Tampere University

Henri Pulkkinen

SAFE SECURITY SCANNING OF A PRODUCTION STATE AUTOMATION SYSTEM

Master of Science Thesis
Faculty of Engineering and Natural Sciences
Examiners: Professor Emeritus Hannu Koivisto
University Instructor Jari Seppälä
December 2022

ABSTRACT

Henri Pulkkinen: Safe security scanning of a production state automation system
Master of Science Thesis
Tampere University
Master's Degree Programme in Automation Engineering
December 2022

The amount of cybersecurity threats against industrial automation systems, OT and ICS environments, as well as critical infrastructure grows at a rapid pace. Cyberattacks against such systems might cause significant economic, physical, or reputational damage to the target organization. Due to the seemingly non-ending dangers these systems face, detection methods and tools against such threats are also continuously developed.

The purpose of this thesis is to study the current possibilities regarding security scanning of production state automation systems, such as industrial systems and critical infrastructure. The common scanning methods can be divided into active scanning and passive detection. Due to different issues in these methods, the best practice has conventionally been to use them both side-by-side, but more innovative practices have also been proposed and tested.

As a theoretical background for the study, it is relevant to define the pros and cons of the so-called conventional solutions and the most common tools. It is also important to study the basic characteristics of the automation systems being scanned, and the effects the studied security scanning solutions have on the systems. After the preliminary study, existing commercial products, such as Tenable Active Querying and Nozomi Smart Polling, as well as emerging technologies and proposed solutions, such as delay-based scanning and UDP based scans, are studied and analysed in appropriate depth to determine possible improvements for the commonly used methods in the area.

The thesis finally presents a proposal for optimal utilization of current and emerging technologies and solutions regarding security scanning of production state automation systems, based on the capabilities of current commercial products, as well as prior studies and the most recent developments in the area.

Keywords: information security, cybersecurity, security scanning, active scanning, passive detection, OT, ICS, vulnerability scanning, industrial automation systems

TIIVISTELMÄ

Henri Pulkkinen, Automaatiojärjestelmän turvallinen tietoturvaskannaus tuotantotilassa
Diplomityö
Tampereen yliopisto
Automaatiotekniikan diplomi-insinöörin tutkinto-ohjelma
Joulukuu 2022

Teollisiin automaatio-, OT-, ja ICS-järjestelmiin kohdistuvien tietoturvauhkien määrä kasvaa jatkuvasti. Kyberhyökkäykset näitä järjestelmiä vastaan voivat aiheuttaa merkittävää haittaa niin kohdeorganisaation taloudelle, fyysiselle ympäristölle, kuin maineellekin. Loputtomilta vaikuttavien uhkien takia myös keinot niiden havaitsemiseksi kehittyvät jatkuvasti.

Tämän työn tarkoituksena on tutkia tämänhetkisiä mahdollisuuksia tuotantotilassa olevan automaatiojärjestelmän, kuten teollisuusjärjestelmien, tietoturvaskannaamiseen. Perinteiset skannausmetodit voidaan jakaa kahteen kategoriaan: aktiiviskannaukseen ja passiiviseen havaitsemiseen. Koska sekä passiivisissa että aktiivissa metodeissa on puutteita, on yleisesti ottaen paras ratkaisu perinteisesti ollut käyttää näitä kahta keinoa rinnatusten, mutta myös uusia innovatiivisia ratkaisuja on alkanut viime vuosina ilmaantua niin uusien tuotteiden kuin tutkimustenkin muodossa.

Teoreettisena taustana tässä työssä käydään ensin läpi perinteisten metodien vahvuudet ja heikkoudet, sekä yleisimmät työkalut. On myös oleellista tutkia automaatiojärjestelmien ominaisuuksia, sekä tietoturvauhkien ja tietoturvaskannaamisen vaikutuksia niihin. Pohjatyön jälkeen tutkitaan olemassa olevia kaupallisia tuotteita, kuten Tenable Active Querying ja Nozomi Smart Polling, sekä uusia tutkimuksia, jotka tähtäävät skannaukseen liittyvien ongelmien ratkaisemiseen.

Lopulta kootaan tutkitusta materiaalista ehdotus parhaaksi mahdolliseksi ratkaisuksi turvalliseen tuotantotilassa olevan automaatiojärjestelmän tietoturvaskannaamiseen.

Avainsanat: tietoturva, kyberturvallisuus, tietoturvaskannaus, OT, ICS, haavoittuvuusskannaus, teollisuusautomaatio, automaation tietoturva

PREFACE

Many obstacles during the almost seven years of studies at Tampere University have been overcome to reach the gates of graduation. I want to thank all the lecturers and personnel at Tampere University, with special thanks to Jari Seppälä and Hannu Koivisto for all the valuable advice regarding the writing of this thesis. I would also like to thank all the fellow students I have met during the past years for all the adventures.

Tampere, 18th December 2022

Henri Pulkkinen

CONTENTS

LIST OF FIGURES

LIST OF SYMBOLS AND ABBREVIATIONS

ANSI/ISA	American National Standards Institute / Society of Automation
AP	Access Point
API	Application Programming Interface
ARP	Address Resolution Protocol
CB	Carbon Black
CIP	Common Industrial Protocol
CPE	Common Platform Enumeration
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DB	Database
DCS	Distributed Control System
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DoS	Denial of Service
DPI	Deep Packet Inspection
EOL	End of Life
ERP	Enterprise Resource Planning
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IACS	Industrial Automation and Control Systems
ICS	Industrial Control System
IDS	Intrusion Detection System
IE	Industrial Ethernet
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IIoT	Industrial Internet of Things
IO	Input/Output
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
LIMS	Laboratory Information Management System
MAC	Media Access Control
MDNS	Multicast Domain Name System
MES	Manufacturing Execution System
MITM	Man in the Middle
MS	Microsoft
NAS	Network-attached Storage
NBNS	NetBIOS Name Service
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OS	Operating System
OT	Operational Technology
OWASP	Open Web Application Security Project
PID	Proportional-integral-derivative
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SPAN	Switch Port Analyzer

SSDP	Simple Service Discovery Protocol
SSH	Secure Shell
SYN/ACK	Synchronize/Acknowledge
TAP	Test Access Port
TCP/IP	Transmission Control Protocol
TSN	Time-sensitive networking
UPnP	Universal Plug and Play
US	United States
VPN	Virtual Private Network
WinRM	Windows Remote Management
WLAN	Wireless Local Area Network
WMI	Windows Management Instrumentation

.

1. INTRODUCTION

This chapter defines the basis and motivation, as well as the research questions and limitations for the thesis.

1.1 Background

Cybersecurity has been gaining more and more attention in business decision making, IT management, and even in media. The most major breaches in cybersecurity make headlines just as any other disaster. For example, the Colonial Pipeline ransomware attack in the US, and the Log4Shell vulnerability (CVE-2021-44228) received global attention in 2021 [1, 2]. In 2022, the war in Ukraine has also put cybersecurity in the spotlight, especially regarding critical infrastructure, such as the electrical grid and power plants, as well as government websites and banking services [3]. Cyberwarfare was also a common topic especially during early stages of the invasion. A sign of the growing attention to cybersecurity is also the cybersecurity voucher program launched by the Finnish government, supporting companies in enhancing their cybersecurity capabilities, especially regarding critical infrastructure. [4]

For industrial internet of things (IIoT) and operational technology (OT) systems, such as industrial control systems (ICS) the risks posed by cyber threats are also significant. An attack against such system could for example be an unauthorized starting or stopping of a system, possibly putting personnel within the physical production site in danger or causing the destruction of production machinery. Leakage of personal or otherwise critical data, such as technical details of products or production methods might cause the victim economic harm either in the form of losing competitive advantage, having to purchase and install new production equipment, having to pay a ransom to the attacker, or being fined by authorities for data privacy related mismanagement. Of course, such events might also lead to reputational damage to the target organization.

Examples of cybersecurity incidents targeted at industrial control systems include for example the infamous Stuxnet malware, discovered in 2010, damaging the Iranian nuclear program and the BlackEnergy 3 malware, targeting the Ukrainian power grid in 2015. In both of these cases the damage was caused through affecting the target's Supervisory Control and Data Acquisition (SCADA) system. [5]

Industrial systems, for example manufacturing sites, production lines and power plants, can consist of hundreds, if not thousands of different components and devices. This is nothing new, as such systems have been quite complex from the time they started to emerge decades ago. The technological development during the past decades however, highlighted by the invention of the internet, has however created a whole new dimension to the complexity of these systems. Modern data transfer protocols and communication channels allow the components and devices in these systems to be continuously connected and communicating between each other, creating the so-called Internet of Things (IoT), a core concept in modern automation systems.

These latest advancements in industrial systems are also often combined under the term Industry 4.0, or the fourth industrial revolution, likening the significance of IoT and the impact it has had and will have to industrial systems to that of the invention of the steam engine during the original industrial revolution in the 18th century, the utilization of mass production and assembly lines in the late 19th century, and the emergence of computers and automation in industry in the 20th century. [6]

New technologies, such as IoT and IIoT, have made the automation systems like ICS more efficient and more profitable, but also more prone to cybersecurity issues. The systems can include a massive number of various kinds of components with different functions and abilities, some of which have security vulnerabilities in their own designs as well. The complexity of these systems makes them difficult to manage, allowing malware and other security issues to stay hidden, and creating an opportunity for external, malicious, devices to connect to the automation network in secrecy.

The balance between cybersecurity and economically efficient production is however a slippery slope for many businesses. Security is not free, and the cheaper the devices in the automation environment are, the more vulnerable they tend to be. For a large organisation, the cost of maintaining functional and competent cybersecurity personnel and security tools might also be expensive. The arsenal of security solutions developed for protecting these environments from outside threats is nowadays also vast. Common solutions include firewalls, antivirus software, intrusion detection systems (IDS) and intrusion prevention systems (IPS). Network management and configuration solutions, like network segmentation, are also recommended. This thesis focuses on one specific solution: security scanning.

Scanning is a common technique used by security personnel, penetration testers, as well as cyber criminals and other malicious actors, to collect data about several attributes, like active hosts, devices, open ports and used protocols within a network. The main

benefits of scanning are discovering existing assets in order to obtain an asset inventory, as well as identifying security vulnerabilities in the network and the devices in it.

Active scanning, in which the network is commonly mapped with an automated or semi-automated scanner that sends requests to all possible IP addresses within the network, has however not been seen as viable option in production state industrial automation networks, as the devices, and the network itself, are usually not designed to handle the kind of traffic generated by the scanners. Passive detection, in which data is only collected by monitoring the network's natural traffic flow, can on the other hand not identify all required data needed for a comprehensive vulnerability analysis, and can also be completely evaded by malicious and silent devices.

This thesis attempts to identify solutions for achieving the benefits and results of conventional active scanning, while avoiding congesting the network, harming the devices or otherwise interrupting production. The study is conducted by gathering and analyzing relevant existing commercial solutions aiming to solve issues regarding security scanning of a production state automation system, as well as academic and scientific studies related to the topic.

1.2 Research questions

The objectives of this thesis are:

- Mapping and analyzing any recent developments, emerging technologies and recently proposed solutions that aim to achieve vulnerability identification and asset inventory results similar to that which active scanning tools like Nmap and Nessus scanner can achieve, without disturbing the production ICS network's and devices' normal functions.
- Based on studied material, compiling the best possible set-up for security scanning in a production state ICS network for asset discovery and vulnerability identification purposes.
- Estimating future developments and study subjects regarding the topic.

1.3 Limitations

The execution of this thesis does not include any practical experiments and focuses only on open-source theoretical study. The scope is limited to the security scanning of OT and ICS networks.

1.4 Thesis structure

Chapters 2 and 3 introduce the reader to the basic components laid out in the title of the thesis, i.e., what is meant by automation systems, as well as the relevant aspects of security scanning. Chapter 2 discusses automation systems through relevant frameworks and concepts as well as the development history of these systems and the security issues they face. Chapter 3 presents the motivation behind security scanning, and defines relevant concepts, including passive detection and active scanning, as well as their shortcomings. Chapter 4 discusses the existing commercial solutions aiming to solve the issues regarding the security scanning of production state automation systems, while Chapter 5 focuses on recent studies regarding novel solutions and technologies that could help solve these issues in the near future. Finally, Chapter 6 summarizes the findings of the conducted research and Chapter 7 provides a best possible set-up for obtaining information about the assets within an automation network based on the conducted research.

2. AUTOMATION SYSTEMS AND SECURITY ISSUES

Modern automation enables consistent, reliable and efficient production, which is more important than ever in today's fast paced world. Optimized utilization of such modern technology can give a major competitive advantage to a business. Advanced equipment, such as precise sensors and computer-based control allow for example manufacturing machinery to be fine-tuned continuously to reach the highest production levels.

Automation systems can vary in their size, structure, and architecture. They can be small-scale smart home systems or massive industrial complexes, flat networks or carefully segmented networks, or anything in between. In this chapter, some relevant background regarding automation systems, relevant models, and their development history, as well as other relevant concepts, are discussed.

2.1 Industrial systems

A common concept with industrial automation systems is operational technology (OT). The term OT has traditionally covered systems that manage the creation of physical value and manufacturing processes, complementing information technology (IT), which focuses on technologies related to information processing [7]. In more detail, the National Institute of Standards and Technology (NIST) defines OT to consist of systems and devices that interact with the physical environment, causing or detecting changes to physical devices or objects through monitoring or control of devices, processes, and events [8].

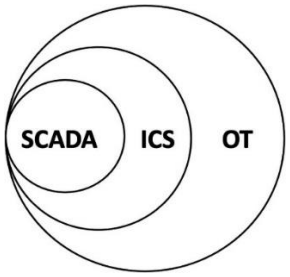

Figure 1. *Relation of OT, ICS, and SCADA. [9]*

One subset of OT is an industrial control system (ICS). ICS is a general term but can be defined to mean systems that are used to control industrial processes, such as manufacturing. Systems that ICS encompasses include for example supervisory control and

data acquisition (SCADA) and programmable logic controllers (PLC). The hierarchical relation of OT, ICS and SCADA is visualised in Figure 1 above. [9]

The term Internet of Things, or IoT, was first used as early as the year 1999. The heart of IoT are “smart objects”, that are able to generate, exchange and consume data with minimal human intervention, and a network that is formed by such devices is nowadays commonly called an IoT network. The continuous connectivity of these devices, resulting in the possibility for each “thing” to continuously communicate its state with other objects within the environment, is the feature most commonly associated with IoT. [10]

IoT systems can be found even in households, where they are usually small-scale smart home systems, in which the things might include appliances such as toasters, televisions, or automated garage doors. For this thesis, the focus turns to industrial internet of things, or IIoT systems, which may form large industrial complexes, such as factories. These systems may in turn consists of “things” of all sizes, such as engines, power grids and sensors that are all connected through a network. Despite the similarities in their natures, the features of IIoT devices, including their security features, might differ from plain IoT devices. For systems considered in this thesis, OT systems are often also IIoT systems. [11]

2.2 Purdue model

A common way to present a conventional automation system is the usually pyramid-shaped Purdue model, which was developed already in the 90s to work as a reference model of the segmentation of an industrial control system (ICS). It consists of five distinct control layers: enterprise (layer 4), planning (layer 3), supervisor or operator (layer 2), control (layer 1), and field (layer 0). Each layer is associated with a separate control network, which would in a securely configured network be assigned as different network segments. In some sources the model divides the system further into six layers and an industrial demilitarized zone (DMZ) might be considered [12]. Additionally, the layers might be number from 1 instead of 0. Some sources might also alternatively refer to the ANSI/ISA-95 standard, which presents a model very similar to the Purdue model. Figure 2 presents an illustration of the Purdue model as it is interpreted within this thesis. [14]

At the bottom of the figure, in layer 0, we have components that are located physically in the production environment, such as sensors, transmitters and control valves. The functionality of the devices in this layer consists of sensing and measuring the environment and manipulating it accordingly, as steered by level 1 devices. This is where the largest number of components within the whole automation system reside, meaning the largest

possibility of variance between different communication methods and security capabilities is also within this layer.

Layer 1 contains control systems, such as programmable logic controllers (PLC), distributed control systems (DCS), proportional-integral-derivative (PID) controllers and batch controllers. Layer 1 systems are responsible for automated monitoring and controlling of the layer 0 systems, and a typical response time is measured in sub seconds. Layer 1 systems communicate with layer 0 devices both to collect data about the functional, physical status of the system, and to correspondingly control it. The lower levels 0 and 1 utilize process sensor networks, which have traditionally, in the absence of wireless solutions, utilized control bus and field bus solutions with at times large physical wirings.

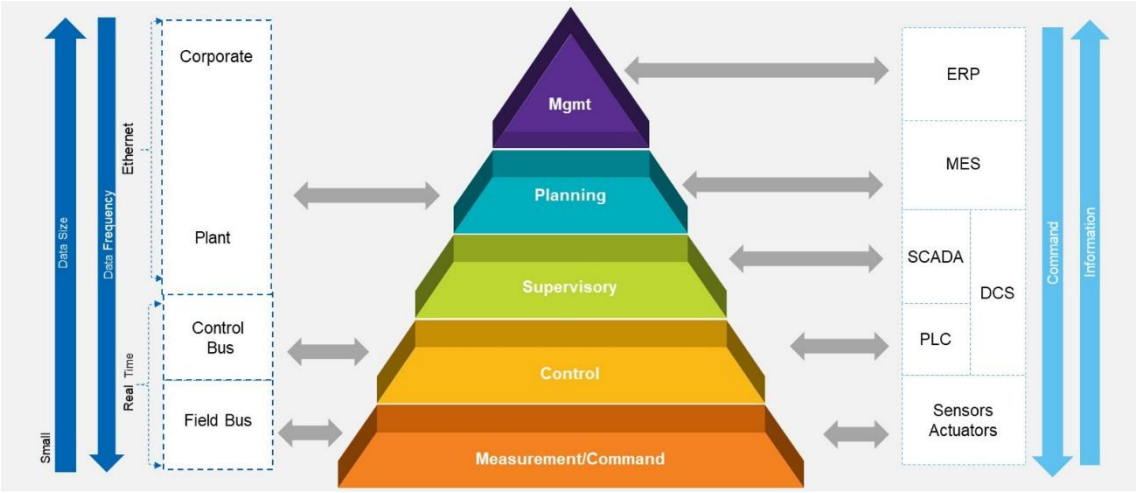

Figure 2. *Purdue model for automation system infrastructure. [13]*

Layer 1 systems are in turn connected to layer 2 operator or supervisory systems, like human-machine interfaces (HMI) or supervisory control and data acquisition (SCADA), via a plant control network. The functionalities of these systems are mainly so-called manufacturing operations management tasks, such as quality assurance and inventory movement functions. The list of devices might also include engineering workstations.

Layer 2 is connected by a plant information network to layer 3. Layer 3 consists of IT systems intended to perform detailed scheduling, production execution and production analysis. The layer includes systems such as manufacturing execution system (MES) or laboratory information management system (LIMS). These systems produce reports to corporate systems at layer 4 and correspondingly receive orders and distribute them the OT systems in the lower levels.

At the top of the hierarchy there is layer 4, which consists of systems like enterprise resource planning (ERP), that provide management information systems and decision support systems. These systems might span across multiple plants and provide information for example on the overall production rates, inventory, and demand on the corporate level. [14]

2.3 Modern automation systems

Automation systems have evolved greatly during the past decades. The emergence of new technologies has allowed a rapid incorporation of novel solutions and more sophisticated and efficient devices to the systems. Simultaneously, the architectural solutions and security requirements have also changed. To counter problems caused by the rapid change within the industry, alternative, modernized models, solutions and standards have also been developed.

As previous, generally IT focused standards have not been appropriate for OT environments, new, OT targeted standards have been developed. One such is International Electrotechnical Commission's IEC 62443 standard series. The standard family aims to especially address risks related to cybersecurity threats in modern industrial automation and control systems. [15]

Especially the IEC 62443-3-2 standard, Security Risk Assessment and System Design, covers several topics relevant to this thesis. As part of the processes aimed to securing an industrial automation and control system (IACS), the standard talks about threat identification and vulnerability identification. [16] Regarding these objectives, implementing a regular, scheduled security scanning routine would be recommended.

A central concept in the IEC 62443 is the partition of the manufacturing network into security zones (Figure 3) that are based on specific security requirements shared by the elements within a zone. An additional concept are conduits, which define the communication paths between different security zones. Zones and conduits, which are not inherent to for example the Purdue model, are also a cental part of IEC 62443-3-2. [17]

The applicability of IEC 62443 to an IIoT environment has also been under the microscope. *Leander et al.* concluded in their study that the several parts of the standard are well suited in the context of IIoT systems, but there are also some concepts that might prove difficult for such systems to comply with. The problematic parts include for example the prementioned security boundaries within a system, as such boundaries are more difficult to withhold due to the dynamic characteristics of IIoT, and the need for devices to communicate over zone boundaries. [17, 18]

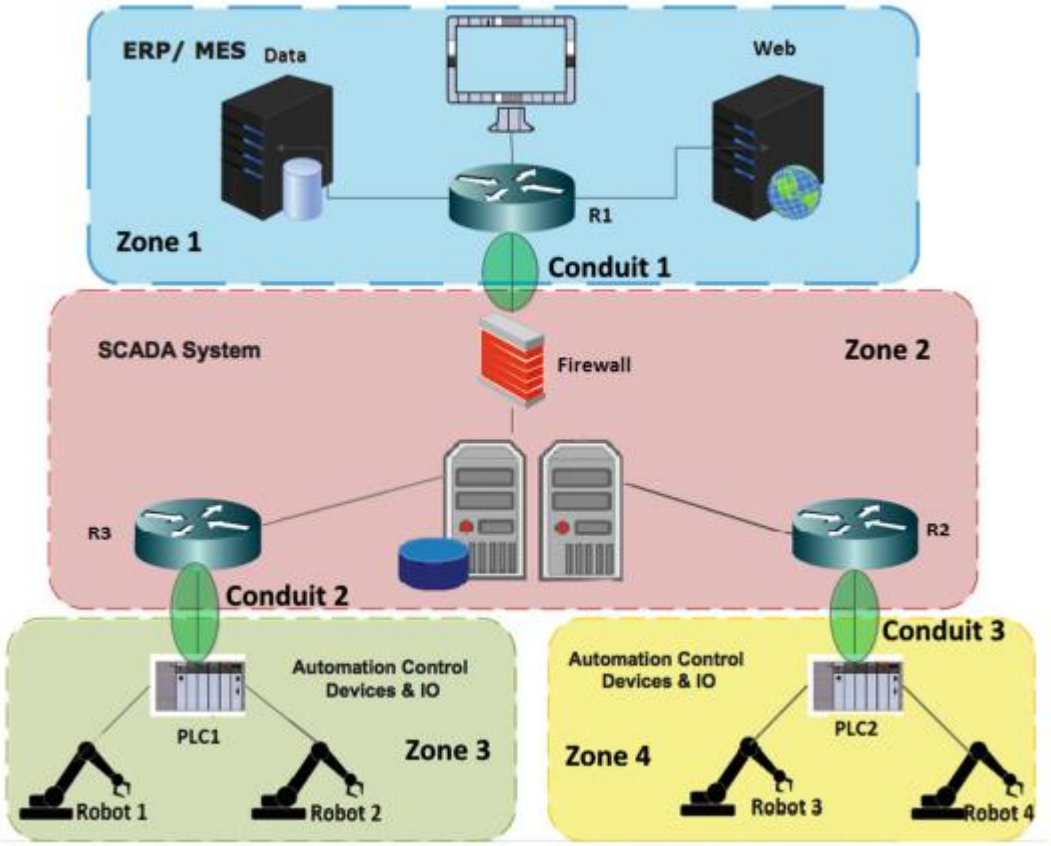

Figure 3. *Security zones and conduits. [17]*

Another key concept of modern automation systems is industrial ethernet (IE). Ethernet was originally designed for office use with the basic task of transmitting a signal between two devices. It was however not very suitable for industrial systems, as it did not for instance distinguish or prioritize packets in any way and had rather limited bandwidth (10 Mbps). Technical advancements, such as the appearance of Fast Ethernet (100 Mbps) and further Gigabit Ethernet (1 Gbps) have however enabled Ethernet to be used by industrial applications as well. Industrial Ethernet does however still face problems, such as latency issues when mixing a variety of data streams. [19, 20]

A major ongoing research subject in the area since 2012 is time sensitive networking (TSN), a joint project between the International Electrotechnical Commission (IEC) and the Institute of Electrical and Electronics Engineers (IEEE), which aims to provide a collection of standards for deterministic time-sensitive transmission of a variety of data streams on standard Ethernet with zero loss from congestion. To achieve this, TSN is set to utilize for instance synchronization for time-sensitive applications, bandwidth reservation, frame preemption and redundant message transmission. The advent of TSN could change the industrial automation landscape drastically. [19, 21]

2.4 Industrial automation security issues

Many automation systems are attractive targets for malicious actors. There are many reasons to why someone might purposefully attack such a system, like vandalism, search for adrenaline, search for a challenge, curiosity, political, as well as environmental reasons, and simply economic motivations. Certain state actors might also be interested in the possibility of causing harm to critical infrastructure systems, such as power grids and power plants. [22]

The spectrum of cybersecurity risks is vast. Many typical risks seen in all IT systems are relevant for automation systems as well. These might include subjects like malware, man-in-the-middle attacks, data leakage, and denial-of-service (DoS) attacks. Most of the time vulnerabilities are caused by flawed design of the systems, misconfigurations, or other human error. Making these complex systems completely secure is a burdensome and difficult, if not impossible task.

The Open Web Application Security Project's (OWASP) 2018 IoT top 10 list provides a good overall view of the security issues associated with the Internet of Things. [23] Many of them are especially relevant for automation and industrial IoT systems. The list consists of the following ten topics:

1. Weak, Guessable, or Hardcoded Passwords
2. Insecure Network Services
3. Insecure Ecosystem Interfaces
4. Lack of Secure Update Mechanism
5. Use of Insecure or Outdated Components
6. Insufficient Privacy Protection
7. Insecure Data Transfer and Storage
8. Lack of Device Management
9. Insecure Default Settings
10. Lack of Physical Hardening

Regarding the list's topic number 5, Use of Insecure or Outdated Components, it is worth noting that conventionally automation systems typically have a long lifespan compared to IT systems. Normally device and software manufacturers provide support for their products at most up to a couple of years (e.g., Microsoft Windows operating system). An industrial automation system's lifespan might however be measured in decades. Even

with good lifecycle management, some components might reach their end-of-life, leaving them vulnerable for attacks. For larger industrial automation systems, the usage of end-of-life components is almost inevitable. Thus, the importance of OWASP list's topic number 5 is especially relevant for automation systems. [24]

Additionally, regarding topic number 5, the selection of IIoT devices is abundant, and the components might come from various third-party sources. Especially when going for the cheapest option when selecting a certain IIoT device, especially in layer 0, it is possible for the software or hardware to be compromised from the get-go. An untrusted party may have cloned the physical characteristics and firmware of an IIoT device, while reverse engineering and altering its software, for example by adding a backdoor. It is possible that such an altered device is even intended to control another, genuine device, work as a man-in-the-middle device or perform some other type of attack. Therefore, procurement and supply chain management also play a role in IIoT and industrial security. [25]

The wide variety of different types of devices also means different types of communication systems, each of which might have their own security related protocols in place. The compatibility of these devices and the heterogenous communication systems may require data format conversion, which might be problematic. Furthermore, the presence of unknown and undetected information channels is possible, presenting a constant threat. [26]

OWASP topic number 2, insecure network services, is an interesting one regarding the objectives of this thesis, as discovering such unneeded and insecure services is a major objective in security scanning. Many automation systems also have some type of remote-control systems for control or maintenance purposes. These systems create an additional attack vector, which poses a characteristic, major risk for automation systems. When configured insecurely, these remote systems might be vulnerable for example to command injection or emergency stop abuse attacks. The usage of insecure network services magnifies the risk even further. [27, 28]

For most industrial systems, software updates can only be applied during maintenance breaks or other production stoppage. In some cases, factory personnel, such as engineers responsible for the functionality of the factory, might choose to not update systems even then with the purpose of minimizing changes that are deemed unnecessary, with the purpose of ensuring the system stays functional. For systems that are run around the clock, this means that update intervals might be significantly stretched, highlighting the OWASP topic number 4, lack of secure update mechanism. [29]

Some of the technologically light, efficient, and possibly cheap components might also not be designed with security in mind and might thus have fundamental vulnerabilities in them. This is especially true for layer 0 devices (Figure 2). Many devices do also simply not have the features, such as required memory, storage, and power resources to equip any security software or intrusion prevention system (IPS), which further enlarges the possible attack surface. [25, 30]

Automation systems can also be very sensitive to even minor deviations to normal circumstances. Automation systems typically have for example specifically strict real-time requirements, meaning they have a certain response time which they must be able to fulfil. These requirements may have hard deadlines and missing one could lead to the failure of the entire control flow, rendering the entire system unusable [26]. For critical infrastructure, even such minor deviation could be catastrophic, possibly causing severe physical danger. An example of such a system could be, for example, a control system of a nuclear power plant.

A more concrete threat is the possibility of outside, unauthorized devices to be connected to an internal ICS network. For example, in a factory environment, this could be done simply by an individual person gaining access to the factory floor and planting the device there. The individual could be an unauthorized person, or even an authorized one, such as maintenance personnel from an IT supplier turning out to be a malicious actor or for example bribed. Therefore, physical security dimensions are also important to the overall cybersecurity. A carelessly configured wireless network can also be visible beyond its intended physical coverage area, such as the premises of a factory building, which would make it possible for unauthenticated devices to be connected to the network even from outside the building.

A network visible to the outside, whether that be the WLAN visible outside the physical building or the network being visible on the internet, ICS networks may also be vulnerable to man-in-the-middle (MITM) attacks. In a man-in-the-middle attack, a malicious actor intercepts, modifies, and finally transmits data, appearing to be the original sender, attempting to steal information from the network or inserting malicious data into the network or devices in it, endangering the integrity of the data.

An end-to-end encryption may mitigate this problem. However, some devices in the network, especially ones in the lower levels of the system (levels 0 to 2), might not have the abilities, like required memory, to manage encryption. There are however some cheap, effective hardware crypto systems available that aim to solve this issue. Alternatively, a more powerful platform, for example a 32-bit device instead of an 8-bit one, could be

used to tackle this issue. However, encrypting the data might lead to issues regarding the real-time requirements of these systems, which in current networks renders the listed solutions unsuitable. Additionally, while disturbing malicious activity in the network, encryption would also weaken the possibilities for detecting assets through passive detection. The lack of proper encryption also relates closely to the OWASP list's topic number 7, insecure data transfer and storage. [30, 31]

3. SECURITY SCANNING

Security scanning is an automated or semi-automated function, which aims to find security flaws and weaknesses in a certain target network, sub-network, host, or other specified target, even the whole internet. This chapter discusses the purposes, techniques and some common tools used in such scanning, as well as relevant theory behind it. Scanning methods can be categorized in many ways, and for the purposes of this thesis, it is especially relevant to discuss the differences between passive detection and active scanning.

3.1 Purpose of scanning

Security scanning has several objectives and benefits. One of the main purposes is mapping the network for security vulnerabilities, both by cybersecurity personnel and attackers looking to hack into the system. Another objective for many organizations is maintaining an asset inventory of the found devices and their properties. These results can further help in tasks such as event logging, troubleshooting, threat modelling, patch management, security hardening, segmentation verification, intrusion detection, incident response, disaster recovery, forensic investigation, as well as testing and verifying configuration changes.

3.1.1 Vulnerability identification

The main purpose for security scanning is, of course, security. Security scans can be utilized in pinpointing different kinds of cybersecurity vulnerabilities and issues within the target host or network, making it a major tool for cybersecurity personnel as well as outside attackers.

Scanning can for example allow the finding of unnecessary open ports and services running on them, which could make the target susceptible for attacks over the internet. Another found vulnerability might be the usage of default password and usernames, or other vulnerable security setting configurations. The usage of weak credentials in the prementioned unnecessary services would be a fundamental security blunder, but might be reality due to carelessness, the complexity of a system, or plain incompetence. In any case, such mishaps can easily be found with proper security scanning procedures. [31]

A common security scanning finding is missing patches or updates, as well as the discovery of end-of-life (EOL) components. Most found vulnerabilities in software are fixed

with security patches from the component vendor, and neglecting these patches essentially leaves the systems vulnerable for attacks. Most such known vulnerabilities have exploits for them, sometimes even with step-by-step instructions available on the internet. This means that a capable malicious attacker should have no problem exploiting such vulnerabilities, should he or she discover them in the target system. Therefore, it is essential for the defensive side to find the vulnerabilities as soon as they appear to be able to mitigate the risk these vulnerabilities impose by either patching the system or otherwise minimizing the harm a possible attacker could do. For EOL components, the best mitigation action is to upgrade the device to a supported one. Merely the existence of an EOL device in a network, regardless of if it has known vulnerabilities or not, is usually already considered a major risk. [32]

Scanning can also reveal the usage of vulnerable protocols within the network. One such protocol would be hypertext transfer protocol (HTTP) instead of hypertext transfer protocol secure (HTTPS). The usage of HTTP would leave the network vulnerable for man-in-the-middle (MITM) attacks [34] However, due to automation system's typical real-time requirements, as well as the usage of very old machinery, the utilization of encrypted protocols might cause problems. In an otherwise properly secured or isolated internal network this vulnerability might also be deemed acceptable or not relevant. However, for a proper assessment and mapping of protocols used in a network, and the security issues they pose, a security scanning is arguably the most useful and efficient tool.

Scanning can also be utilized in detecting unauthorized, malicious, rogue, or otherwise unknown devices connected to the network. Such devices might be for example leftover testing platforms, left in the network due to negligence, or even purposefully planted devices used for harming or spying on the network. For such devices, the only way for discovering their existence might be scanning the network. [32]

The types of security scanning results mentioned here can generally be achieved with active scanning methods known as port scans or vulnerability scans. Typical security scanning tools for IP networks include Nmap, Tenable Nessus and OpenVAS. General vulnerability identification tools and scanning types are discussed further in Chapters 3.3 and 3.4.

3.1.2 Asset discovery and inventory

Network scanning is a major component in maintaining an up-to-date asset inventory of an industrial automation system. Indeed, besides having a flawless change management process, network scanning is arguably the best approach for such a task. A proper asset inventory helps in asset management, which is important for several reasons, including

but not limited to security. As a system grows larger and larger and new components are introduced to it, scanning becomes more and more essential for the maintenance of such an inventory.

A comprehensive asset inventory includes information regarding OS and software versions, as well as patch status, helping system owners and security personnel ensure that all hosts and software are properly patched, preventatively minimizing the system's attack surface. Task related to maintaining the security posture of a system, such as mapping for example unpatched devices, would in a large organization be extremely inefficient and time consuming without an up-to-date asset inventory.

An accurate inventory also enables shorter response times to security alerts and incidents, as security personnel have up-to-date data regarding e.g., device configuration, software versions, system owners, and other critical information about affected systems, available to them. An asset inventory is thus valuable also for disaster recovery purposes after an attacker has already managed to do some damage to the organization. The security dimensions of asset discovery and inventory are also included in the prementioned OWASP IoT top 10 list in topic 8, lack of device management [23].

An asset inventory has non-security related benefits as well. Comprehensive asset inventory can be further enriched or used as raw data to help businesses optimize their functions. It can for example provide auditors detailed system information, shorten help desk response times, and help an organization identify how many software licences are used in relation to how many have been paid for. [34]

3.2 Internal and external scanning

Security scanning can be either internal or external, depending on the placement of the scanning appliance. In an external scan, the scanning is performed over the internet, from the perspective of an attacker on the outside. An internal scan is performed from within the internal network, mimicking a scenario where the attacker has already gained access to the network. Many IIoT and IoT devices are, either intentionally or unintentionally, visible on the internet and to external scanning, and thus form a significant security risk. However, for this thesis, the focus is on internal security scanning. [32]

3.3 Passive detection

Passive asset detection, in some sources passive scanning, is the method used to map devices in a network by monitoring, reading, and analyzing the raw network traffic without inserting any extra input to the network flow. Passive asset detection can be performed

continuously, 24 hours a day and it detects all active assets in the network as they become active, i.e., when they produce traffic for the asset discovery application to detect. A well-executed configuration can achieve real-time visibility to the target network's active assets.

3.3.1 Packet capture

A typical technology used for reading the raw network traffic is packet capture (pcap), Common implementations of pcap include WinPcap, libpcap, and Nmap project's pcap library for Windows, Npcap. It allows software to capture, or *sniff*, raw network traffic (including wireless networks, wired ethernet, localhost traffic, and many VPNs) using a simple, portable application programming interface (API). Common sniffing software that utilize Npcap include Nmap, p0f and Wireshark. It also allows for sending raw packets to the network, meaning it is also used for active scanning. Nmap and active scanning are discussed in more detail in Chapter 3.4. There are also specifically designed automation system management tools that utilize Npcap in inventorying specific devices. One example for such software is Profinet Commander, which uses Npcap technology for listing active PLCs. [35, 36, 37, 38]

3.3.2 Passive detection sensors

Passive detection systems have passive sensors placed in the system. These sensors do the actual detection of traffic flow within the network. Usually, they then send it to a controlling device, which analyses the traffic. Figure 4 below is an example of such a sensor, Nozomi Guardian's NSG-HS Series for large enterprises, which can cover over a million devices and has a maximum throughput of 6 Gbps [39]. The larger sensor can further be connected to a maximum of 50 remote collectors, such as the Nozomi NRC-5 low-resource sensor in Figure 5, which has a maximum throughput of 15 Mbps. [39]

Figure 4. *Nozomi NSG-HS sensor. [39]*

Figure 5. *Nozomi NRC-5 sensor. [39]*

Passive detection sensors are connected in the target network at certain access points so that they can observe the by-passing traffic. Sensors might be placed for example in each network segment in a plant, and an access point might be for example a Test Access Point (TAP) or a switch's Switched Port Analyzer (SPAN) port. With such techniques, the network traffic is replicated by the switch from respective ports to a spare port, often the SPAN port [40]. The usage of SPAN is also known as spanning and port mirroring [38]. Figure 6 is an illustration of port mirroring with a switch placed between a controller, such as a PLC, and a corresponding workstation, and the passive sensor connected to the SPAN port of the switch. [42, 43]

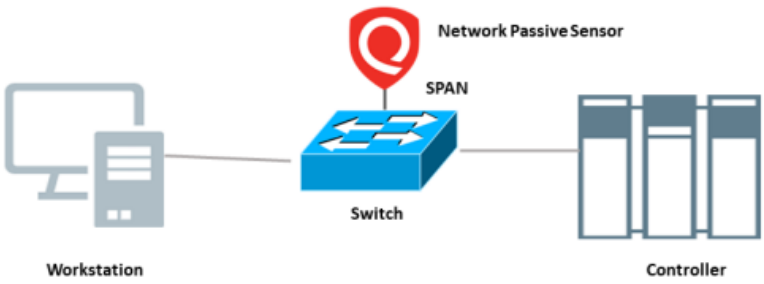

Figure 6. *Illustration of port mirroring. [40]*

3.3.3 Traffic analysis

The strategies for processing asset information through passive detection can vary. The core function is to maintain a list of IP addresses within the automation network. This can be achieved by simply monitoring and logging the addresses from the IP packets. Other key details to track include for example device type, and operating system (OS). Even such basic pieces of information can reveal security vulnerabilities, and methods for acquiring that information have been around for years. For example, the Satori tool, for which the development started already in 2004, identifies operating systems by analyzing dynamic host configuration protocol (DHCP) message's features [44]. Passive packet detection can also utilize deep packet inspection (DPI) to analyze the network traffic, such as in the case of Nozomi Guardian [45].

Figure 7 presents an illustration of the basic architecture of passive detection with Claroty products by Garland Technologies. In this scenario the switches at the edge of the network on levels 0-2 are used as an access point for the passive sensor at the edge of level 3. The intercepted traffic is analyzed with techniques such as DPI, and the found

assets, vulnerabilities and threats are presented visually on the level 4 graphical user interface, in this case Claroty Continuous Threat Detection. [46]

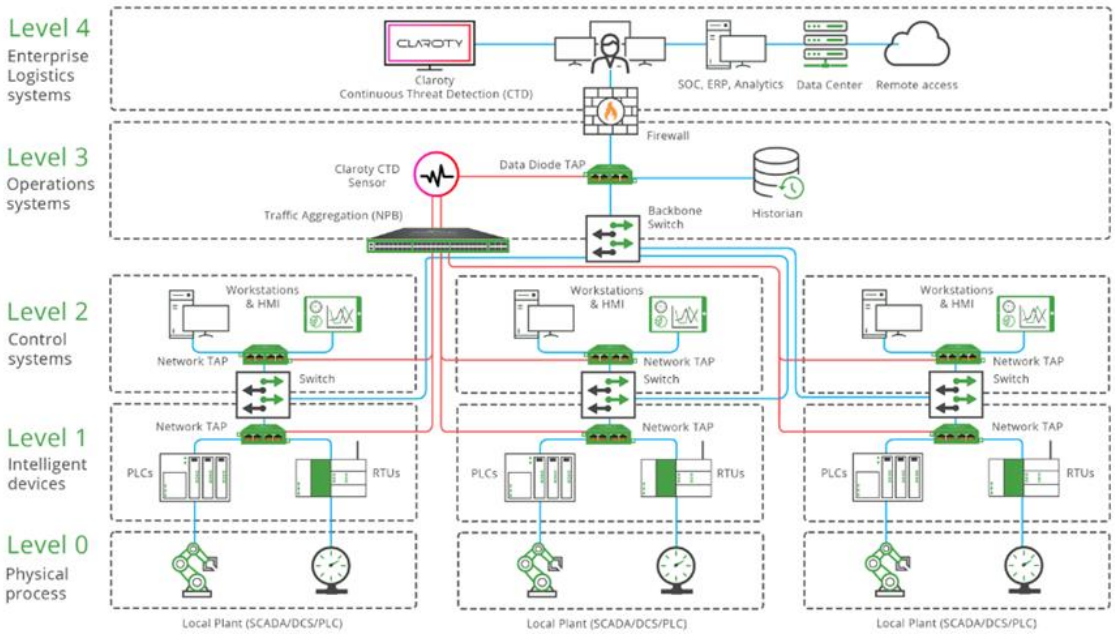

Figure 7. *Basic architecture of passive detection. [46]*

Data collected via passive detection can be further enriched to provide even more information about assets. Pieces of data can be used to identify devices for example by fingerprinting. The basic idea of fingerprinting is to identify unique patterns or features from the network flow in order to create a unique signature to identify specific devices or their attributes. A sufficient fingerprinting tool must however be able to differentiate between actual and forged fingerprints. *Xu et al.* provide a taxonomy of features that can be used in wireless device fingerprinting. Such features might be extracted not only from the TCP/IP stack's data link layer, but also physical, application and transport layers. [47]

Advanced solutions regarding plain IoT asset analysis have been studied and developed to an increasing extent in recent years. For example, *Miettinen et al.* present a device-type fingerprinting framework for IoT devices, called IoT Sentinel, which uses a novel method to collect data through passive monitoring to identify specific model and software version of each device. Furthermore, *Miettinen et al.* propose a novel device-type-specific anomaly detection solution to detect compromised IoT devices with few false alarms, called Dïot. The applicability of these approaches to an automation environment should however be studied further. [48, 49]

3.3.4 Modern passive detection products

An example of a state-of-the-art passive discovery and vulnerability detection software is Nozomi Guardian, which combines passive threat detection, asset inventory and vulnerability identification. Combining the benefits and possibilities of passive detection into one product, it has a significant foothold on the market.

Nozomi Guardian provides information on security risks on the network. It utilizes the U.S. government's National Vulnerability Database (NVD) for vulnerability scoring and cataloguing. NVD scores vulnerabilities using the Common Vulnerabilities and Exposures (CVEs) system, as well as the Common Vulnerability Scoring System (CVSS) and matches the devices to these known vulnerabilities. Both Guardian and NVD utilize the Common Platform Enumeration (CPE), allowing detected devices to be matched to vulnerabilities seamlessly. All this considered Nozomi Guardian appears to be able to automatically uphold an up-to-date view on current and emerging threats in a system. [50]

Nozomi Guardian also detects anomalies in asset behaviour. Nozomi claims the product is able to understand normal, expected changes in the analyzed assets, allowing it to filter out false-positive alerts for anomalies caused by such behaviour. It also utilizes deep packet inspection to analyze the traffic. With an additional subscription, Guardian will also receive regular updates for device profiles and behaviour data. Another additional subscription service provides threat intelligence regarding emerging threats.

Figure 8 below is a screenshot of a Nozomi Guardian single asset view. The information regarding a single asset in an asset inventory includes, for example, IP address, MAC address, used protocols, and the level of information gathered on the specific node (learning status). For this Windows Desktop machine, several vulnerabilities have also been identified. Nozomi Guardian's active scanning features are discussed further in Subchapter 4.1.

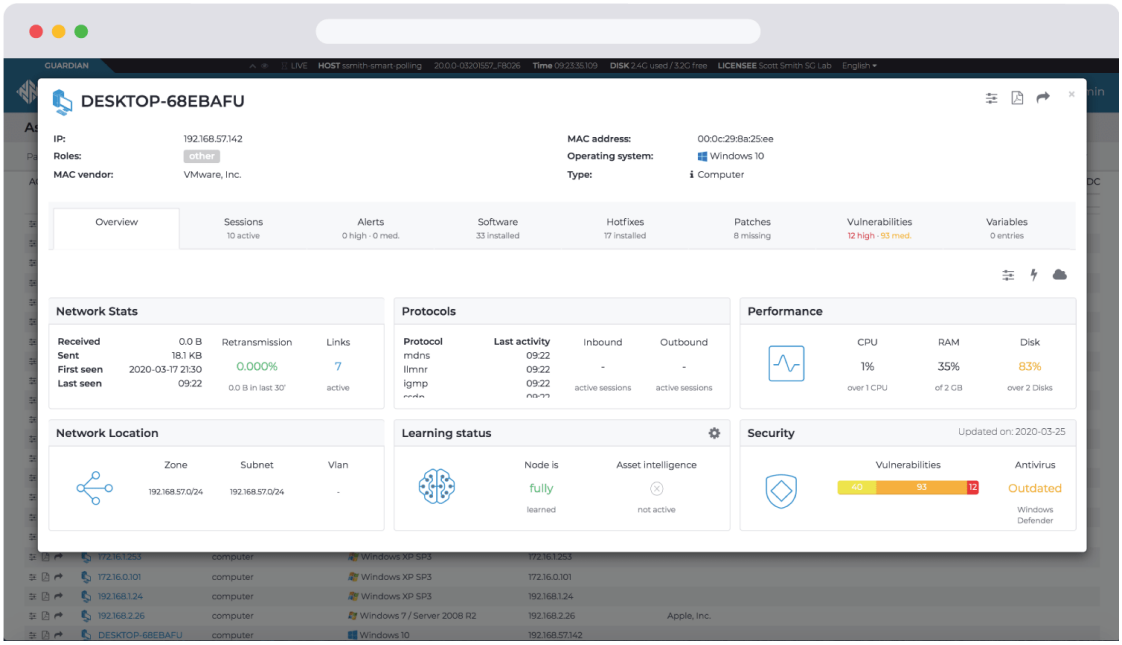

Figure 8. *Nozomi Guardian single asset view. [51]*

3.3.5 Passive detection shortcomings

Even though a well-configured passive detection system is able to maintain a real-time inventory of devices, applications and services in a network relatively well, it can only detect ones that are active in the network. Silent, passive devices might therefore be able to evade detection. Malicious devices and applications might be configured to stay silent until certain time has passed or until they are triggered by an outside signal. Such dormant devices would thus remain unknown to the environment, and to the asset detection application, until they introduce themselves. Additionally, passive detection might not detect devices, even authorized ones, that are active but do naturally not produce much traffic to the network. Such device could be for example a sensor that only transmits alarms under certain circumstances. [40]

Additionally, passive detection can only acquire data from the natural traffic flow in the network, and it is likely that some required piece of data might not be visible in the traffic. In some scenarios it might be possible to parse the required data from other traffic, but that is always not the case. In such situations the asset detection results would be incomplete, leaving the asset inventory data and vulnerability detection capabilities imperfect as well.

As the detected devices need to first produce traffic for the passive detection appliance to notice them, it takes a significant amount of time to collect a complete set of data from a defined set of devices. In general, a passive detection appliance can therefore be called slow regarding this task, definitely slower than an active scanner.

3.4 Active scanning

In active scanning, an automated or semi-automated scanning appliance actively interacts with devices in the target network, often by sending requests to all possible IP addresses within a target scope. The object is often to map all hosts in the target network, while also gathering additional data, such as open ports and version systems to identify security vulnerabilities. [40]

3.4.1 Network scanning

The first step of active network reconnaissance, regarding both network asset discovery and network vulnerability assessment, is to scan the network for connected hosts. A network scan usually tries to ping every possible IP address within a defined scope. A typical tool used for this task is Nmap. Nmap is a free, open-source product that was originally designed for scanning large networks but works just as well for small ones or even single hosts. Nmap has reached a dominant status as the go-to tool for host discovery and is commonly used by both network administrators and hackers.

While Nmap is the most common network scanner, others have reached better results in certain performance metrics. For example, the open-source Masscan scanner has been found capable of scanning the entire global internet in a matter of minutes, while such task would take Nmap several weeks. [52]

3.4.2 Port scanning and service enumeration

After mapping active hosts within the network, a common next step is to do a port scan, usually a transmission control protocol (TCP) port scan, to discover open ports in the previously discovered active hosts. Open ports can be corresponded to services that usually run on those ports. These services may, due to unsecure design or configuration, be vulnerable to attacks. Enumerating the used services is a core task when determining the overall attack surface of the target system. Additionally, service enumeration tools, such as Amap can be used ensure which application or service is running on a specific port. [53]

For example, older versions of Server Message Block (SMB) communication protocol, which uses port 445, are vulnerable to the WannaCry ransomware that spread rapidly in the year 2017. A scan finding this port open should alert cybersecurity personnel to investigate what services run on that port and ensure only end-of-life versions of the SMB are in use. Alternatively, if no service or protocol is found to actually be using the port, traffic through it should be blocked. [54, 55]

TCP port scanning can further be divided into different approaches. The two most common ones are a TCP scan, a SYN scan, and a zombie scan. TCP scan, or a connect scan, maps the network IP addresses by attempting to complete a common three-way handshake, used to establish a TCP connection, with each target. A completed handshake is interpreted by the scanner as an open port on the host. A SYN scan, or a stealth scan, works in a similar fashion. It does not however include transmitting the last ACK packet back to the target. Some logging solutions only register fully established connections, meaning this approach would not leave any evidence of the scan on the logs. The diagram below (Figure 9) presents the three-way handshake, which is used in the prementioned approaches. [32]

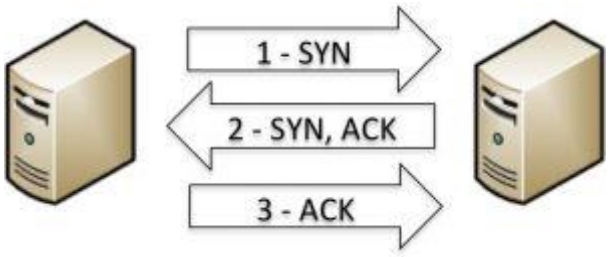

Figure 9. *Illustration of the three-way handshake. [56]*

3.4.3 Vulnerability scanning

The third step of network reconnaissance is performing a vulnerability scan. The purpose of the scan is to identify security weaknesses and vulnerabilities in the target system that could then be used for penetration testing and hacking purposes.

There are many automated vulnerability scanning tools available, both commercial and free. Some of the more common tools include the commercial Tenable Nessus and the open-source Greenbone Open Vulnerability Assessment System (OpenVAS), originally a fork of the Nessus scanner [57]. These vulnerability scanners use libraries of known vulnerabilities to automatically map possible security risks in the scan targets. Figure 10 shows an example of a Nessus vulnerability report, rating the found vulnerabilities from low to critical based on their CVE. For Nessus, newly found vulnerabilities are continuously incorporated to the scanning with *plug-ins* that contain an algorithm to test for the presence of the vulnerability, as well as generic information regarding the vulnerability and how to remediate it [58]. The plug-in algorithms might be quite simple, for example simply trying common credential combinations for any login interface in the system to discover the usage of weak or default credentials. The vulnerabilities to be found through scanning might also include:

- Unpatched, out-of-date, and end-of-life components, operating systems
- Vulnerable software
- Vulnerable encryption ciphers
- Vulnerable algorithms [57, 30]

As scanning the whole network with such a scanner would be overly time consuming, the scan is usually targeted at certain hosts and ports. Prior host discovery and port scan results are used as input for the vulnerability scan.

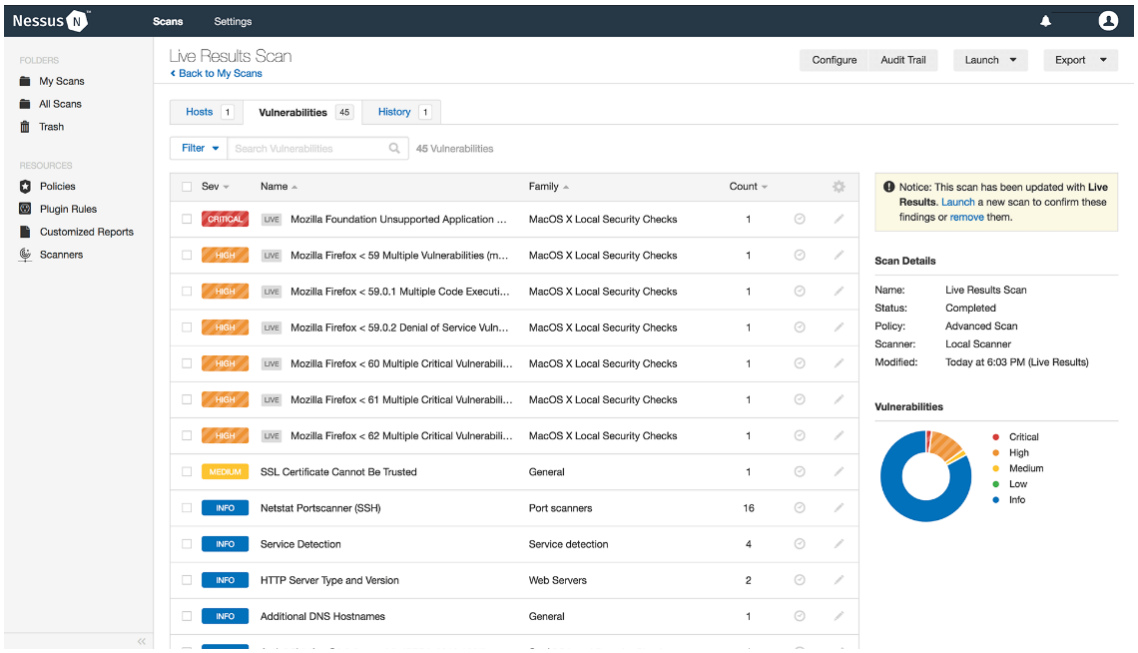

Figure 10. *Nessus vulnerability report. [59]*

Vulnerability scanning can be categorized in certain ways. It is relevant to define whether the scan is authenticated or unauthenticated, network-based, or agent-based. To get the best and most comprehensive results in a vulnerability scan, it is recommended to perform an authenticated scan. In a significantly large network, an authenticated scan can however be troublesome, as the variety in different types of targets and authentication methods grows larger. Authenticated scanning might also require changes in firewall rules. For example, with Windows machines, TCP ports 139 and 445 need to be open for an authenticated scan to be possible. In an automation network the scan is also generally network based. An agent-based scan would require an agent to be installed on the target of the scan, which is not possible for the majority of smaller devices, especially layer 0 devices. [60]

3.4.4 Active scanning shortcomings

Active scanning, as described in the previous subchapters, can unfortunately easily cause problems in active automation systems. The queries sent by the scanning tool might not be compatible with the devices being scanned, causing erroneous behaviour, especially if the device is not properly designed to handle unexpected input. Even if the scanned device is compatible to be scanned, an active scan can cause delay in the normal functions of the device, as the scan can generate a significant amount of traffic. Extensive delays in the network can also lead to scanners considering ports blocked, if the scan time passes the set timeout duration, resulting in an inaccurate scan.

Additionally, the network being scanned might not have the bandwidth to handle the traffic generated by the scanning at all, causing the whole network to stall, which can cause other critical damage, even to the physical environment. In a recent paper published at the 2021 International Symposium on Computer Science and Intelligent Controls (ISCSIC) [61], active scanning was performed on a simple, 3 layered automation system. In one experimental case, a certain Nmap scan resulted in an 80ms delay on the network, which eventually caused an engine failure. Another common cause for devices to crash are address resolution protocol (ARP) queries, often used in active discovery [62].

Because of these issues, a traditional active scan cannot typically be performed against active automation systems. Such scans can only be performed during maintenance breaks or other production stoppages. This can leave temporary devices within the network undetected by the scanner, meaning a real-time asset inventory and network monitoring cannot be achieved with tools such as Nmap.

3.5 Conventional best practices

Marksteiner et al. divide their black-box network reconnaissance procedure into three distinct main phases, as presented in Figure 11 below. The first phase consists of passive detection modules gathering information from the network traffic. The second phase consists of an analyzer module processing the results from the passive phase, and the final phase consists of active scanning. This approach as whole is a common one within the field. [63]

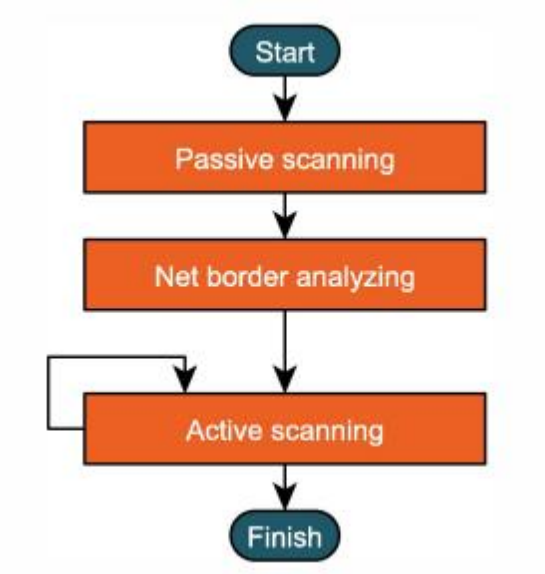

Figure 11. *Three phased network reconnaissance procedure. [63]*

As passive detection has proved to provide significant amount of information about a network with good real-time capabilities, a common best practice is to deploy passive detection to all levels of the target system. This means everything from layer 0 sensors and IO modules to the layer 4 ERP and SAP systems would be monitored by passive sensors. [42]

As passive detection cannot reveal every detail required for a comprehensive security analysis of the network and its devices, active scanning is usually needed. As traditional active scanners, such as Nmap, are deservingly considered too reckless to be used in active automation network environments, causing network congestion and other problems, active scanning has usually been performed only during maintenance breaks or other production stoppages, while the system itself is inactive. It is recommended to have a constant schedule for active scanning to ensure it is performed at an adequate frequency. [64]

The collaboration between passive detection and active scanning is both important and unavoidable. While passive detection cannot achieve the results an active scan can, active scanning is also usually reliant on the results of passive detection. Information from passive detection is for example used to add IP addresses to the active scanners “do-not-scan” list, leaving them out of the active scanning scope and making the scanning more efficient. Alternatively, an active scan can be strictly limited to the IP addresses obtained with passive detection. [60]

Although the sample size is quite small, the tests carried out by *Marksteiner et al.* show the huge benefit of adding active scanning on top of passive methods, as the number of

discovered hosts multiplies as a result. It also shows the significance of the passive detection phase results as an input to the active phase, as dozens of devices are left unscanned by the active scanner when the passive methods have failed to identify certain sub-networks completely. [63]

4. EXISTING COMMERCIAL SOLUTIONS

This chapter discusses existing commercial solutions for asset discovery and vulnerability identification in an automation network with active scanning features. The optimal tool would be able to achieve vulnerability identification and asset inventory results similar to that which tools like Nmap and Nessus can achieve, without disturbing the production state automation network and devices' normal functions.

4.1 Nozomi Smart Polling

Some existing commercial solutions perform active scanning in a reduced volume to avoid congesting the network. One such is Nozomi Smart Polling, an active scanning tool that is considered an add-on to the Nozomi Guardian passive detection tool. Nozomi Guardian is discussed in more detail in Chapter 3.3.4.

Smart Polling performs its active scanning while targeting only selected hosts or devices. With its selected group of targets, smart polling attempts to not perform any unnecessary scanning, thus minimizing emitted traffic and avoiding congesting the network. The limited scope also minimizes the chance of causing unexpected behaviour in the targets, should they not be capable of handling the requests from the scanner. [65]

Nozomi Smart Polling gathers a variety of information regarding the target devices, including operating system versions, firmware, patch levels and installed software. Therefore, Nozomi Smart Polling can also detect EOL components, a major vulnerability, from a production automation environment. The targeted devices are defined from the Nozomi Guardian passive detection results. If passive methods have not revealed enough information to adequately evaluate a device's weaknesses and vulnerabilities, it becomes a target for smart polling. Devices that are considered to be correctly identified already with passive detection can be left out of the scope of Smart Polling. This might however be unwise, as Smart Polling is smart enough to for example overwrite the operating system information if its data is more accurate than the data from passive detection [66].

Nozomi Smart Polling has a selection of *strategies* i.e., scanning methods to be used with different devices. If a device has for example exposed the use of EthernetIP (EIP), a specifically industrial protocol, Smart Polling will use a dedicated *EthernetIP strategy* for the active scanning of that device. The list of supported strategies, as listed in the Nozomi Guardian user manual of 2020, are listed in Table 1. More detailed or technical descriptions of the strategies are not publicly available. [67]

Table 1. Nozomi Smart Polling strategies [67].

Strategy	Description
Ethernet/IP	To be used with devices that support the Ethernet/IP protocol
Modicon Modbus	To be used with Modicon Modbus devices
SEL	To be used with SEL devices
SNMPv1	To be used with devices that expose the SNMPv1 service
SNMPv2	To be used with devices that expose the SNMPv2 service
SNMPv3	To be used with devices that expose the SNMPv3 service
SSH	To be used with devices that expose the SSH service
WinRM	To be used with Windows devices that expose the WinRM service
WMI	To be used with Windows devices that expose the WMI service
CB Defense (External Service)	To be used with Carbon Black services
DNS reverse lookup (External Service)	The strategy extracts information about nodes by using DNS protocol
Aruba ClearPass (ExternalService)	The strategy send and extract assets information from ClearPassthrough HTTP Rest APIs
Cisco ISE (External Service)	This strategy extracts assets information from Cisco ISE using thepxGrid HTTP API
ServiceNow (ExternalService)	This strategy extracts assets information from ServiceNow using theREST Table API. It also allows you to automatically close Guardian's incidents whenever their corresponding incidents in ServiceNow are closed

Nozomi Smart Polling appears to tackle the issues of network congestion quite well while being able to fulfil its task of acquiring device information that passive detection could not acquire. This would especially be true when operating in a network with known bandwidth capabilities, and when the targeted devices' capabilities to handle the scanning is known. The tool also being in wide commercial use would suggest no major problems regarding availability of the target network and devices during scanning exist.

It is worth noting that the Smart Polling list of supported protocols from 2020 was still missing for example Profinet. The 2020 list also includes strategies that were not present in the corresponding 2019 protocol list, further highlighting the constant development in the area [68].

As an add-on to Nozomi Guardian, Nozomi Smart Polling tool's main function is to complement the passive detection results. It is not capable of detecting any devices on its own and does also not contribute to any solution towards detecting rogue devices that have not been detected with passive detection, or any other dormant devices.

4.2 Tenable Active Querying

Tenable's OT solution, Tenable.ot, and specifically its active scanning component, Tenable Active Querying, communicates with target devices using only the device's native communication methods to avoid disrupting the device's normal functions. Because of the rather delicate nature of the Active Querying process, Tenable insists Active Querying is not even considered to be scanning anything, but instead simply *querying.* [69]

Like the general approach presented in Figure 11, Tenable's solution first collects information with passive detection methods. The information gathered from the passive detection is then used to determine the device's "native" language, which will be used to query the device for more detailed information. This information includes a wide variety of details, such as configuration information, firmware versions, user information, backplane information, vulnerabilities, metadata, and other security issues.

Active querying is also able to detect devices that do not actively produce traffic to the network at the time of the scan, but that have been communicating with a network switch. According to a webinar related to an early version of Tenable.ot, hosted by Tenable and Indegy prior to Tenable's purchase of Indegy, titled *Tenable and Indegy: the First Unified, Risk-Based Platform for IT and OT Security (APAC),* this done by interrogating network switches ARP tables to map out the communication paths of those devices. [70]

Tenable.ot has a major focus on detecting changes in devices and their configurations and it keeps track of all such alterations, whether they are made over the network or directly onto the device. These changes are analyzed by the product and alerts are raised should there be any security issues. Tenable.ot utilizes plug-ins similar to those of Tenable Nessus vulnerability scanner, to identify vulnerabilities [71]. Thus, it is safe to say it also has rather well-developed vulnerability identification capabilities regarding information acquired via both passive and active methods.

Forrester's Industrial Control Systems (ICS) Security Solutions ranking of Q4 2021 also gave Tenable full points for vulnerability risk management for OT, supporting this statement [72]. Although the scope of Forrester's ranking is not limited to simply a certain product, like Tenable.ot, but companies as a whole, and does not consider the products capabilities from the same angle as this thesis, but from a rather business oriented point of view, it still manages to provide a good general sense of their OT-tailored vulnerability risk management capabilities.

4.3 Claroty Active Querying and AppDB

Claroty has also decided to name their active discovery approach as Active Querying, and it works much the same way as Tenable's solution. The queries to the system components are made in such protocols that the query is indistinguishable from regular network traffic and appears the same as a regular request from for example an engineering workstation to the component, minimizing the chance of causing disruptions to the device's normal functions. [73]

Like other asset discovery solutions presented here, Claroty also provides a passive detection tool based on SPAN port mirroring to be used in cooperation with the active tool. Additionally, Claroty AppDB tool uses the backup and restore configuration files for industrial devices to identify devices that are left undetected by other passive and active methods. This does not only include silent, rarely actively communicating devices, but also air-gapped devices that would otherwise be outside of the scanners reach. [73, 74]

Out of the existing active scanning products investigated for this thesis, Claroty Active Querying is the only one with the supported protocols list available [75]. The list is likely outdated, as it dates back to July 2019. More recent list is not available on open sources. Claroty also lists 26 types of controllers from different manufacturers that are supported for AppDB. It is worth noting the provided list is directly from the product vendor and should be at least partly interpreted as marketing material. The list of supported ICS and IT protocols for active querying consists of the following:

- BACnet
- Beckhoff
- CIP
- Cisco Profile
- DNP3
- ENIP Scan/Query
- Hirschman Discover Scan/Query
- Hirschman Profile
- HTTP Query
- IoT Query
- Modbus Object Information
- MS Net Bios
- Net Bios
- Ping Sweep
- Profinet – DCP Scan/Query
- R&B Profile/Query
- Rockwell Profile
- S7comm
- Schneider Unity Query
- Siemens Profile
- Siprotec 5
- SNMP Scan/Query
- SNMP Siprotec 5
- TCP Port Scan
- Telnet
- Windows Profile
- WMI
- WSD Discovery/Query

Claroty's active scanning solutions appear remarkably similar to other ones presented in this chapter. However, the usage of backup data to identify additional devices widens the asset discovery scope a little bit further. This technique does also not appear to pose the risk of causing disruptions in the network, as the backup data is instead directly shared with AppDB for parsing. However, if the backups are not refreshed regularly, the bad quality of the backup data, i.e., its old age, might lead to incorrect vulnerability assessment on the device.

While the process for the AppDB tool to acquire the backup information is an active action, it does not technically qualify as actively scanning the devices, as it does not even require a connection to the examined device to be formed. Claroty themselves divide their solutions into three aspects: passive, active (querying), and AppDB, thus refusing to put AppDB into either the passive or active categories. Regardless of the classification, the AppDB approach is still an interesting one for the regards of this thesis.

4.4 Cisco Cyber Vision Active Discovery

Cisco's asset discovery solution is focused on industrial control systems (ICS), and it only supports three protocols: Ethernet/IP (Rockwell devices), Profinet, and Siemens S7 Discovery. Even though the scope of the protocols is rather limited, they do cover a

relatively significant number of automation devices, as these protocols are all automation specific. [76]

The cooperation of passive and active components is at the core of the Cisco asset discovery approach as well. First, the passive detection informs the active detection component of the detected protocols active in the network. Then, the active component broadcasts a hello request in a specific ICS protocol, while the passive discovery component captures and decodes the responses from the devices, utilizing deep packet inspection.

Cisco Active Discovery is, out of the tools examined in this thesis, the only one that does actual active scanning. The collected information for example for a Profinet multicast scan is however limited to IP address, subnet mask, manufacturer name and the name of the station.

The Cisco solution does not utilize SPAN ports for network traffic flow monitoring, and thus does not require the installation of further SPAN network. Rather, it uses Cisco Cyber Vision sensors that are embedded in certain Cisco equipment:

- Cisco IC3000 Industrial Compute Gateway
- Cisco Catalyst® IE3300 Rugged Series switch
- Cisco Catalyst IE3400 Rugged Series switch
- Cisco Catalyst IE3400 Heavy Duty Series switch
- Cisco Catalyst IR1100 Rugged Series Routers
- Cisco Catalyst IR8300 Rugged Series Router
- Cisco Catalyst 9300 Series switch
- Cisco Catalyst 9400 Series switch

However, the solution requires strictly these devices to function. Thus, in the case of network segments without any of these devices on its edge, one of them needs to be installed. [61, 77]

The Cisco solutions lacks scalability due to the limited scope of applicable protocols, as well as the requirement of certain switches to be used for the solution to function. However, in an automation system that already utilizes said Cisco equipment and where the traffic is limited to the supported protocols, the solution appears to be applicable. However, it does not offer any other innovative solutions for the active scanning of an active

automation network. Additionally, the Cisco Active Discovery solution's abilities to scan the larger IP address space of an IPv6 network need more studies.

4.5 Dragos Platform

Dragos Platform OT solution, much like other solutions presented in this chapter, utilizes SPAN ports for port mirroring, and deep packet inspection for analyzing the traffic flow. The Dragos OT solution supports devices and protocols from 15 different vendors, covering a rather large number of devices. [78, 79]

With the so called ruggerized passive sensors, developed in cooperation with Schweitzer Engineering Labs, Dragos has a significant position in the market. However, Dragos does not provide an active scanning dimension in its product portfolio, instead having an increased focus on providing incident response playbooks and threat intelligence driven analysis services.

4.6 Microsoft Defender for IoT and Selective Probing

Microsoft's Windows Defender for IoT also offers both passive and active asset discovery. Much like other solutions presented in this chapter, Defender for IoT utilizes the switches' SPAN ports for port mirroring to analyze the network traffic flow. It can also identify over 100 IoT, OT, ICS, and SCADA protocols, covering a very large number of devices for passive asset discovery. [80]

Defender for IoT also has an active scanning solution that is alternatively called *Selective Probing*. Much like Tenable.ot, Selective Probing uses native vendor-approved queries to acquire information from OT devices, thus minimizing the possibility of causing disruptions to the device's normal functions. [81]

The Microsoft product appears to have very good scope regarding passive asset detection with a long list of supported identifiable protocols. The active discovery options also take into consideration the limitations the production environment sets. However, there is very limited documentation available regarding Microsoft's Selective Probing, and evaluating its capabilities from open sources is rather difficult.

5. NEW SOLUTIONS AND EMERGING TECHNOLOGIES

This chapter reviews recent studies that could help solve the issues regarding active scanning of a production state automation environment, as discussed in Subchapter 3.4.4.

5.1 UDP-Based Active Scan for IoT Security (UAIS)

As an alternative to traditional TCP scanning methods, UDP based scans have also been studied. *Jung et al.* present a novel method for scanning IoT devices in their paper regarding UDP-Based Active Scan for IoT Security (UAIS). [82]

The method identifies IoT devices using Universal Plug and Play (UPnP) protocols Simple Service Discovery Protocol (SSDP), Multicast Domain Name System (MDNS) and NetBios Name Server (NBNS), using UDP as the transport protocol. These protocols were picked for the study, as they, according to *Jung et al.*, are the most common UDP-based protocols used by IoT devices. All 50 devices used in testing the UAIS algorithm were identified with these 3 protocols.

The UAIS algorithm consists of 2 separate scans: primary scan and auxiliary scan. The primary scan uses SSDP through unicast to request information about the device. If there is no response or the algorithm is not otherwise able to parse a device type from it, the auxiliary scan using NBNS and MDNS is performed.

In general, UDP packets are more simple than equivalent TCP packets, resulting in a more lightweight scan. This also means that not all information regarding a device is transmitted. UAIS algorithm mitigates this issue by refining received packets according to known IoT device classification. *Jung et al.* argue this method is more efficient and accurate in determining IoT device types. According to their tests, the method is as much as 1524 times faster than Nmap, while providing accurate results (Figure 12). For instance, for IP cameras, the average elapsed time with Nmap was 138,64 seconds and with UAIS 0,12 seconds.

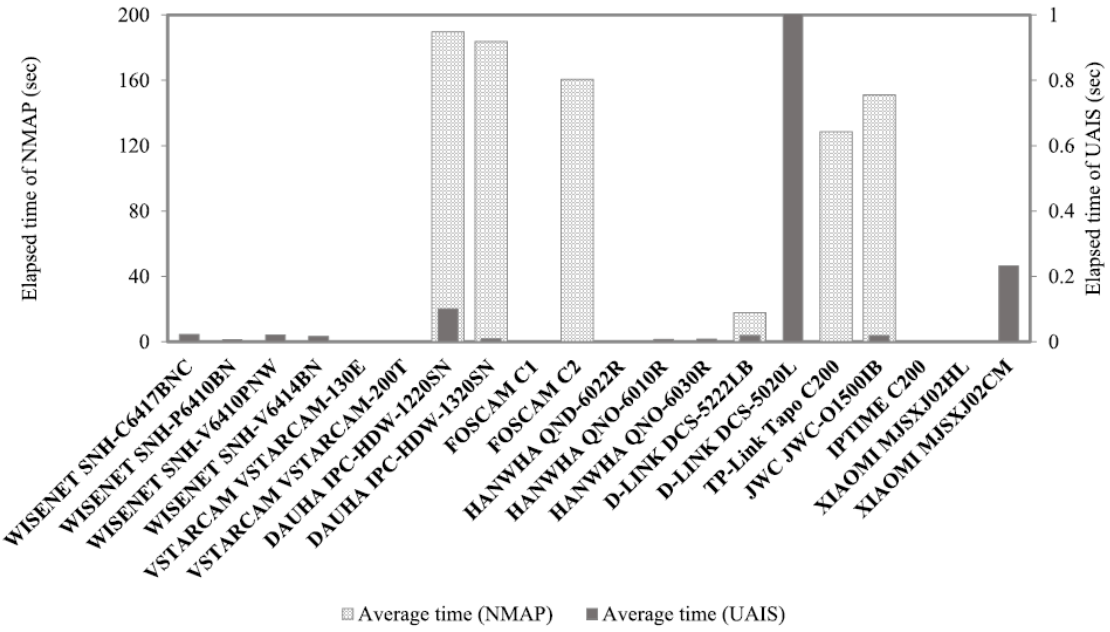

Figure 12. *UAIS and Nmap scan time comparison. [82]*

Such difference in the scan time may be significant, especially for remarkably large networks. Thus, this kind of approach would appear to be able to provide a more snapshot-like status of the target system. However, while this method is more lightweight and appears to be less stressful to the network, it also does not appear to be suitable for the scanning of an active industrial system, as it still provides a significant amount of network traffic. This should however be studied further, as the paper itself does not discuss the problem of congesting the network. Nevertheless, the method could already be utilized in traditional active scanning during production pauses, assuming the mentioned protocols are indeed found in the target network.

The paper also acknowledges a wide variety of different types of IoT devices, but only three types of devices, Access Points (AP), IP cameras, and Network Attached Storage (NAS) were used in the conducted experiment. Thus, the applicability of the UAIS method, and especially the used protocols, should be further studied in the context of different types of devices, especially more primitive ones, like sensors. Especially, the applicability of the method with industrial devices and networks also still needs to be studied further.

5.2 Modified passive available bandwidth estimation (MPABE)

The congestion problem can, with current technology, be solved by accurately defining the available bandwidth in the target network. With accurate data on the available bandwidth, scanners can, when needed, transmit the probe packets with a limited frequency to avoid congesting the network. Much like asset detection itself, bandwidth reconnaissance can be divided into passive and active techniques. *Bandung et al.* propose a mathematical model, called Modified Passive Available Bandwidth Estimation (MPABE), to estimate the available bandwidth of a network [83].

The mathematical model that makes up MPABE has four main variables, which are the proportion of bandwidth used by the waiting time and ACK, the proportion of bandwidth used by the ACK mechanism, the successful packet transmission probability, and the idle period synchronisation of the sender and receiver.

Bandung et al. also put a lot of focus on comparing MPABE with previous work related to the topic. The previous models include, for instance, Distributed Lagrange Interpolation Available Bandwidth Estimation (DLIABE) (Chaudhari & Biradar, 2014) [84], Accurate Passive Bandwidth Estimation (APBE) (Park & Roh, 2010) [85], and Passive Available Bandwidth Estimation (PABE) (Rizal & Bandung, 2017) [86].

The experiments carried out by *Bandung et al.* show that the model was successful in estimating the available bandwidth in the targeted WLAN networks. It was also measured to be significantly more accurate than related models developed earlier. [83]

The improvements in defining the available bandwidth within a network, as seen by the improved results for MPABE in comparison to previous models, have been stellar. There is still work to be done though, as there is still a significant margin of error in the experimental results the paper presents. Additionally, the applicability of this method in an industrial automation network needs more studying. The implementation of such a solution could however improve the prospects of using traditional, Nmap type active scanners in production state automation networks.

5.3 Delay-Based Scanning

Hashida et al. present an active scanning method, which already takes into account the bandwidth of the network. In the so-called delay-based scan, the scan rate is optimized by running a scan at the highest possible, continuously adjusted rate, while avoiding congesting the target network. In the scenario presented in the paper, a scanning server adjusts the scanning rate, i.e., the number of probe packets sent per time unit, while the

devices being scanned are located in a WLAN network, which is connected to the internet. The broad objectives of the method are presented in Figure 13. If the scan rate is considered to be too high for the network, meaning congesting it, the scan rate is lowered. If the scan rate is deemed to be lower than the available bandwidth, the scan rate is raised. The results of the experiments conducted for the paper are promising, and as a conclusion, *Hashida et al.* conclude that their method is more efficient than more conventional scanning methods. The conducted experiments utilized SYN scanning. [87]

The method consists of two mathematical models, which are used to optimize the scan rate. These are the IoT data throughput model and the scanning delay model. The IoT data throughput model is used to describe the impact of the scanning traffic to the IoT network's data throughput, while the scanning delay model is used to express relationship between the scan rate and the scanning packet's measured delay time.

The method considers several parameters, including packet transmission and arrival probability, length of scanning packet, mean length of IoT data packet, response rates, the service time in saturated conditions where data transmissions happen at maximum capacity, and mean service time, to evaluate the rate of transmitted packets (throughput) related to the scan rate. The model considers both uplink (device to AP) and downlink (AP to device) traffic.

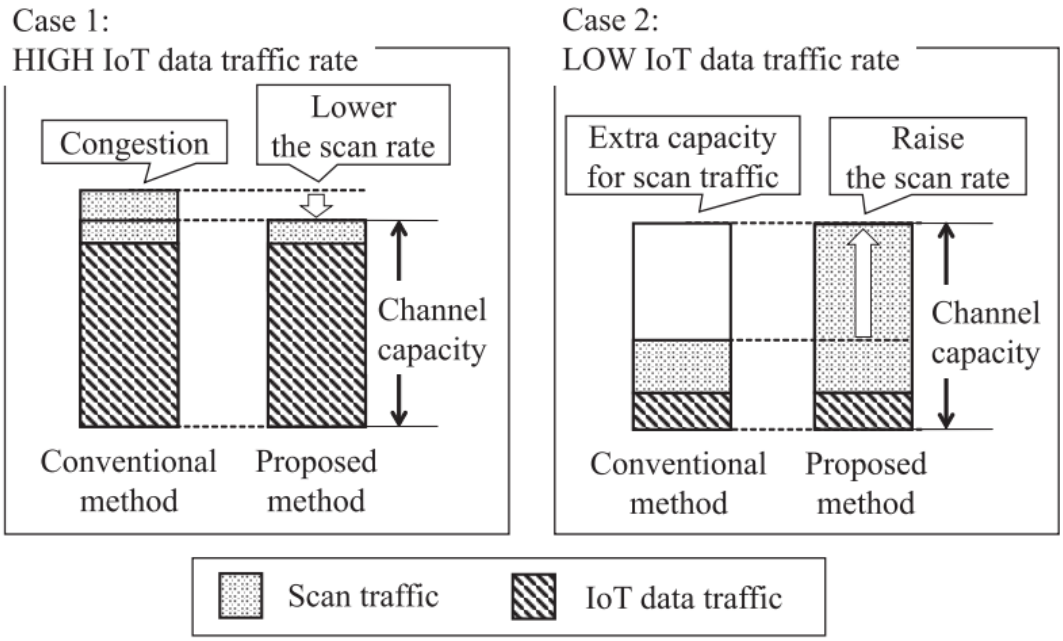

Figure 13. *Illustration comparing delay-based scan and a conventional scan. [87]*

The way the presented mathematical models calculate the optimal rate, allegedly, in real-time, makes the method worth looking into. While the limited testing results provided in the paper do not yet guarantee a completely congestion free active scanning, the model's apparent ability to proactively adjust the scan rate accordingly is promising, compared to for example an Nmap scan, which, with default parameters, instead increases the scan rate, when responses are not received in time [88].

It is worth noting the proposed solution is focused on devices connected to the internet via WLAN, and not a closed automation environment. Therefore, the mathematical model's applicability to an ICS environment remains unknown and needs to be studied and experimented further to gain more information on the issue.

6. RESEARCH RESULTS AND FUTURE CONSIDERATIONS

This chapter summarizes the studied existing products and emerging technologies, highlights their abilities to solve the main problems regarding active scanning of production state automation systems. Topics for required future studies are also discussed.

6.1 Discovery of active devices

All the examined existing commercial solutions utilize passive detection methods as the core component for asset discovery and inventory. The cooperation between passive and active scanning in these products is remarkably similar to how it was described already in Subchapter 3.5. All the products use SPAN ports for port mirroring, expect for the Cisco product, which requires specific Cisco switches for passive detection.

A common unifying factor with the existing commercial active querying tools, excluding Cisco's product, is the usage of native communication protocols to interact with the target devices in order to avoid causing the devices to function erroneously. The correct protocols are also always identified from the passive detection results. The existing commercial active querying products claim to be able to obtain various types of information from the scanned devices, including operating system, firmware, patch levels, installed software, configuration information, user information and backplane information, depending on the target device.

The available information regarding the supported protocols for the queries these active tools use is limited. However, Microsoft's listing of protocols identifiable by Defender for IoT does cover a large number of protocols, including also automation specific ones, such as Profinet, Omron FINS and Emerson OpenBSI. However, for example Tenable's listing of protocols supported for active querying is rather limited, lacking for example the prementioned three protocols. It is also worth mentioning the provided lists are directly from the product vendors themselves and should be at least partly interpreted as marketing material.

Even if none of the mentioned products are currently able to both identify all relevant protocols and use them to communicate with the targeted automation devices, considering the continuous development in the area they should be able to do it eventually. The remaining study subjects and future developments in this area would be to ensure that indeed all major protocols are within the querying or active scanning portfolio, and then

move on to more rare and obscure protocols. An additional topic for further research would be to look into the IPv6 compatibility of all the active querying approaches, as the reviewed documentation does not really cover this topic. For passive detection, IPv6 is already supported to some extent [66].

6.2 Discovery of silent devices

Most of the existing commercial products do not focus on the issue of discovering silent or dormant devices that might not show up on passive detection results. Instead, the listed active scanning appliances Nozomi Smart Polling, Tenable active querying, Claroty Active Querying and Microsoft's Selective Probing are only capable of interacting with devices that have already been discovered.

An exception is the Cisco Active Discovery tool, which is the only one of these tools that performs an actual scan to the network. The supported protocols, as well as the products capabilities are listed rather clearly. The list of supported protocols is short, yet it covers a very relevant group of devices, and also includes the prementioned Profinet, which was missing from Tenable's list. The information Cisco's product is able to obtain is however rather limited, excluding for example OS detection. The Cisco solution appears to be aimed mainly at networks that have a very specific set of devices that use the specified protocols. The applicability of probing the entire network consisting of a more heterogenous group of devices, even when using these automation specific protocols, should however be studied further. An additional topic for future research would be to find ways to add more protocols to the scope of this technique, as well as obtaining more information from the scanned devices.

Tenable active querying has the capability to review network switches' ARP tables to gather information regarding the communication paths to figure out which devices are connected to which switch. This solution widens the extent of the asset discovery range while not disturbing the scanned devices themselves. Interrogating the ARP tables does therefore qualify as a valid partial solution for the issues of active scanning of a production state automation environment. It is however difficult to tell how much Tenable's ARP table interrogation technique helps the issue due to the limited sources and available documentation regarding it.

Due to the limitations on the existing products, the only way to safely gather an all-inclusive asset inventory without gaps would appear to be a conventional active scan while the automation environment is not in production state. This of course does not solve the research questions of this thesis regarding the active scanning of a production

environment. Solutions for discovering certain devices that have not been detected by passive detection methods do however exist.

Claroty's AppDB solution provides another additional tool for discovering devices not detected by passive methods. AppDB interrogates the devices' backup and restoration files to discover information about the backed-up devices. This is done without interacting with said devices, as AppDB does indeed not need any kind of connection to the target devices themselves, thus avoiding disturbing their normal functions. The usage of backup data to discover devices does therefore qualify as a valid partial solution for the issues of active scanning of a production state automation environment. Even though it requires the backup data to be specifically provided to it, meaning the target device's existence is always already known, it does provide additional visibility to the device's configuration. It is however difficult to tell how much this technique helps the issue due to the limited sources and available documentation regarding it.

6.3 Avoiding congestion

The current commercial products' active querying solutions produce a rather limited amount of traffic to the network. The bandwidth requirements for these limited scope queries are small and the vendors appear to have taken the congestion issue into consideration appropriately. As the conventional scanners like Nmap are taken out of the equation, congestion does not appear to be a major problem at the moment. However, future developments still unknown might lead to a demand for a larger scan volume. Also, the bandwidth requirements of Cisco Cyber Vision Active Discovery might cause issues. For such scenarios, the studies reviewed in Chapter 5 might provide interesting development paths.

Modified passive available bandwidth estimation (MPABE) studied by *Bandung et al.* presented an approach for estimating the bandwidth within a network. The study does not provide any experimental results regarding specifically industrial networks, and the applicability of this mathematical model in such a network needs to be studied further. Additionally, the presented experimental results are not comprehensive, and have a rather large margin of error. Regardless, this kind of a technique could indeed be useful in an industrial automation environment as well.

The delay-based scan discussed in 5.3 is also an interesting development topic in the area. For this technique, more studies will also need to be conducted regarding its applicability to an industrial automation environment. Just like MPABE, a delay-based scan

in an industrial automation network might be useful in the future, should for example the required scan rate increase from the growing number of devices.

However, would this solution proof to be applicable for an industrial automation environment, its usefulness with current active querying should also be looked into. The objective could be to integrate delay-based scanning into a current active querying solution to further confirm the queries do not congest the network and to adjust the querying or scan rate if needed. This could also be complemented by the prementioned bandwidth estimation (MPABE) to further optimize the querying or scan rates.

UDP-based active scan for IoT Security (UAIS), discussed in Subchapter 5.1, would provide a lighter scan compared to conventional TCP scanning, but also requires further studies to be conducted. Especially the applicability of the used protocols UPnP, SSDP, MDNS and NBNS for such scans in an industrial network needs to be looked into. If they are deemed too reckless, others need to be considered instead. Some automation specific protocols, such as Omron FINS, uses UDP, so a UDP based scan might indeed prove to provide some additional value for industrial automation environments.

Additionally, the usefulness of UAIS regarding active scanning during production breaks might be a worthy topic for future study, as UAIS is significantly faster than for example Nmap. It is possible that UAIS could be applicable for this purpose already. Even if UAIS would not be able to detect all devices, its results could be used to at least shorten the Nmap scan time by removing devices discovered by UAIS from the Nmap scan scope. This of course does not contribute the issues with active scanning of a production automation environment, should the usage of Nmap be out of question.

6.4 Summary

As active scanning still cannot provide a comprehensive asset inventory and vulnerability identification capabilities on its own, passive detection is still a core tool for these objectives. Passive detection results are commonly further used as the base for active asset discovery, and active tools attempt to obtain relevant information missed by the passive tools. Such approach should be utilized in the future as well. Current passive detection capabilities appear to be rather well optimized, and no major developments paths are apparent. However, the accuracy of passive detection could possibly be further developed and fine-tuned, for example by investigating the industrial automation applicability of approaches, such as the fingerprinting taxonomy for IoT devices presented by *Xu et al.*

Cisco Cyber Vision Active Discovery was the only product looked at in this thesis that performed actual active, broadcast and multicast scans. For now, regarding asset discovery and vulnerability identification, this would be the starting point for a state-of-the-art active scanning for environments that have devices using Ethernet/IP, Siemens S7 or Profinet protocols. For remaining devices, querying approaches using devices' native protocols, like Nozomi Smart Polling or Tenable Active Querying, are needed. The next step for these active discovery methods should be to implement more and more protocols used by industrial devices to their repertoire.

A technique for interrogating network switches' ARP tables could be utilized for additional visibility to the target network, as well as the parsing of information from any available device backup data. Device databases should also be utilized for maximum device identification accuracy, as well as ensuring only suitable devices are introduced to the environment.

Once all detected devices have been accurately identified, a harsher active scan could be performed on the remaining IP addresses to detect any rogue devices, given that there is enough network bandwidth available for such a task. Regarding the estimation of available bandwidth, as well as optimizing scan rates, more studies are needed.

With all possible data regarding the devices collected, vulnerabilities can be identified and assessed from it. The current products have quite comprehensive capabilities regarding vulnerability identification. A good example is Tenable.ot, which uses plug-ins, similar to those associated with Tenable Nessus, for vulnerability identification. Device databases such as Armis Device Knowledgebase can also be utilized to identify vulnerable devices. Additionally, more research is needed regarding the industrial compatibility of approaches such as IoT Sentinel and Dïot, presented by *Miettinen et al.*

7. PROPOSED SET-UP

This chapter presents the best possible set-up for security scanning of a production state industrial automation network based on the solutions studied in this thesis.

7.1 Objectives

The optimal solution would be able to achieve vulnerability identification and asset inventory results similar to that which active scanning tools like Nmap and Nessus scanner can achieve, without disturbing the production network and devices' normal functions. These normal functions might be disturbed, as discussed in Subchapter 3.4.4, by congesting the network by eating up the network bandwidth or causing a denial-of-service state on individual devices by querying them with requests they cannot handle or by bombing them with too many requests.

Passive detection methods are already common in industrial environments. They however have limited capabilities and can also not achieve the results that conventional active scanners can. An alternative point of view is to seek a solution that can obtain relevant information that passive detection methods, as discussed in Subchapter 3.3.4, cannot, i.e., a solution that has the ability to discover dormant, silent or rogue devices that might not be discovered with passive methods. The current products on the market do not unambiguously achieve these goals.

7.2 Optimal set-up with current technology

The active querying solutions require a list of IP addresses of the known devices in the network to function properly. Such list should be obtained by passive detection methods through an extended period of time, and for best visibility to the network be complemented by a conventional security scan, such as an Nmap scan, during stoppages within the production environment.

To combat the shortcomings of passive detection, and to gain the best possible visibility to the network, active scanning of a production environment is also needed. In a perfect environment all used devices would be capable of handling thorough security probing even when in production state, but as mentioned in 3.4.4, that is usually not the case. Therefore, an active querying application should be customized for each known device according to each device's technical limitations, i.e., their native communication protocols. Usage of for example an active querying product, such as Nozomi Smart Polling,

Tenable Active Querying, or Claroty Active Querying would be recommended. Simultaneously, an active scan like Cisco Cyber Vision Active Discovery should be used to directly map all devices using the limited protocols the product supports. Interrogation of the ARP tables of the network switches should be utilized to gain further visibility to possibly still undetected devices. Additional visibility can also be obtained by parsing information from devices' back-up data, similar to Claroty AppDB.

In addition, a comprehensive device database, such as the Armis Device Knowledgebase [89], should be used as a reference when deciding on the acquisition of new devices to the network, ensuring the new devices are recognized as legitimate products, and that the device's features allow for it to be scanned and monitored properly.

After it is ensured that the IP addresses of all known devices within the network are catalogued, an active scan for discovering rogue and unknown devices could be performed on the remaining IP addresses. Should the bandwidth capabilities of the network allow this sort of harsh scan, the functionality of the known devices would not be disturbed.

Overall, the optimal approach can be laid out in the steps 1-6 listed below. Steps 1-2 together form the so-called conventional approach of passive detection during production and active scanning during production breaks, as laid out in Chapter 3. Steps 3-4 add the recent trend of using the native protocols of the target devices for active detection, as laid out in Chapter 4. Steps 5-6 add additional visibility to any devices still left undetected.

1. Passive detection
2. Conventional active scan, such as Nmap, during production breaks
3. Active querying of the known devices using the native protocols of the devices
4. Cisco Active Discovery
5. ARP tables and backup data interrogation
6. Harsh active scan for still unknown devices

8. CONCLUSION

The objective of this thesis was to determine the capabilities of current and emerging active scanning technologies to achieve vulnerability identification and asset inventory results similar to that which conventional active scanning tools like Nmap and Nessus scanner can achieve, without disturbing the normal functions of the production state network and devices in it.

The approach for achieving this objective was to perform open-source research on the features and technologies used in currently existing commercial products, as well as on any recently conducted scientific studies that aim to solve the issues with active scanning of a production automation environment.

From the conducted research it is safe to conclude that no individual product on the market manages to achieve the prementioned goals. Therefore, to even come close to results that tools like Nmap and Nessus scanner can achieve, multiple techniques and tools need to be used. Thus, the best possible solution with current technology would still include both passive and active methods.

Regarding the passive detection capabilities, the current products are rather similar. Passive detection also appears to be quite optimized for its capabilities, and the current methods achieve their purpose well. For active scanning, there is however work to be done, and the field is developing quickly, which is evident from the products' release notes, as well as the differences in the variance of supported protocols between current products. The development has also caused the products to have some other differences, as the vendors have implemented certain new, innovative ways to expand their scanning scopes, such as Claroty AppDB, and the interrogation of switch ARP tables by Tenable.ot.

The most major development in active scanning has been to utilize the target devices' native communication protocols to query the devices for information. This mitigates the risk of causing erroneous behaviour that could be caused by sending requests that the devices are not able to process. Usually, the querying is performed to singular devices, with the attempt of obtaining additional information regarding devices that had previously been discovered by passive detection. This has now become the default approach in the field.

An exception to the trend is Cisco Cyber Vision Active Discovery, which probes the entire network using certain automation system specific protocols. For Cisco, the supported

protocols list is particularly limited. However, this is the only reviewed active detection product that is capable of discovering devices in a production state environment through an actual active scan, and the only one capable of discovering silent, previously unknown devices in a production state network.

Due to the limited protocols and other differences between the current products, there would be a place for both active querying, such as with Nozomi Smart Polling, and active scanning, such as with Cisco Cyber Vision Active Discovery. The optimal solution for the most comprehensive asset discovery and vulnerability identification set-up would contain both of these methods. Additional visibility to the environment would be provided by the ARP table interrogation and AppDB backup data interrogation techniques. Passive detection would also remain as a foundational core function. Vulnerability detection from the obtained asset information should be performed by using vulnerability plug-ins similar to those of the Nessus vulnerability scanner, as done by Tenable.ot, and by utilizing device databases, such as the Armis device knowledgebase.

For future studies, a relevant topic would be to ensure all relevant protocols are within the scope of both the active querying, and Cisco-like active scanning. Additionally, even though the current solutions do appear to not cause congestion of the network, studies are also needed regarding topics such as UDP-based scanning, bandwidth estimation, and delay-based scanning, and especially their applicability to industrial automation systems, to ensure continuous development of the active scanning methods and to solve issues related to congestion.

It is also worth noting that while current technology might restrict the possibilities for active scanning of a production state automation network, for example regarding traffic delay issues, future developments, such as time-sensitive networking, might create more opportunities for such scans to be suitable in industrial networks.

REFERENCES

[1] CNN, The Log4j security flaw could impact the entire internet. Here's what you should know, 2021. Available (referenced 21.11.2022): https://edition.cnn.com/2021/12/15/tech/log4j-vulnerability/index.html

[2] Reuters, Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed, 2021. Available (referenced 21.11.2022): https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/

[3] Aalto.fi, Kybersota Ukrainassa – mitä on tapahtunut ja mitä on odotettavissa?, 2022. Available (referenced 21.11.2022): https://www.aalto.fi/fi/tapahtumat/kybersota-ukrainassa-mita-on-tapahtunut-ja-mita-on-odotettavissa

[4] Kyberturvallisuuskeskus, Tietoturvasetelin haku aukeaa pian - tutustu tietoturvan kehittämisen tuen ehtoihin ja hakemiseen, 2022. Available (referenced 22.11.2022): https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturvasetelin-haku-aukeaa-pian-tutustu-tietoturvan-kehittamisen-tuen-ehtoihin-ja

[5] Hemsley K, Fisher R. A History of Cyber Incidents and Threats Involving Industrial Control Systems. In: Critical Infrastructure Protection XII. Cham: Springer International Publishing; 2018. p. 215–42.

[6] Popkova EG, Ragulina YV, Bogoviz AV. Industry 4.0: Industrial Revolution of the 21st Century. 1st ed. 2019. Popkova EG, Ragulina YV, Bogoviz AV, editors. Cham: Springer International Publishing; 2019.

[7] Tripwire.com, The IoT Convergence: How IT and OT Can Work Together to Secure the Internet of Things, 2015. Available (referenced 21.11.0222): https://www.tripwire.com/state-of-security/the-iot-convergence-how-it-and-ot-can-work-together-to-secure-the-internet-of-things

[8] NIST, Computer Technology Resource Center Glossary. Available (referenced 21.11.2022): https://csrc.nist.gov/glossary/term/operational_technology

[9] Sekar M. SCADA and Operational Technology. In: Machine Learning for Auditors. Berkeley, CA: Apress; 2022. pp. 131–135.

[10] Boyes H, Hallaq B, Cunningham J, Watson T. The industrial internet of things (IIoT): An analysis framework. Computers in industry. 2018.

[11] Real-Time Innovations Inc, Industrial Internet of Things, RTI FAQ, 2015. Available (referenced 22.11.2022): https://info.rti.com/hubfs/docs/Industrial_IoT_FAQ.pdf

[12] Check Point, Purdue Model for ICS Security. Available (referenced 22.11.2022): https://www.checkpoint.com/cyber-hub/network-security/what-is-industrial-control-systems-ics-security/purdue-model-for-ics-security/

[13] HCL Tech, Five Considerations For A Successful IT/OT Convergence Program. Available (referenced 22.11.2022): https://www.hcltech.com/blogs/five-considerations-successful-itot-convergence-program

[14] B.R. Mehta, Y. Jaganmohan Reddy. Industrial Process Automation Systems. Butterworth-Heinemann; 2014.

[15] IEC, Understanding IEC 62443. Available (referenced 22.11.2022): https://www.iec.ch/blog/understanding-iec-62443

[16] IEC, IEC 62443-3-2 Preview. Available (referenced 22.11.2022): https://webstore.iec.ch/preview/info_iec62443-3-2%7Bed1.0%7Db.pdf

[17] Shaaban AM, Kristen E, Schmittner C. Application of IEC 62443 for IoT Components. In: COMPUTER SAFETY, RELIABILITY, AND SECURITY, SAFECOMP 2018. Cham: Springer International Publishing; 2018. pp. 214–223.

[18] Leander B, Čaušević A, Hansson H. Applicability of the IEC 62443 standard in Industry 4.0 / IIoT. In: 14TH INTERNATIONAL CONFERENCE ON AVAILABILITY, RELIABILITY AND SECURITY (ARES 2019). NEW YORK: ACM; 2019. pp. 1–8.

[19] Messenger JL. Time-Sensitive Networking: An Introduction. IEEE communications standards magazine. 2018;2(2):29–33.

[20] Mouser Electronics, Applications and Technologies, Industrial Ethernet Standards. Available (referenced 13.12.2022): https://www.mouser.fi/applications/industrial_ethernet_standards/

[21] IEEE 802.1 Working Group, Time-Sensitive Networking (TSN) Task Group. Available (referenced 13.12.2022): https://1.ieee802.org/tsn/

[22] Han C, Dongre R. Q&A. What Motivates Cyber-Attackers? Technology innovation management review. 2014; 4(10), 40–42.

[23] OWASP, OWASP IoT Top 10, 2018. Available (referenced 22.11.2022): https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf

[24] Automaatioseura, Teollisuusautomaation tietoturva – Verkottumisen riskit ja niiden hallinta, 2005.

[25] IRTF, Internet of Things (IoT) Security: State of the Art and Challenges, 2019. Available (referenced 22.11.2022): https://www.rfc-editor.org/rfc/rfc8576

[26] Burg A, Chattopadhyay A, Lam KY. Wireless Communication and Security Issues for Cyber-Physical Systems and the Internet-of-Things. Proceedings of the IEEE. 2018;106(1):38–60.

[27] Computer Weekly, Millions of industrial remote controllers open to attack, 2019. Available (referenced 22.11.2022): https://www.computerweekly.com/news/252455894/Millions-of-industrial-remote-controllers-open-to-attack

[28] Security Intelligence, CISA: Industrial Attacks Could Remotely Control Devices, 2022. Available (referenced 22.11.2022): https://securityintelligence.com/news/industrial-control-system-attacks-remote-control-cisa/

[29] Mugarza I, Flores JL, Montero JL. Security issues and software updates management in the industrial internet of things (Iiot) era. Sensors (Basel, Switzerland). 2020;20(24):1–22.

[30] Adryan B, Obermaier. The Technical Foundations of IoT. Norwood: Artech House; 2017. pp 405-407.

[31] U-Blox, IoT device security vs man-in-the-middle attacks, 2022. Available (referenced 22.11.2022): https://www.u-blox.com/en/blogs/insights/iot-device-security-man-in-middle

[32] Sairam J, Rahalkar S. Securing network infrastructure: discover practical network security with Nmap and Nessus 7. 1st edition. Birmingham, 2019.

[33] Cloudflare, What is an on-path attacker?, Available (referenced 22.11.2022): https://www.cloudflare.com/learning/security/threats/on-path-attack/

[34] NIST, Special publication 1800-5, IT Asset Management, 2018. pp 2.

[35] Npcap, Npcap or WinPcap? Available (referenced 22.11.2022): https://npcap.com/vs-winpcap.html

[36] Profinet University, PROFINET Tools – PROFINET Commander. Available (referenced 22.11.2022): https://profinetuniversity.com/profinet-development/profinet-tools-profinet-commander/

[37] Profinet, PROFINET Commander User Manual V5.1.0.8, 2022.

[38] Npcap, npcap.com. Available (referenced 22.11.2022); https://npcap.com/

[39] Nozomi, Nozomi Guardian Sensors, Technical Specifications & Protocols. Available (referenced 22.11.2022): https://www.nozominetworks.com/products/technical-specifications/

[40] Qualys, Qualys Passive Sensor, Deployment Guide, 2022. Available (referenced 22.11.2022): https://www.qualys.com/docs/qualys-network-passive-sensor-deployment-guide.pdf

[41] Techopedia, Dictionary, Port Mirroring. Available (referenced 22.11.2022): https://www.techopedia.com/definition/16134/port-mirroring

[42] Tenable, Passive Monitoring or Active Scanning for Operational Technology Environments, 2018.

[43] Forescout, Device Visibility and Control: Streamlining IT and OT Security with Forescout, 2019.

[44] Github, Python rewrite of passive OS fingerprinting tool Available (referenced 22.11.2022): https://github.com/xnih/satori

[45] Nozomi, Nozomi Networks Deep Packet Inspection S4 2017, 2017.

[46] Garlan Technology, Claroty partner. Available (referenced 22.11.2022): https://www.garlandtechnology.com/claroty

[47] Qiang Xu, Rong Zheng, Saad W, Zhu Han. Device Fingerprinting in Wireless Networks: Challenges and Opportunities. IEEE Communications surveys and tutorials. 2016;18(1):94–104.

[48] Miettinen M, Sadeghi AR, Marchal S, Asokan N, Hafeez I, Tarkoma S. IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT. In: 2017 IEEE 37TH INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING SYSTEMS (ICDCS 2017). LOS ALAMITOS: IEEE; 2017. p. 2177–2184.

[49] Nguyen TD, Marchal S, Miettinen M, Fereidooni H, Asokan N, Sadeghi AR. DÏoT: A Federated Self-learning Anomaly Detection System for IoT. In: 2019 39TH IEEE INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING SYSTEMS (ICDCS 2019). LOS ALAMITOS: IEEE; 2019. p. 756–767.

[50] Nozomi, Nozomi Guardian Data Sheet, 2022. Available (referenced 22.11.2022): https://www.nozominetworks.com/downloads/US/Nozomi-Networks-Guardian-Data-Sheet.pdf

[51] Nozomi, Guardian Sensors. Available (referenced 22.11.2022): https://www.nozominetworks.com/products/guardian/

[52] The Chief I/O, How To Scan the Internet in 5 Minutes. Available (referenced 22.11.2022): https://thechief.io/c/editorial/how-to-scan-the-internet-in-5-minutes/

[53] Ali S, Heriyanto T. BackTrack 4 assuring security by penetration testing : master the art of penetration testing with BackTrack. 1st edition. Birmingham, U.K: Packt Open Source; 2011.

[54] Microsoft, Direct host SMB over TCP/IP, 2021. Available (referenced 22.11.2022): https://docs.microsoft.com/en-US/troubleshoot/windows-server/networking/direct-hosting-of-smb-over-tcpip

[55] CISA, What is wannacry/wannacrypt0r? Available (referenced: 22.11.2022): https://www.cisa.gov/uscert/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_WannaCry_Ransomware_S508C.pdf

[56] Hixon M, Hutchens J. Kali Linux Network Scanning Cookbook - Second Edition. Birmingham: Packt Publishing, Limited; 2017.

[57] Intruder, OpenVAS vs. Nessus - A Comprehensive Analysis, 2021. Available (referenced 22.11.2022): https://www.intruder.io/blog/openvas-vs-nessus

[58] Tenable documentation, About Nessus Plugins. Available (referenced 22.11.2022): https://docs.tenable.com/nessus/Content/AboutNessusPlugins.htm

[59] Tenable, products, Nessus. Available (referenced 22.11.2022): https://www.tenable.com/products/nessus

[60] Tenable, Passive Monitoring or Active Scanning for Operational Technology Environments, 2018. Available (referenced 22.11.2022): https://lookbook.tenable.com/ponemonotreport/whitepaper-active-vs-passive-in-OT-environments

[61] Pospisil O, Blazek P, Fujdiak R, Misurec J. Active Scanning in the Industrial Control Systems. In: 2021 International Symposium on Computer Science and Intelligent Controls (ISCSIC). Piscataway: IEEE; 2021. pp. 227–232.

[62] Cisco, Cyber Vision Distributed Edge Active Discovery, 2020. Available (referenced 22.11.2022): https://www.cisco.com/c/dam/en/us/products/se/2020/11/Collateral/cyber-vision-active-discovery.pdf

[63] Marksteiner S, Jandl-Scherf B, Lernbeiß H. Automatically Determining a Network Reconnaissance Scope Using Passive Scanning Techniques. In: Advances in Intelligent Systems and Computing. Singapore: Springer Singapore; 2020. pp. 117–127.

[64] Automation.com, Active Network Scanning in OT Environments, 2019. Available (referenced 22.11.2022): https://www.automation.com/en-us/articles/2019/active-network-scanning-in-ot-environments

[65] Nozomi, Nozomi networks smart polling data sheet, 2021. Available (referenced 22.11.2021): https://www.nozominetworks.com/resources/data-sheets/smart-polling

[66] Nozomi, Nozomi Networks Solution – N2OS 21.7.0, Release notes. Available (referenced 22.11.2022): http://downloads.nozominetworks.com/bf67a4b0-7945-497c-b8d7-2caaa79e66e4/N2OS-ReleaseNotes-21.7.0.pdf

[67] Nozomi, Nozomi Networks Solution – N2OS 20, User manual, 2020.

[68] Nozomi, Nozomi Networks Solution – N2OS 19.0.4.1, User manual, 2019.

[69] Tenable, Tenable.ot Active Querying solution overview, 2021. Available (referenced 22.11.2022 https://www.tenable.com/solution-briefs/tenable-ot-active-querying

[70] Tenable, Tenable and Indegy: the First Unified, Risk-Based Platform for IT and OT Security (APAC) on-demand webinar. 2020. Available (referenced 22.11.2022): https://www.tenable.com/webinars/apac-tenable-and-indegy-the-first-unified-risk-based-platform-for-it-and-ot-security

[71] Tenable, Tenable.ot 3.13.21 release notes. Available (referenced 22.11.2022): https://docs.tenable.com/releasenotes/Content/tenableot/tenableot31321.htm

[72] The Forrester Wave™: Industrial Control Systems (ICS) Security Solutions, Q4 2021 Available (referenced 22.11.2022): https://reprints2.forrester.com/#/assets/2/1552/RES176441/report

[73] Claroty, Feature Spotlight: Claroty Active Queries, 2022. Available (referenced 22.11.2022): https://claroty.com/blog/feature-spotlight-claroty-active-queries

[74] Claroty, Feature Spotlight: Asset Discovery Methods, 2021. Available (referenced 22.11.2022): https://claroty.com/blog/product-spotlight-asset-discovery

[75] Claroty, Industrial Control System and IT Procotols Support, 2019. Available (referenced 22.11.2022): https://uploads-ssl.webflow.com/5e4909e69065e742eb15fa24/5e4909e69065e76af615fdf4_ProtocolDataSheet250719.pdf

[76] Cisco, Cisco Cyber Vision Active Discovery Configuration Guide, Release 4.1.0. Available (referenced 22.11.2022): https://www.cisco.com/c/en/us/td/docs/security/cyber_vision/publications/Active-Discovery/b_Cisco_cyber_vision_active_discovery_configuration/m_annex_active_discovery_protocols.html

[77] Cisco, Cisco Cyber Vision Data Sheet, 2022. Available (referenced 22.11.2022): https://www.cisco.com/c/en/us/products/collateral/se/internet-of-things/datasheet-c78-743222.html

[78] Dragos, Dragos SEL datasheet. Available (referenced 22.11.2022): https://www.dragos.com/wp-content/uploads/relocated/d/DragosSEL_DataSheet-1.pdf

[79] Dragos, Dragos platform supported protocols. Available (referenced 22.11.2022): https://www.dragos.com/resource/dragos-supported-protocols/

[80] Microsoft, Microsoft Defender for IoT - supported IoT, OT, ICS, and SCADA protocols, 2022. Available (referenced 22.11.2022): https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/concept-supported-protocols

[81] Microsoft, Microsoft Defender for IoT FAQ. Available (referenced 22.11.2022): https://azure.microsoft.com/en-us/products/iot-defender/#faq

[82] Jung HC, Jo H geun, Lee H. UDP-Based Active Scan for IoT Security (UAIS). KSII transactions on Internet and information systems. 2021;15(1): pp. 20–34.

[83] Bandung Y, Tanuraharja J. Modified passive available bandwidth estimation in IEEE 802.11 wlan. Journal of ICT. 2020;19(4): pp. 483–511.

[84] Chaudhari SS, Biradar RC. Available Bandwidth Estimation Using Collision Probability, Idle Period Synchronization and Random Waiting Time in MANETs: Cognitive Agent Based Approach. Wireless personal communications. 2015;85(3): pp. 597–621.

[85] Park HJ, Roh BH. Accurate Passive Bandwidth Estimation (APBE) in IEEE 802.11 Wireless LANs. In: 2010 Proceedings of the 5th International Conference on Ubiquitous Information Technologies and Applications. IEEE; 2010. pp. 1–4.

[86] Rizal A, Bandung Y. Passive Available Bandwidth Estimation Based on Collision Probability and Node State Synchronization in Wireless Networks (PABE), 2017.

[87] Hashida H, Kawamoto Y, Kato N. Efficient Delay-Based Internet-Wide Scanning Method for IoT Devices in Wireless LAN. IEEE internet of things journal. 2020;7(2):1364–1374

[88] Nmap, Scan code and algorithms. Available (referenced 22.11.2022): https://nmap.org/book/port-scanning-algorithms.html#scan-methods-adaptive-retransmission

[89] Armis, resources, Device Knowledgebase. Available (referenced 22.11.2022): https://www.armis.com/videos/device-knowledgebase/