detection tool which listens for ARP broadcasts in order to discover a device. Harvesting of the MAC address contained within the captured ARP messages allows for rudimentary classification of the device although such reliance on ARP means confinement to device discovery within the local subnet.

Before undertaking experimentation to find and highlight the issues encountered with passive asset discovery in industrial control environments, a 'deep dive' was undertaken on a product to ensure a full understanding of its use cases and capabilities. The software package chosen, largely down to its market presence, was Tenable Network Security's Passive Vulnerability Scanner.

The Passive Vulnerability Scanner is a service designed to continuously monitor the flow of traffic entering and leaving the monitored network interfaces. According to vendor documentation, "PVS continuously discovers and tracks users, applications, cloud infrastructure, trust relationships, and vulnerabilities. It also automatically discovers users, infrastructure and vulnerabilities across

[6]http://www.tenable.com/products/passive-vulnerability-scanner
[7]http://passive.sourceforge.net/about.php
[8]https://www.alienvault.com/products
[9]http://nixgeneration.com/jaime/netdiscover/

operating systems, network devices, hypervisors, databases, tablets, phones, web servers, cloud applications, and critical infrastructure" Tenable Network Security (2013) and claims to be capable of:

- detecting when systems are compromised based on application intrusion detection
- highlighting all interactive and encrypted network sessions
- detecting when new hosts are added to a network
- tracking exactly which systems communicate with other systems and on what ports
- detecting what ports are served and what ports are browsed by each system
- detecting how many hops away each monitored host is

Originally designed for enterprise IT environments, PVS has a number of plugins available for an ICS environment and allow the passive detection engine to be extended with new detection rules. To support this Digital Bond's project Basecamp has developed a set of ICS specific PVS plugins to help enumerate or identify the ICS equipment before checking for default credentials and other common vulnerable configuration settings[10]. Contained within the current plug-in repository are over 170 plugins belonging to the 'SCADA' family including:

- MODBUS/TCP Client Detection
- Schweitzer Engineering Laboratories Default telnet Account Detection
- Modicon telnet Default Account/Password Detection
- Rockwell Automation Service Detection
- Siemens Device Detection
- RuggedCom Rugged Operating System < 3.12.2 Multiple Security Vulnerabilities

As with any passive discovery solution, due to its inability to actively probe the network PVS relies on communications traversing its network interfaces in order to perform device and vulnerability discovery. This approach can be quite successful in a traditional IT environment as hosts are likely to be communicating across common 'choke points', such as network boundaries and Internet gateways. Within an ICS environment, hosts are much more likely to be communicating internally with each other, such as a Programmable Logic Controller (PLC) transmitting process information to a Human Machine Interface (HMI) as shown in Figure 3.

[10]http://www.digitalbond.com/tools/basecamp/

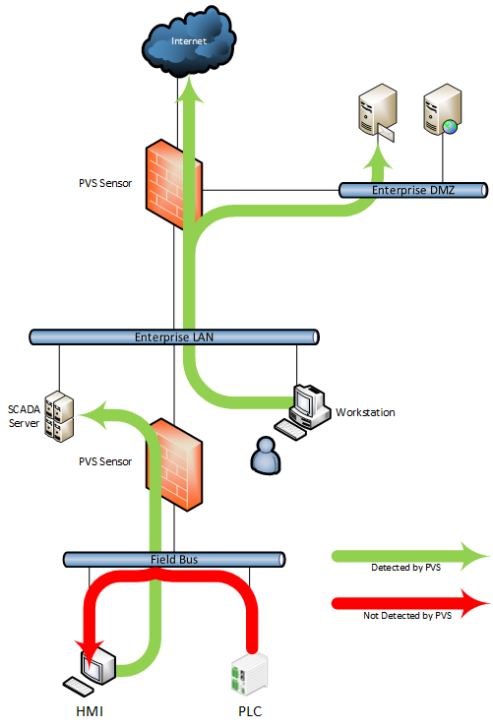

Figure 3: *Example of undetectable devices via passive techniques*

In this ICS communications example based on normal deployment, traffic originating from, or destined to a device may never necessarily traverse a typical choke point. There are likely many instances of such a situation within a typical ICS environment where the system has grown in a piecemeal fashion over a number of years. This makes it impractical to place enough passive sensors to ensure complete coverage of all communications, even where sufficient documentation exists to show where such scenarios exist and makes it very difficult to achieve full network coverage using only passive discovery techniques.

8.1. Broadcast Domains

PVS documentation claims that it listens to network broadcasts as one vector for device discovery. This is a logical feature as many devices broadcast information over the network. A broadcast is a packet of data addressed to a special IP address within the assigned network range. A broadcast is addressed to all hosts within the local subnet, and so network equipment such as switches to ensure the broadcast packet is transmitted to all devices. Routers and other broadcast suppressing devices however, block broadcast packets from propagating further through

the network. This means that if the PVS sensors reside on a different subnet from a device, or is behind a broadcast suppressing device, it will not receive the broadcast packets; thus the device remains undiscovered. It is also possible for a device not to broadcast at all rendering it undiscoverable using this technique.

ARP is an example of a ubiquitously used protocol that makes use of IP broadcasts. Whilst ARP is a dynamic protocol that constantly refreshes its state by issuing broadcast packets, ICS networks tend to be examples of very static environments therefore, it is possible in many places that ICS devices will be configured with static ARP tables to help ensure both high reliability and low network utilisation. Scott (2012) highlights that static ARP table entries are often deployed as a security mechanism to help safeguard against ARP-facilitated man in the middle attacks.

8.2. Port Mirroring

Port Mirroring is a technique generally used on Ethernet switches that duplicates all traffic traversing the device and outputs it to a dedicated interface or Virtual LAN (VLAN). Port Mirroring is a common solution to enable the use of intrusion detection and prevention systems. By duplicating all network traffic onto a dedicated port the need for a security device to sit 'in-line' with the traffic flow is eliminated, therefore reducing single points of failure. The ability to port mirror onto a dedicated VLAN enables the use of a centralised sensor, instead of requiring a sensor at each network switch.

Within a traditional IT environment it is likely to see the prevalence of managed switches, routers and firewalls allowing for the widespread use of port mirroring technology and achieving comprehensive network coverage. Port Mirroring is not as effective at achieving full network coverage in an ICS environment however as unlike in an enterprise environment, an ICS network will typically contain many small groups of devices connected together with simple (unmanaged) switches unlikely to support both Port Mirroring and VLANs and unable to supply a central passive sensor with traffic information.

9. EXPERIMENTAL TEST SETUP

In order to evaluate the effectiveness of a passive network scanner to detect network equipment, a test environment was created to simulate a range of scenarios that are likely to be found in a typical ICS environment. The architecture of the test system is shown in Figure 4 including PLC, HMI, and routing.

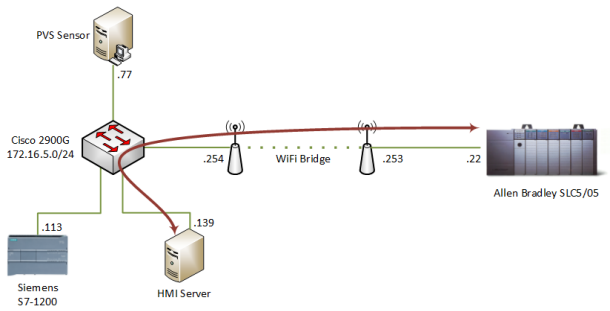

Figure 4: *Physical representation of test system*

To simplify the configuration and offer a best-case scenario for PVS, all devices are situated within a common broadcast domain. No broadcast suppressing devices were in use, although it is worth noting that the remote side of the WiFi bridge translates MAC addresses into a pool of virtual MAC addresses. The HMI server continually communicates with the Allen Bradley SLC5/05 in order to maintain constant status information. The switch is not configured with any port mirroring capabilities and no static entries in ARP tables have been made.

A process continually executes on both the Allen Bradley and the Siemens PLCs and the system was left with both PLCs in 'Run Mode' for a period of 24 hours in order to allow any protocol time-outs, such as ARP tables entries, opportunity to expire and refresh.

10. RESULTS

The results of the PVS device discovery session over the 24 hour period are shown in Figure 5 in that PVS has discovered many other devices present within the test environment that are not relevant to this experiment. Not present in the results however are the Siemens and Allen Bradley PLCs at IP addresses 172.16.5.113 and 172.16.5.22, respectively. This is despite the Allen Bradley PLC being in constant contact with the HMI server at 172.16.5.139, which has been detected. Evidently, the HMI server is generating broadcast packets that are being received by PVS whereas the PLCs are not. Also worth noting is that the remote side of the WiFi bridge, 172.16.5.253, has been discovered, proving connectivity between it and the passive sensor.

As a control test in order to prove both connectivity to the PLCs and PVS' ability to detect them, ICMP Ping packets were sent to both PLCs from the PVS host. The successful Ping requests prove that the PLCs were active and reachable on the network

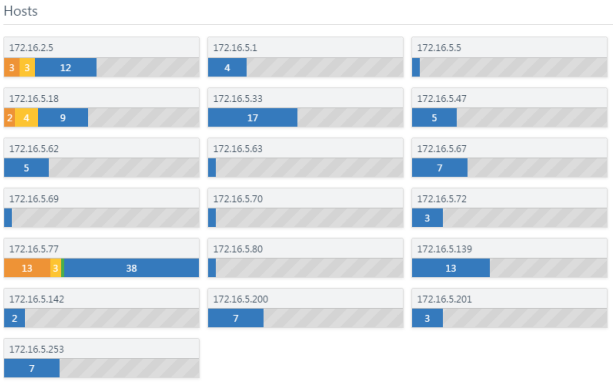

Figure 5: *Results of passive device discovery on test system*

Figure 6: *Results of passive discovery after 'Pinging' the PLCs*

at the time of testing. Predictably, after listening to the Ping requests and responses traversing its network interfaces, PVS discovered the presence of the PLCs. This can be seen in Figure 6, although note that no further information about the PLCs is available, other than their presence.

The results obtained during this experiment prove the inadequacies of relying solely on existing passive scanning techniques to achieve a full inventory of network connected devices. The classification capabilities of PVS were not exercised during this experiment, therefore one can be reasonably sure that these results will be repeated across any product using the same passive scanning technology as this result highlights its inherent weakness.

11. CONCLUSION

Passive network scanners have the potential to be incredibly useful for auditing the presence of devices and vulnerabilities on a network and to monitor misuse and unauthorised access. The inherent requirement of passive scanners however, is to maintain visibility of all traffic traversing the monitored network in order to provide complete coverage. The characteristics of a traditional enterprise network can cater for this due to the typical nature of its traffic flows and the organisation and capability of its networking equipment. In contrast, the nature of an ICS network does not typically provide favourable conditions for a passive scanner as its traffic flows are generally decentralised, and networking equipment is often simple and unable to offer the required services.

This paper has explored scenarios under which ICS equipment may commonly be deployed and identified use cases where passive scanning techniques are either unable, or impractical, to provide full network coverage. The auditing of devices present on safety critical control networks is entirely necessary to properly ensure the security and safety of such systems.

Fragility of the network and connected devices within legacy ICS environments almost entirely precludes the use of active scanning technologies due to the risk of unintentionally interrupting the process. The risk could potentially be minimised by using the approach taken by the Shodan search engine, as there have been no reported incidents of ICS equipment failure attributed to a Shodan scan. The success of Shodan appears to be due to it scanning a limited range of ports only, avoiding the more obscure and likely unstable services. Whilst this is undoubtedly a safer approach, it may not achieve full coverage. Actively scanning using the ubiquitous ARP protocol is also an option as the scanning process does not deviate from normal usage of the protocol, although the local subnet range of ARP and the possibility of it being disabled introduces limitations.

In conclusion, current technologies do not currently provide a complete solution to the device discovery problem which is one of the most fundamental steps in the security and monitoring of ICS/SCADA environments. Further research is required in a number of areas in order to advance design, development, and deployment of such technologies.

12. FURTHER RESEARCH

In order to perform full and effective inventory audits of ICS networks current tool-sets will need development to allow them to deal with the challenges and requirements of such environments. To facilitate this development, further research is recommended into the following areas:

12.1. The Shodan Approach

The lack of documented incidents attributed to Shodan scans, as discussed in Section 6.1, merits further investigation into this approach. Specific areas of interest are; what services are probed by Shodan and what is the prevalence of these services across common ICS components, what other services are ubiquitous across ICS components and are candidates for scanning, what is the likelihood of such an approach being accepted by vendors, integrators and owner/operators.

12.2. Vendor Tools

Some vendor tools are known to perform device discovery prior to proceeding with programming operations, in some cases using active polling techniques. An example of such a tool is Siemens Totally Integrated Automation (TIA). Further research should be conducted to determine what discovery techniques are used by these vendor tools. To support this research, it should also be understood how and where vendors recommend these tools be used.

12.3. Deployment Architecture

Where and how should passive sensors be placed within the network infrastructure, and how should the be configured. With an enterprise IT environment sensors can be reasonably at or near network gateways to capture typical traffic flows. ICS devices often will not communicate outside their subnet or group of locally connected devices. This behaviour dictates that a new strategy for sensor placement should be employed.

12.4. Effective, Efficient and Secure Device Discovery

If port mirroring or traffic replication technologies are used it should be understood what impact these may have on existing devices and infrastructure. What is the confidentiality or latency impact of replicating control network traffic to be fed into of if replicated traffic leaked onto the control network.

12.5. Metrics to Assess Coverage and Results

How can the level of network coverage that has been achieved during the scanning process be measured and quantified. If only partial coverage is achieved, it should be possible to assess or infer the full scope of the system in order to enable correct decision making about risks, asset vulnerabilities, and security architectures.

REFERENCES

Tenable passive vulnerability scanner data sheet (2013, Sept.) Tenable Network Security White Paper.

Optimizing it technology refresh policies (2015) An approach to balancing capital spending, operating efficiency, and risk mitigation. Archstone Consulting White Paper. Available from http://www.archstoneconsulting.com/services/it-strategyopeations/white-papers/optimizing-it-technology.jsp.

Bodenheim R. C. (2014 Mar.)*Impact of the Shodan computer search engine on internet-facing industrial control system devices* M.S. thesis, Air Force Institute of Technology Wrightpatterson AFB Oh Graduate School of Engineering and Management.

Byres, E. (2012 July) #1 ICS and SCADA security myth: Protection by air gap. *Tofino Security White Paper*

Choi M. (2013) Wireless communications for SCADA systems utilizing mobile nodes. *Int. J. Smart Home*, 7 (5), 1–8.

Dumont C. (2014 Jan.) NERC (CIP-002) identification of critical cyber assets

Galloway B. and Hancke G. (2013) Introduction to industrial control networks. *IEEE Commun. Surveys Tuts.*, 15 (2), 860–880.

ICS-CERT. (2014 Feb.) The ICS-CERT year in review 2013. USA Homeland Security ICS-CERT, Tech Rep

Liu G. and Neufeld N. (2009 Nov.) *Management of the LHCB network based on SCADA system*. CERN The European Organization for Nuclear Research Technical Report

Mohan, V. (2013 Nov.) It asset management benefits & best practices. *SolarWinds Worldwide LLC White Paper*

Nicholson, A. Janicke, H. and Cau A. (2014) Safety and security monitoring in ICS/SCADA systems. In: *Proceedings of the 2nd International Symposium for ICS & SCADA Cyber Security Research*

Nicholson, A et al. (2012) SCADA security in the light of cyber-warfare. *Comput. Secur.*, 31 (4), 418–436.

Oliva, S. A. and Crowe, B. (2003 Feb.) Network system and method for automatic discovery of topology using overhead bandwidth

Pauna, A. and Moulinos, K. (2013, Dec.) *Window of exposure a real problem for SCADA systems? recommendations for Europe on SCADA patching*. European Union Agency for Network and Information Security (ENISA), Tech Rep

Permann M. R. and Rohde K. C (2005) Assessment methods for SCADA security. In: *Proceedings of 15th Annual Joint ISA POWID/EPRI Controls and Instrumentation Conference*

Peterson, D. (2006 Nov.) Using the Nessus vulnerability scanner on control systems. *Digital Bond White Paper*

Peterson D. (2012) Using cyber security assessment tools on industrial control systems. *Digital Bond White Paper*

Scott, A. (2012, Apr.) SCADA security and the data link layer. Available from http://blog.cimation.com/blog/scada-security-and-theosi-data-link-layer

Stirland, J (2014, Dec.) Developing cyber forensics for SCADA industrial control systems. In: *Proceedings of the International Conference on Information Security and Cyber Forensics, Universiti Sultan Zainal Abidin, Kuala Terengganu, Malaysia*

Trabelsi Z. and El-Hajj W. (2010) On investigating ARP spoofing security solutions. *Internet Protocol Technology*, 5 (1/2).

Valladares C. (2012, Dec.) 20 critical security controls control 1: Inventory of authorized and unauthorized devices.

van der Knijff R. (2014) Control systems/SCADA forensics, what's the difference? *Digital Investigation*, 11 (3), 160–174. Special Issue: Embedded Forensics.

Wiberg K. C. (2006, Sept.) *Identifying supervisory control and data acquisition (SCADA) systems on a network via remote reconnaissance*. M.S. thesis, Naval Postgraduate School, Monterey, California.

Williams P. (2014 June) *Distinguishing internet-facing ICS devices using PLC programming information*. M.S. Thesis, USA Air Force Institute of Technology

Wu, T. et al. (2013) Towards a SCADA forensics architecture. In: *Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research*

Zhu, F., Mutka, M. and Ni L. (2002 Sept.) *Classification of service discovery in pervasive computing environments*. Michigan State University