Identification of open ICS and IoT ports using Shodan

Project Report for Information Security Course

Carl Fransson
Linköping University
Linköping, Sweden
carfr548@student.liu.se

Anna Höglund
Linköping University
Linköping, Sweden
annho238@student.liu.se

Supervisor: Andrei Gurtov
andrei.gurtov@liu.se

ABSTRACT

Devices connected to the Internet come with both great advantages but also disadvantages. In areas of Industrial Control Systems and the Internet of Things being connected to the Internet could come with great flexibility but also expose devices to vulnerabilities depending on what communication protocols they use. Therefore it is of great importance how devices are connected to the Internet. The search engine Shodan can scrape the Internet for connected devices both in the areas of ICS and IoT and output a list of them. The security of the most widely used protocols, both in Sweden and the wide world, is then analyzed using vulnerability databases such as Rapid-7, ExploitDB, and the National Vulnerability Database. The result indicated that many of the most commonly used communication protocols were those that were well known in the industry, such as Modbus, but few of them had deployed security mechanisms. The result also indicated that when the data collection is done, the time of the day could possibly alter the result for IoT devices.

KEYWORDS

SCADA, Industrial Control Systems (ICS), Internet of Things (IoT), Shodan

1 INTRODUCTION

To be connected to the Internet comes with both advantages and disadvantages. For example, a device that is connected to the Internet can be monitored by distance, it can also enable communication with other devices while at the same time being more exposed to malicious users and entities [7, 9]. There is a wide range of devices connected to the Internet and the areas they are related to are broad. It can for example be the Internet of Things (IoT) devices such as refrigerators and vacuum cleaners, or Industrial Control Systems (ICS) devices such as water flow monitors or electrical power transmission and distribution.

The ICS cybersecurity landscape is broad, and widening, due to the increasing connection to the Internet [11, 12]. This connection can conduce and increase the pool of vulnerabilities and possibilities to attack and take control of the processes controlled by the ICS. In the past, those vulnerabilities have been exploited, e.q. when a Turkish pipeline was infiltrated and hacked in 2008 leading to a loss of 30 000 barrels of oil [3]. The malicious attackers managed to take control over the system due to a weakness in a wireless camera software and then moved down further into the network layer. They ultimately managed to increase the pressure in the pipeline without notifying the monitoring systems.

Figure 1: Turkish pipeline explosion [3]

One important factor to contribute, or derail, to the security of ICS, as well as IoT, was the use of communication protocols. What protocols are most common, and their possible vulnerabilities, will be the focus of this paper. Data were captured using the tool Shodan [1], which is a database consisting of scraped open network ports and devices. To compare the result gathered by Shodan with previous findings a literature study of related work was completed. The paper is organized as followed. In section section 2 important keywords such as IoT, ICS, and SCADA are explained. In section 3 the use of Shodan is described. It is then followed by section 4 which includes the result and an evaluation of the Shodan queries. The result is then compared with previous work in section 5 and lastly, the paper is concluded in section 6.

[1] https://www.shodan.io/

2 BACKGROUND

Short explanation of important building blocks that is related to the topic of the report.

2.1 ICS

ICS is a term used for control systems responsible for monitoring, operating, and/or automating industrial installations. Such installations could be supervisory control and data acquisition systems (SCADA), automated manufacturing systems and, processes using programmable logic controllers (PLC) [15, 17]. Thus ICS is a combination of software and hardware used to monitor and control different aspects of an industrial process. They are more complex than basic IT business systems however, they share basic constructs. Due to the complexity, there have been multiple cyber incidents related to ICS devices [7, 8, 17]. It is also important to note that due to ICS devices transitioning towards internet and communication systems at a later stage they needed to implement the use of communication protocols [5]. These protocols however were created before this transition and seldom implement, for example, proper authentication is needed for today's environment of the Internet. This is also a vulnerability of ICS devices, once again being the target/victim of possible cyber incidents.

2.2 IoT

The Internet of things is an umbrella term for devices connected to the Internet that has a limited computational power that allows them to send and receive data [2]. Such devices can be refrigerators, light bulbs, and, temperature controllers. Similar to ICS, many IoT devices use protocols that are without security mechanisms. Therefore they can be vulnerable to adversaries. Examples of commonly used IoT protocols are AMQP, COAP, and XMPP.

2.3 Protocols

As previously mentioned ICS devices use protocols for communications. A variety of protocols exists with different purposes and areas they excel in. To get an understanding of how different protocols work, and why they are needed, some of the protocols that are in use today will be explained.

2.3.1 Modbus. The Modbus protocol is used for data communication between PLCs and was created by Modicon in 1979. Modbus uses a master-slave principle to transmit information over serial lines between the devices. The master is singular and can, in a traditional Modbus network, have up to 247 slaves [3]. The Modbus protocol is free for use for companies to build into their products without having to pay royalties. In regards to security mechanisms, Modbus has a low level of security. All messages in the transmission media are transmitted as clear text and it also does not have any authentication between master and slave [4].

2.3.2 BACnet. The BACnet protocol is a data communication protocol used for Building Automation and Control (BAC) networks such as for example fire detection systems, air-condition control systems, etc [4]. The first version of BACnet was launched in 1995 and has since then been upgraded to be of ANSI/ASHRAE standard 135-2012 [13]. It has also been accepted as a global standard by the International Organization for Standardization (ISO). *BACnet: The Global Standard Building Automation and Control Networks* by Newman describes the BACnet security architecture to be applicable to all BACnet network types (Ethernet, ARCNET, etc.), device types, messages types, and so on. The security architecture (BSA) of BACnet is configured in the network layer, however, according to Newman (in 2013) it had at the time not yet been implemented in any commercially available product.

2.3.3 Lantronix. The Lantronix protocol (77FEh) is used by Lantronix XPort devices. Lantronix XPort [5] is an embedded Ethernet device server that can be used to incorporate network connectivity and includes features of both hardware and software such as an embedded server, e-mail notifications as well as an operating system.

2.3.4 KNXnet/IP. The KNXnet/IP protocol is used to connect a KNX bus over an IP network such as a local LAN or the Internet. A KNX system is a bus system used for building control. All buses in the network are required to use the same transmission method and to be able to exchange data via a common bus-network. KNX devices are for example used to manage lighting, energy, audio, video, etc.

2.3.5 Starlight Networks Multimedia. Starlight Networks Multimedia is a transport protocol that is used over port 1911 according to IANA. The company starlight networks creates video-on-demand and other streaming products.

2.3.6 Comparison of different protocols. The above mentioned protocols are the most used ICS protocols. While some properties between them are clear, such as initial release dates, some properties are less obvious. All of the protocols are used for different ICS devices, but with different focus. BACnet focuses on HVAC and mechanical, Modbus focuses on more industrial systems, and KNX on all kinds of systems related to HVAC. Furthermore, their markets also differ, where KNX for example is primarily used in Europe, while the others are used worldwide [1].

[2] https://www.oed.com/

[3] https://www.se.com/us/en/faqs/FA168406/

[4] http://www.bacnet.org

[5] https://www.lantronix.com/products/xport/

2.4 Shodan

Shodan is a search engine used to find devices connected to the internet. It contains a large database with recent internet crawls with open ports, but can also be used to live-crawl a specific ip-address, for example. The crawlers are working at all times, and since the database is updated in real-time this makes the represented data as updated as possible [10]. Its webcrawler work by generating a random IPv4 address and a port, and then scan whether said port is open or not and identifies what metadata is exposed there. It then repeats the steps, in order to ensure complete fairness instead of only checking related ip ranges and ports [10].

While Shodan is supposed to help researchers and cyber security professionals, it unintentionally simplifies the work for attackers who want to exploit faulty configured devices and ports. In a recent study, it was found that the probability of more attacks against a honeypot was 90% within the next 24 hours when Shodan indexed the honeypot [16]. Another study by [14], that also used honeypots, found a positive correlation between devices being noticed by Shodan and contacted by unknown peers.

2.5 Vulnerability Databases

Vulnerability databases are used to document and explain security vulnerabilities, threats, and exploits. There is more than one database with exploit information that can be used, and they do not necessarily keep the same information. Therefore, this report will use more than one vulnerability database to gain a wider range of sources that can potentially complement each other. The used databases will be Rapid-7, ExploitDB, and the National Vulnerability Database.

3 METHODOLOGY

In this study, Shodan was chosen as the tool to identify open devices on the internet, and in order to use it as effectively as possible, all queries were sent to its API. This allowed for easy data collection and storage, as well as easier queries once the setup was done. The setup was installed using The official Python library for Shodan [6], to ensure proper usage.

Once installed, the next step in the process was to choose which queries to run. In Shodan, a query can consist of different filters such as *Country* or *Port*. If a user wants to find how many devices in Sweden are connected to port 20000, then the input would be the following.

country:se, port:20000

The output depends on the output specifications set in the python code, and can for example consist of the top 5 used products or organizations. If the user instead wants to list all ICS devices on the internet, then the input instead would look as follows.

tag:ICS

As with the earlier example with port 20000, the output will be dependent on the specifications set in the code. If the user only wanted to list the amount of ICS devices on the internet, then the output would be as of March 3rd, 2022, 'Total Results: 96814'.

In this report, we mainly focus on IPv4, since IPv6 only is 11.99% of the internet in Sweden [7] and this report mainly focuses on Sweden. However, this can skew the data representation, especially worldwide where IPv6 is more widespread.

4 SOLUTION AND ANALYSIS

In the below subsections the result of the study will be displayed and analyzed.

4.1 Most common ICS devices in Sweden

According to the data collection the top five used protocols for ICS devices are the following.

- **Modbus**: 1287 devices
- **Lantronix discovery protocol**: 542 devices
- **KNXnet/IP**: 294 devices
- **BACnet**: 229 devices
- **Starlight Networks Multimedia Protocol**: 44 devices

In the Appendix the top-five organizations using each protocol are listed in Table 4, Table 6, Table 5, Table 7, and Table 8. From the result, we can conclude that the highest usage is of telephone companies such as Telia, Telenor, and Tele2 for more than one protocol. It is therefore mainly Telecom and Internet providers that are connected to these protocols, similar to the result found in [5]. The total amount of found ICS devices was 2563 in Sweden as of March 7th, 2022. To be noted is that 50% of those were using the protocol Modbus despite being a protocol from 1997 with very few security mechanisms.

4.2 Most common ICS devices connected to Internet

ICS devices are used worldwide for numerous purposes. In Figure 2 the top ten countries with devices connected to Internet are displayed. The most widely used protocols are the following.

[6] https://github.com/achillean/shodan-python

[7] https://www.google.com/intl/en/ipv6/statistics.html

- **Modbus**: 25403 devices
- **KNXnet/IP**: 12728 devices
- **BACnet**: 12295 devices
- **Starlight Networks Multimedia Protocol**: 11077 devices
- **Lantronix discovery protocol**: 5253 devices

The data was collected from Shodan with the use of the tag *tag:ics* which measures the exposure of industrial control systems worldwide. The search resulted in 96814 found devices worldwide, with 31,8 % of those originating from the US. The country with the second most connected devices was Spain with 6 % of all ICS devices connected to the Internet. Sweden came in 10th place with 2,6 % of worldwide connections. The most widely used protocol in the world was Modbus according to the collected data. A representation of the no. of found devices for each country is available in Table 3

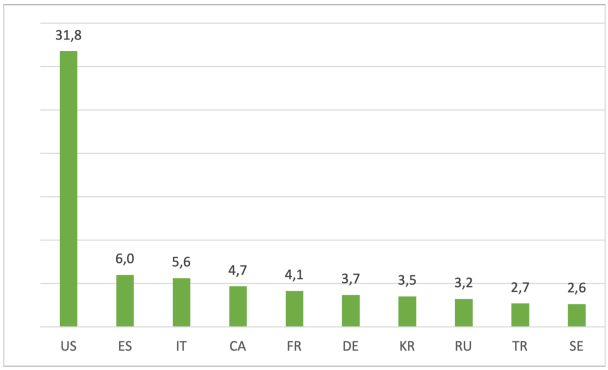

Figure 2: Top 10 countries with ICS devices connected to the Internet

4.3 Most common IoT devices in Sweden

From the data collection the top five IoT devices in use, as of March 7th, 2022 2 pm (CET), could be derived as the product in Table 1. The result indicates that streaming services and their aids (such as Chromecast, and LG webOS TV) are commonly used IoT devices in Sweden. The most commonly used protocol was *Groove GLRPC* over port 9080 with 42307 found connections. To be noted is that port 9080 is opened once a Netflix application is used, presumably in order to run mobile remote control. In second place came *HTTP alternate* over port 8008 with 9399 found connections. Thirdly came *PCSync HTTPS* over port 8443 with 84367 found connections.

4.4 Most common countries with IoT devices

IoT is an area growing constantly and is expected to grow exponentially in the coming years [2], making it an interesting sector to analyze regarding security and vulnerabilities.

Protocol	Number of devices
Netflix	42305
Chromecast	17807
LG webOS TV	5532
Home Assistant	2478
openHAB	1571

Table 1: Most used IoT devices in Sweden.

Considering its expected growth, it would also be of interest to analyze the amount continuously over time instead of only once. That is however out of the scope of this report.

According to our data collection, there are a total of 1996274 IoT devices exposed to the internet as of March 7th, 2022. However, since many IoT devices are turned off when not in use, the amount might be varying and the result should be considered as a timestamp more than a total exact number. As can be seen in Figure 3, Korea dominates the market with almost twenty times the amount of the country with the second most amount of IoT devices. Out of all the results, 51,6 % is tagged as Chromecast, making it the most popular IoT device.

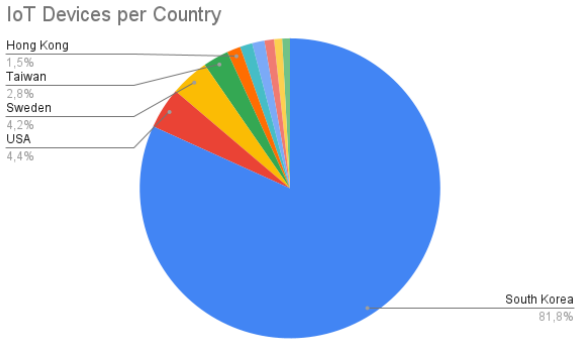

Figure 3: Top 10 countries with IoT devices connected to the Internet

4.5 Protocol exploits

4.5.1 Modbus. As mentioned earlier, Modbus is one of the most popular ICS protocols on the internet as well as one of the older, making it the protocol with the most documented vulnerabilities out of the ones studied in this report.

The National Vulnerability Database lists 110 vulnerabilities[8], ranging from *Missing Authentication for Critical Function*[9] to *Authentication Bypass by Spoofing*[10].

[8]https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=modbus&search_type=all&isCpeNameSearch=false
[9]CVE-2021-22772
[10]CVE-2021-22779

Rapid7 on the other hand only lists 10 vulnerabilities in their database, primarily related to other software using the protocol. An example of such software is libmodbus[11], which is a free library for using Modbus.

Finally, ExploitDB has stored 11 Modbus vulnerabilities in their database. However, since only 2 of those are verified, that is the number we deem as trustworthy in this report. The remaining 2 exploits [12] are both from 2011, and might therefore be patched as of now.

4.5.2 BACnet. According to Rapid7 [13] and ExploitDB [14] BACnet has a known client buffer overflow vulnerability related to the protocol being used in a SCADA Engine's BACnet OPC Client. Such an exploit could lead to an arbitrary code execution which potentially could lead to the system being compromised.

4.5.3 Lantronix. Lantronix vulnerabilities differ greatly depending on which vulnerability database is used, and how you define Lantronix (difference between their hardware and their protocols). Rapid7 [15] has no saved vulnerabilities related to Lantronix, while ExploitDB [16] has one stored exploit with four vulnerabilities related to privilege escalation and buffer overflow using the command line. It also lists a directory traversal vulnerability that could grant access to the underlying operating system, making Lantronix an entry point to the system. Finally, The National Vulnerability Database lists 29 vulnerabilities where the latest critical vulnerability was published on December 22, 2021. The vulnerability [17] is similar to the one listed on ExploitDB where an attacker potentially can get access to the underlying file system.

4.5.4 KNXnet/IP. The national vulnerability database keeps track of a few found vulnerabilities related to KNXnet/IP. The vulnerabilities are of CVE standard which indicates that their impact negatively affects confidentiality, integrity, or availability. One identified vulnerability exists in MDT's firmware for the KNXnet/IP Secure router SCN-IP100.03 and KNX IP interface SCN-IP000.03. The vulnerability existed before v3.0.4 and allowed a remote attacker to make a device unresponsive to all requests on the KNXnet/IP secure layer [18].

4.5.5 Starlight Networks Multimedia. No known vulnerabilities according to Rapid-7, ExploitDB as well as NVD.

[11] cve-2019-14463
[12] CVE-2011-4535, CVE-2010-4709
[13] https://www.rapid7.com/db/modules/exploit/windows/fileformat/bacnet_csv/
[14] https://www.exploit-db.com
[15] https://www.rapid7.com/db/?q=lantronix&type=nexpose
[16] https://www.exploit-db.com/exploits/26100
[17] CVE-2021-21894
[18] CVE-2021-37740

	Rapid7	NVD	ExploitDB
Modbus	17	110	2
BACnet	0	32	2
Lantronix	0	29	1
KNXnet/IP	0	2	0
Starlight Networks	0	0	0

Table 2: ICS protocol vulnerabilities in different vulnerability databases

Country	Number of devices
USA	30757
Spain	5803
Italy	5445
Canada	4531
France	4009
Germany	3591
Korea	3426
Russia	3136
Turkey	2619
Sweden	2563

Table 3: Top 10 countries with ICS devices open to the internet.

4.6 Evaluation and comparison

The study will mainly compare its result with the data collected by Hansson et al., 2018 [5]. The purpose is to find out new trends in the world of ICS and IoT. First, by comparing Figure 2 and Figure 4 it can be noted that Brazil was the top country with connected ICS devices in 2018 and it is now, in 2022, not part of the top ten list. Instead, the number one spot has been taken by the US with 31,8 %, which previously only counted for 14,5 % of connected devices. One major difference between the data collections is the number of found ICS devices then and now: 2 280 652 respectively 96 814. Why the result varied could be due to numerous aspects. One theory is the awareness of the possible security exploits with having devices connected to the Internet. Another theory is the variation of the Shodan search phrase compared to our study and the one from 2018, supplemented by data from [6], indicating that *category:ics* includes far more ICS devices than *tag:ics*. However, to be noted is that *tag:ics* is the search filter proposed by Shodan[19] to find all ICS on the Internet. It is the same thing as writing *category:ics* and then filtering out *-http -html -ssh -ident*.

Another aspect that varies from the result of Hansson et al. is the most popular ICS protocols that are in use. Modbus is still the top protocol in use, however the standings of other

[19] https://www.shodan.io/explore/category/industrial-control-systems

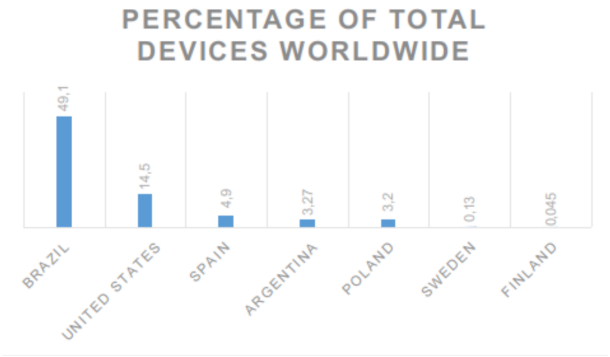

Figure 4: Top 5 countries with ICS devices connected to the Internet from [5]

protocols have been changed. Once again, the difference could be due to the change of search phrase (*tag:ics* vs. *category:ics*). To be noted from the result, as a possible weakness of *tag:ics*, is that the five most widely used protocols are the same in the worldwide search as in Sweden. This seems illegitimate partly due to the low amount of information about protocols such as Starlight Networks Multimedia. It is also only Modbus and BACnet that are explained on Shodans website regarding ICS. Other known well-used protocols, as seen in the collection by [5] are Niagara Fox (Tridium) and Siemens that is mentioned by Shodan but did not show up in our result. Niagara Fox however showed up as the most common product. The issue with *tag:ics*, in relation to a comparison with data collected by *category:ics* could be that the former catches industrial control systems running an industrial protocol [20]. It could therefore be, that some of the more common protocols are disregarded in this search. On the other hand, this feature could increase the probability that the collected result is of ICS devices connected to the internet, and not, for example, a web server connected to a certain protocol.

The results shown in Figure 3 imply that South Korea has more IoT devices than the rest of the world combined. This might be due to the time of the data collection, which was around 2 pm in Sweden. This results in the data from South Korea being gathered at 9 pm local time, while the time in Los Angeles was 5 am local time. Since the majority of the devices were Chromecasts, it is possible that many in South Korea were watching TV, unintentionally skewing the IoT data.

Not all IoT devices were Chromecasts though. The data collection found many cameras open to the internet. One example of such a camera used in South Korea is provided by Xiongmai, and example data from Shodan is shown in Figure 5. Said camera has a known vulnerability [21], making it both open for others to view, and vulnerable to buffer overflow attacks.

(a) Xiongmai Camera

(b) Image from Shodan

Figure 5: Example case from Shodan where both the IoT device and its output is listed and displayed

5 RELATED WORK

A study by Hasselqvist et al. from 2019 [6] plots trends in ICS and includes data about ICS in Sweden and worldwide. Their study was conducted using Shodan to search for devices using a mixture of filters, such as *country* and *port* that were all combined with the *category:ics* filter. Their data collection was then compared to other ICS collections resulting in a span of data from 2013 and 2015 to 2019. The collection showed that the use of protocols Modbus, MQTT, BACnet, Niagara Fox, and DNP3 increased from 2017 to 2019 in Sweden, and also noted that DNP3 had increased usage worldwide. The paper further discusses means to avoid detection by Shodan such as port-knocking. In comparison, our study includes a more recent data collection that indicates that connected ICS devices are decreasing. Their study concluded, on the other hand, that the numbers had stayed roughly the same but at the same time concluded that the trend of connected ICS devices should increase. Our study

[20] https://www.shodan.io/search/examples

[21] CVE-2018-10088

can conclude a similar result, however, the variation of connected devices in our study, concerning previous collections, has mainly been linked to the use of the Shodan search filter *tag:ics*.

The study by Hansson et al. from 2018 [5] conducted a study with the aim of studying the vulnerabilities of ICS and IoT devices connected to the Internet. They collected data from Shodan using queries with filters such as *category, port* and *ip*. Their result includes the most common ICS and IoT devices in Sweden and the most common ICS devices worldwide. Their result concluded that connected deployed ICS and IoT devices decreased in many countries. Their result was also compared to another article that searched for connected devices without Shodan and concluded that Shodan was more accurate. Our study has not sought to understand the accuracy of Shodan but has either way, unintentionally, shown how the result may vary based on the used search filter.

6 CONCLUSION

This study's findings conclude that protocols with vulnerabilities are widely used. As previously seen in [5] and [6] Modbus is still the top protocol of use in Sweden, with 50% of all protocol usage of ICS devices in Sweden. The result indicates that connected ICS and IoT devices are decreasing, however, this trend could also be due to using a new Shodan filter. As seen in the IoT collection, the time during the day that data is collected could be an important element of the result.

REFERENCES

[1] 2019. Which is "better"? BACnet, Lonworks, Modbus, or KNX. https://optigo.net/blog/which-better-bacnet-lonworks-modbus-or-knx

[2] Shadi Al-Sarawi, Mohammed Anbar, Rosni Abdullah, and Ahmad B. Al Hawari. 2020. Internet of Things Market Analysis Forecasts, 2020–2030. In *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*. 449–453. https://doi.org/10.1109/WorldS450073.2020.9210375

[3] Matthew G Angle, Stuart Madnick, James L Kirtley, and Shaharyar Khan. 2019. Identifying and anticipating cyberattacks that could cause physical damage to industrial control systems. *IEEE Power and Energy Technology Systems Journal* 6, 4 (2019), 172–182.

[4] Liron Benbenishti. 2017. SCADA Modbus protocol vulnerabilities. https://www.cyberbit.com/blog/ot-security/scada-modbus-protocol-vulnerabilities/

[5] Adam Hansson, Mohammad Khodari, and Andrei Gurtov. 2018. Analyzing Internet-connected industrial equipment. In *2018 International Conference on Signals and Systems (ICSigSys)*. IEEE, 29–35.

[6] David Hasselquist, Abhimanyu Rawat, and Andrei Gurtov. 2019. Trends and detection avoidance of internet-connected industrial control systems. *IEEE Access* 7 (2019), 155504–155512.

[7] Vinay M. Igure, Sean A. Laughter, and Ronald D. Williams. 2006. Security Issues in SCADA Networks. *Comput. Secur.* 25, 7 (oct 2006), 498–506. https://doi.org/10.1016/j.cose.2006.03.001

[8] Robert E Johnson. 2010. Survey of SCADA security challenges and potential attack vectors. In *2010 international conference for internet technology and secured transactions*. IEEE, 1–5.

[9] Xingwei Liang and Yoohwan Kim. 2021. A Survey on Security Attacks and Solutions in the IoT Network. In *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*. 0853–0859. https://doi.org/10.1109/CCWC51732.2021.9376174

[10] John Matherly. 2015. Complete guide to shodan. *Shodan, LLC (2016-02-25)* 1 (2015).

[11] Stephen McLaughlin, Charalambos Konstantinou, Xueyang Wang, Lucas Davi, Ahmad-Reza Sadeghi, Michail Maniatakos, and Ramesh Karri. 2016. The cybersecurity landscape in industrial control systems. *Proc. IEEE* 104, 5 (2016), 1039–1057.

[12] European Network and Information Security Agency (ENISA). 2016. Communication network dependencies for ICS/SCADA Systems. (2016).

[13] H.M Newman. 2013. *BACnet: the global standard for building automation and control networks*. Momentum Press.

[14] Alexandru Vlad Serbanescu, Sebastian Obermeier, and Der-Yeuan Yu. 2015. ICS threat analysis using a large-scale honeynet. In *3rd International Symposium for ICS & SCADA Cyber Security Research 2015 (ICS-CSR 2015) 3*. 20–30.

[15] Seppo Tiilikainen. 2014. Improving the national cyber-security by finding vulnerable industrial control systems from the Internet. *School of Electrical Engineering, Aalto University, URL: https://aaltodoc. aalto. fi/bitstream/handle/123456789/12918/master* (2014).

[16] Andrea Tundis, Eric Marc Modo Nga, and Max Mühlhäuser. 2021. An Exploratory Analysis on the Impact of Shodan Scanning Tool on the Network Attacks. In *The 16th International Conference on Availability, Reliability and Security* (Vienna, Austria) *(ARES 2021)*. Association for Computing Machinery, New York, NY, USA, Article 39, 10 pages. https://doi.org/10.1145/3465481.3469197

[17] Joe Weiss. 2008. Assuring industrial control system (ICS) cyber security. *Center for Strategic and International Studies* (2008).

APPENDIX

Organization	Number of devices
Telia Network Services	303
Telia Company AB	280
Telenor Sverige AB	154
Stockholms Stadsnat AB	68
Tele2 Sverige AB	62

Table 4: Top 5 organizations in Sweden using MODBUS.

Organization	Number of devices
Telia Network Services	53
Bahnhof AB	29
Telia Company AB	29
A3 Customer Network	23
Bredband2 AB	22

Table 5: Top 5 organizations in Sweden using KNXnet/IP.

Organization	Number of devices
Telia Company AB	135
Telenor Sverige AB	80
Telia Network Services	80
Tele2 Sverige AB	58
Lulebo Residentials	34

Table 6: Top 5 organizations in Sweden using Lantronix.

Organization	Number of devices
Stockholms Stadsnat AB	50
Telia Network Services	40
Telenor Sverige AB	30
Telia Company AB	28
Ownit Broadband	25

Table 7: Top 5 organizations in Sweden using BACnet.

Organization	Number of devices
Telia Network Services	8
Telia Company AB	4
AxByte Internet Services AB	3
Bredband2 AB	3
Hi3G Access AB	3

Table 8: Top 5 organizations in Sweden using Starlight Networks Multimedia.