Two Decades of SCADA Exploitation: A Brief History

Simon Duque Antón, Daniel Fraunholz, Christoph Lipps,
Frederic Pohl, Marc Zimmermann and Hans D. Schotten
Intelligent Networks Research Group
German Research Center for Artificial Intelligence
DE-67663 Kaiserslautern
Email: {firstname}.{lastname}@dfki.de

***Abstract*—Since the early 1960, industrial process control has been applied by electric systems. In the mid 1970's, the term SCADA emerged, describing the automated control and data acquisition. Since most industrial and automation networks were physically isolated, security was not an issue. This changed, when in the early 2000's industrial networks were opened to the public internet. The reasons were manifold. Increased interconnectivity led to more productivity, simplicity and ease of use. It decreased the configuration overhead and downtimes for system adjustments. However, it also led to an abundance of new attack vectors. In recent time, there has been a remarkable amount of attacks on industrial companies and infrastructures. In this paper, known attacks on industrial systems are analysed. This is done by investigating the exploits that are available on public sources. The different types of attacks and their points of entry are reviewed in this paper. Trends in exploitation as well as targeted attack campaigns against industrial enterprises are introduced.**

I. Introduction

In the 1970's, the third industrial revolution took place [1]. During this phase, computers were introduced into industry in order to automate tasks that, until then, had to be done by hand or by application-tailored solutions. Since then, the computer technology has taken huge steps. Reconfigurable Programmable Logic Controllers (*PLCs*) took the place of hard-wired relay logic circuits [2]. Domain-specific, proprietary fieldbuses, like *CAN* [3] and *Modbus* [4], [5], have been replaced by *TCP/IP*-based solutions, such as *ModbusTCP* [5], [6], *ProfiNET* [7] and *OPC UA* [8], that make use of the vastly available internet infrastructure and its network hardware. Opening networks to the outside enables easier management of production capabilities. Remote maintenance, simpler adjustment of machines and a constant flow of information are but a few of the advantages. There are, however, some downsides. Two of the main reasons why security is inherently absent in virtually every technology and protocol used, are as follows: Industrial networks were physically separated from the internet, when the technology arose [9] and each set up of an industrial company is unique and very hard to get around in [9]. As recent events, many of which are explained in section V, show, both assertions do not hold true anymore, if they ever did. Many recent examples show that industrial networks can and will be breached. It needs to be highlighted, that, as in consumer electronics, the user plays a crucial role in securing a system. Many of the newer botnets, such as Hajime or Mirai, try to gain access by using default credentials, with a tremendous success. This behaviour has been analysed, among others, in our previous works [10], [11]. Many industrial systems use credentials for means of configuration. For reasons of ease of use, however, the passwords are often weak and shared among many users. Attackers that try standard configurations to gain access will succeed if the system credentials have not been altered. This kind of threat is also common in the exploits examined in section IV. It is very hard for intrusion detection systems to discover abuse that is performed with valid credentials. Changing default credentials is therefore a vital step in order to enable security in a system. The remainder of this work is structured as follows. In section II, surveys and analyses of attacks are listed. After that, a statistical analysis of the Common Vulnerabilities and Exposures (*CVE*) list is performed in section III. This is followed by an in-depth analysis of available Supervisory Control And Data Acquisition (*SCADA*)-system based exploits in section IV, as well as a breakdown of attack campaigns against industry in section V. The lessons learned are listed in section VI. This work will be concluded in section VII.

II. Related Work

Even though there are a lot of survey papers, as well as taxonomies that present an overview of different kinds of attacks, there has not yet been a systematic analysis of all publicly available *SCADA* exploits to the best of our knowledge. A very broad and extensive overview over current *SCADA*-based attack-vectors can be found in the works of Zhu, Joseph and Sastry [12]. In addition to that, there are other works that give an overview over existing SCADA-attacks and survey current exploits [9], [13], [14], [15]. Not only attacks on *SCADA*-systems are well documented, but also countermeasures, as well as means for hardening systems, are processed in literature [16], [17]. There are also works presenting taxonomies of attacks, also in order to help operators assess risks and threats to their systems and implement the according countermeasures [18], [19], as well as works for the collection of data that allows for insight about the condition of a system [20], [21]. The German Federal Office for Information Security (*BSI*) periodically releases security advices for

978-1-5386-0725-1/17/$31.00 ©2017 IEEE

industry [22]. Furthermore, there are surveys analysing specific domains, such as automotive and fieldbus-security [23] (some of the relevant works are in German [24], [25]) and wireless-security [26]. Many of the exploits we examine in this paper have already been investigated in literature. The amount of works analysing singular attacks is vast, therefore, we only reference such works in the according sections.

III. Statistical Analysis

An exhaustive list of all *CVEs* can be found online [27]. Since it contains over 100 000 entries, manual analysis was infeasible. We developed a text-processing script in order to gain statistical information about the distribution of exploits. A major drawback was that the most specific information was written in natural language, without any form. We searched the document for keywords while using stemming in order to find any variant of the keyword. Stemming is a technique employed to process natural languages [28]. The word stems of keywords are derived, then similar word stems are searched in the target file. We used the python stemming-library [29]. The results of the statistical analysis are summarised in table I.

The entry "Overall categorized entries", as well as the "Percentage covered by keywords", display the number of different attacks that have been classified, after accounting for entries with multiple keywords. That means 65 919 entries (or 61.87%) in the *CVE* list can be attributed to at least one of the categories. The largest group is Remote Code Execution with 28 000 occurrences, closely followed by Denial of Service (*DoS*) and Injection attacks. *SCADA* exploits are relatively small, with only 373 entries. This shows that, even though it is not as present as office *IT*-based attacks, *SCADA*-based exploits are becoming more of an issue for manufacturers.

IV. In-depth Analysis

In this section, four different types of attacks that are relevant for industrial applications are analysed. First, attacks on *PLC* systems are considered in subsection IV-A. After that, fieldbus-based exploits are discussed in subsection IV-B, followed by wireless- and hardware-attacks in subsections IV-C and IV-D. These types of attacks were chosen to be discussed as they are the industrial-specific attack vectors and have not be discussed at large in the context of office-*IT*-security. *PLCs* can mostly be found in industrial environments as they are used to control production machines. The same goes for fieldbus systems, that, aside from some appliances in home automation, are comonly employed in industrial automation. Wireless networks are also commonly used in office and home environments. There are, however, industry specific protocols that are only applied in this context. These protocols are discussed here. Hardware attacks can have a great impact due to the distributed nature of production environment and the fact that machines have hardware interfaces.

A. Attacks on PLCs

PLCs are resource for industrial applications controlling Cyber-Physical (Production) Systems. Hence, they interact with and operate devices in the physical world. In contrast to office *IT* systems which only handle data, they interact with the real world. Attacks on *PLCs* therefore have an impact on physical entites, be it human workers or production resources. This leads to grave consequences of the successful abuse of *PLCs*. As common computation resources, *PLCs* usually require an underlying operating system. In most cases, this is a version of Windows, adapted to the specific needs for industrial applications. As there is an abundance of exploits and vulnerabilites based on flaws in the operating system, we only consider vulnerabilities that specifically derive from the industrial application of the given system. Furthermore, only threats that occur in this context are analysed. In total, we found about 100 exploits as *metasploit* [30] modules and Proofs of Concepts (*PoC*). All metasploit-modules are listed in the *Rapid7*-database [31]. The databases we searched additionally were *exploit-db* [32], *0day-today* [33] and *packetstorm-security* [34]. This number is smaller than the entries found in the *CVE* list in section III as there is executable code to be found. As a result, anybody can exploit these vulnerabilities without much difficulties, rendering them very dangerous for operators. The number of *CVE* discoveries and exploit developments per year is shown in figure 1. Unfortunately, some exploits could not be attributed to a year; this has been accounted for by a question mark. The list amounts to a mean value of 8.8 and a median of 7 exploit developments per year. A peak of 31 developments per year can be found in 2011. One possible explanation is that it was the year after *Stuxnet* [35] was discovered (see table II) and there was a special interest in *PLC*-exploitation. The trend of *CVE*-development is also rising, meaning that the amount of *CVEs* discovered per year has been rising, starting in 2011.

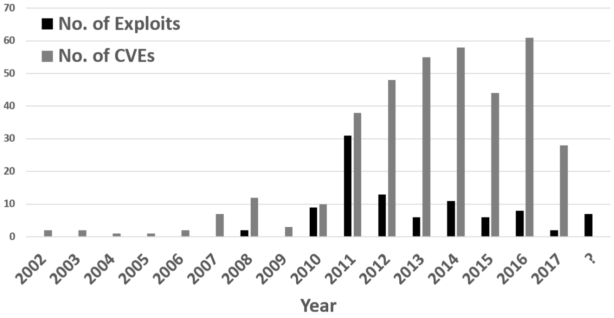

Fig. 1. Number of Exploit and *CVE* Discoveries per Year

We distinguished between four different categories of exploits:

- *Code Execution* is the unauthorised execution of malicious code
- *Data Extraction* is the unauthorised disclosure of information
- *DoS* describes the partial or full degradation of the availability of a service or resource
- *Privilege Escalation* is the process of maliciously obtaining higher privileges on a system than intended

TABLE I
STATISTICAL ANALYSIS OF THE *CVE*-LIBRARY

Description	Keywords	Number	Percentage
All CVEs	-	106 540	100.00%
Remote Code Execution	rce, arbitrary, execution	28 016	26.30%
Denial of Service	denial, crash, instable, consume	19 638	18.43%
Injection attacks	injection, sql	17 280	16.22%
Information Disclosure	traverse, disclose, sensitive, bypass	14 875	13.96%
Buffer Overflows	buffer, overflow	9 800	9.20%
SCADA-attacks	scada, plc, industry, modbus, profinet, beckhoff, siemens	373	0.35%
Overall categorized entries	-	65 919	61.87%
Entries w/ multiple keywords	-	21 620	20.29%

The distribution of these categories on windows-based systems is depicted in figure 2. Of 66 windows-based exploits, almost three quarters allow the execution of arbitrary code. This is a tremendous threat since it allows an attacker to alter, add and delete resources on the affected system.

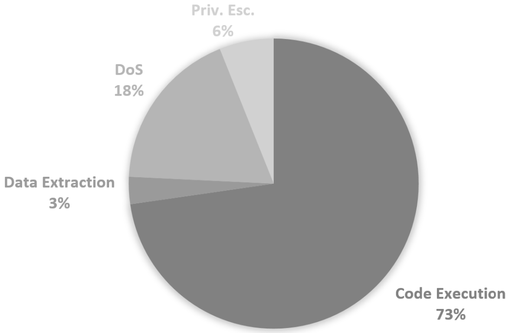

Fig. 2. Distribution of Categories on Windows Platforms

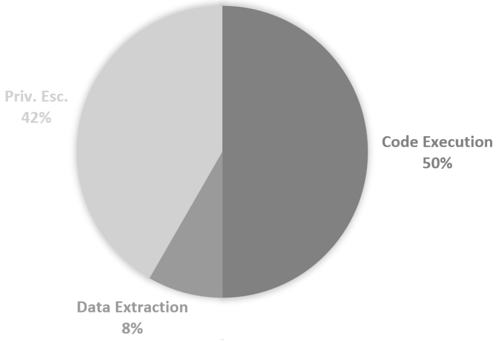

Fig. 3. Distribution of Categories for Local Exploits

Furthermore, we grouped all exploits into *remote* and *local*. *Local* exploits allow an attacker to execute an exploit on a system he already has unprivileged access to, usually in the form of a user account with limited rights. *Remote* exploits can be executed without any prior access to the system, despite some form of network connection. In figure 3, the distribution of the categories for local access is shown. The overall number of local exploits is relatively small, comprising only 12 exploits. In this scenario, the execution of code is most common. The distribution of the categories for remote access is shown in figure 4. It comprises of 84 exploits, most of which are code execution as well. The most prevalent threat for *PLC*-based exploitation is the execution of remote code. This is a very severe threat because of the priorities of industry. While in classic office-*IT*, the *CIA* (Confidentiality, Integrity, Availability) security targets are common, each with about the same importance, the most important security target by far for industry is availability. Unavailable production facilities cost a huge amount of money, making this the top priority of machine operators. *Code Execution* has the potential to disable facilities, rendering them unavailable and costing revenue.

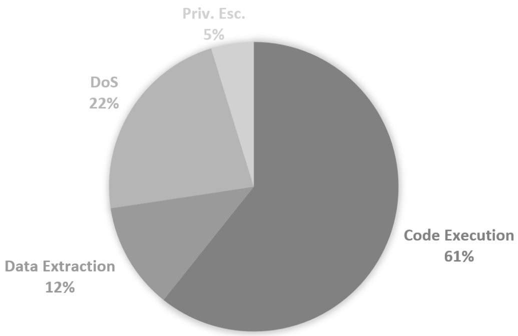

Fig. 4. Distribution of Categories for Remote Exploits

B. Attacks on Fieldbus-Level

Due to the proprietary nature of industrial networks, a vast landscape of fieldbus protocols has emerged. Protocols such as *Modbus* [4], *Profinet* [7], *CAN* [3], *Local Interconnect Network (LIN)* [36], *Media Oriented System Transport (MOST)* [37] and *FlexRay* [38]. These protocols have inherent security flaws. Since there are no means of authentication, identities are not assigned to the participating entities [12]. That means an attacker with access to the bus can appear as a valid communication partner and thus extract and inject messages. This results in a break of confidentiality and integrity. Due to these security flaws and the lack of encryption [39], an attacker can monitor the systems and even deploy attacks. Examples for such attacks are Man in the Middle (*MitM*) and

DoS. In systems using *Modbus*, malicious adversaries can read all messages to discover active controllers and used function codes as well as inject commands themselves. Additionally, they can send incorrect messages or error flags to eliminate single controllers or even the entire system. Many industrial systems have a remote maintenance interface that can be accessed via internet [14]. Often, this interface is secured poorly, or not at all [14]. This means that an attacker with access to the same network as the interface can change system settings and read system conditions. Gateways are used in order to connect several fieldbus networks. Oftentimes, these gateways are not configured securely, allowing an attacker that has access to one fieldbus network, to traverse to different networks [24]. As a counter example, *OPC-UA* [8] needs to be mentioned. It is a very modern fieldbus-protocol that allows definition of entities, including authentication and encryption. The shell model allows for encapsulation of functional units and the definition of interfaces.

C. Attacks on Wireless Systems

Driven by the fourth industrial revolution, wireless communication finds its way into industrial systems. There are some protocols that are commonly used in industrial applications, such as *Bluetooth Low Energy* [40], *ZigBee* [41] and *Z-Wave* [42], *Radio Frequency IDentifier (RFID)* [43] and the *Long Range Wide Area Network (LoRa)* [44]. *Wireless Local Area Network (WLAN)* [45] is also often used in industry, but since it was originally developed for classical office-*IT*, it is not considered in this work. *RFID* is commonly used by industry to tag entities and materials and account for them in storage or production. The other protocols are commonly used for data transmission and communication. There are several flaws and fixes for *WLAN*, but they are out of scope for this work for the reasons named above. As there is no physical access control to the wireless channel, an adversary can listen to the communication, given he is within the range of the wireless signal. Therefore, most wireless communication protocols are encrypted. Still, some encryption schemes can be broken, rendering the content unprotected. If there is no, or weak, encryption, an attacker can listen to the communication and extract information to perform a *MitM* [46] attack. Furthermore, he can inject messages into the network with the purpose of launching *DoS* attacks. A famous example is *Wireless Equivalent Privacy (WEP)* [47], that is broken [48] but still in use. Another example is *ZigBee* whose encryption key, in its default configuration, can easily be recovered by an attacker. Due to poor manufacturer implementations, the secret key is often transmitted in plain text if a new device advertises to the network, for example after restarting [49]. An attacker can obtain this key and gains full access to the network. Another problem in wireless networks are relay attacks. Using those, an attacker can capture a communication packet, transport it over a different protocol, and inject it into the network on a different place. This is commonly done with *Bluetooth* or *RFID*. An attacker can use this method to get a response to a challenge, even though the key is not near a key reader. This method has already successfully been applied to break the *Passive Keyless Entry and Start (PKES)* of different car manufacturers [50]. Spoofing and impersonation are other common attack concepts on wireless protocols. Spoofing means the disguise of an attacker as a valid entity to participate in a communication, impersonation describes an attacker that claims to be an entity she is not. *Bluetooth* is vulnerable to attacks with *Rogue Access Points (APs)* [26], among others. Those are *APs* that are set up by an attacker and imitate valid APs. Because of the ad-hoc nature and the frequency hopping properties of *Bluetooth*, rogue *APs* are hard to detect [26]. The same concept can be applied to *RFID*, where fake tags or readers can read or manipulate entries [51]. Furthermore, wireless channels are inherently prone to jamming attacks. Since there is no access control, an attacker can flood the channel with packets, or simply jam it with noise [52]. This prevents the valid users from communicating with each other. There are also more sophisticated approaches that exploit protocol flaws to prevent communication or that do not jam constantly to make discovery harder [52].

D. Physical-Layer Attacks

Physical, or hardware attacks, are among the most difficult ones. An adversary with physical access to a device or system has more possibilities of inflicting damage and abusing services than one on a remote location. Industrial companies, therefore, put a strong emphasis on obstruction of physical access by perimeters such as, walls, gates and guards. Given access, an adversary can, with enough force, always destroy a system rendering it unusable and creating a *DoS*. There are, however, more sophisticated and subtle approaches in tampering with devices. There are attacks on embedded devices, particularly *PLCs*, that falsify sensor values. This, in turn, creates, inapt reactions from the devices, leading to undesired behaviour. In literature, there is the ”Ghost in the PLC”-attack, that alters the input-pins of a *PLC*, as described by Abbasi and Hashemi [53]. Another work on falsifying input values and creating improper responses from the system is shown by Urbina, Giraldo, Tippenhauer and Cardenas [54]. In addition to tampering with sensor-values, an attacker can read or update the code on a *PLC*. Such an attack is described by Basnight, Butts, Lopez and Dube [55]. In order to stealthily deploy malware on a *PLC*, Garcia, Brasser, Cintuglu, Sadeghi, Mohammed and Zonouz propose a method to read system information and create a fitting rootkit [56]. Even though it is not the most relevant attack vector in practice, securing physical access is a vital task for industry, since adversaries with direct access have many opportunities with a potentially high impact.

V. Attack Campaigns

The exploits that have been introduced in section IV have been used for attack campaigns against industrial players. We found that there were two noteworthy kinds of attacks:

- Spearphishing campaigns against employees
- Attacks on the industrial infrastructure

Phishing and spearphishing are common practices for malicious adversaries intending to gain insight on company secrets by gaining access to the office *IT* infrastructure and stealing data. A timeline of known spearphishing campaigns with an industrial background is shown in figure 5. In phishing, unsuspecting victims are sent emails with malicious content, oftentimes a link to a website that is infected with malware [57]. Attachments with malicious content are another common form of phishing [57]. The chances of an attacker to get a victim to follow the link can be increased by personalizing the email. This is called "social engineering" [57], the application of phishing to selected targets with highly adapted content is called "spearphishing".

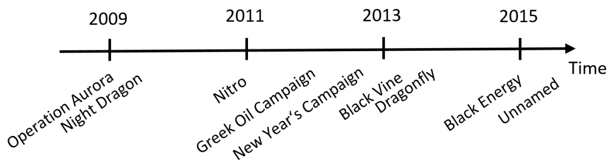

Fig. 5. Timeline of Selected Spearphishing Campaigns

Operation Aurora [58] aimed at the software industry, particularly *Google*. The *Night Dragon*, *Greek Oil* and *New Year's* campaigns aimed at various branches of the energy industry, namely research and petroleum processing [59]. Furthermore, the *Nitro* campaign [60] aimed at the chemical industry and was intended to obtain sensitive documents, designs and schemas for manufacturing. *Black Vine* [61] campaign was used for several targets. First, aerospace companies were in the focus. After that, it was aimed against healthcare institutions in the U.S. The *Dragonfly* [62] and *Black Energy* [63] campaigns aimed at the energy industry as well, this time against *Industrial Control System (ICS)* manufacturing and power generation. In a report, an attack campaign, that is called *Unnamed* [64] in our timeline in figure 5, was described also aimed for the extraction of confidential information about *ICS* manufacturing in the energy industry. Attacks on the industrial infrastructure often aim at sabotaging production. Highly sophisticated malware is employed in these campaigns [57]. A selected list of all known industrial malware campaigns can be found in table II. In this table, the name of the malware is shown, as well as the year of discovery. Furthermore, the presumed target is listed, followed by a *Target Score (TS)* describing the kind of attack that was employed. The *TS* is assigned a value according to the following scheme:

- 1: The malware does not specifically target *ICS*, the incurred consequences are a side effect
- 2: The malware targets *Windows* machines related to *ICS*
- 3: The malware targets software related to *ICS* projects
- 4: The malware targets *PLCs* and other native devices and protocols

In addition to that, the presumed purpose, the affected *ICS* and *CVEs* that were used in the exploit are listed. *Slammer* and *Conficker* were computer worms that also infected nuclear power station [65] respectively air force stations in France and Germany [66]. *Stuxnet* [35] is one of the most renowned industrial malwares. It was aimed at Iranian nuclear enrichment facilities, but, due to programming errors, also infected other systems and therefore was found. It used several different 0-day exploits, depending on the operating systems it encountered, and showed a deep understanding of *Siemens S7-300 PLCs*. *Duqu* and *Duqu 2.0* [67], [68] were used for spying on industrial project documents. *Shamoon* and *Shamoon 2.0* [69] were intended on sabotaging the Saudi-Arabian oil industry. *Stuxnet 0.5* [70] was aimed at sabotaging Iranian nuclear enrichment facilities, also by infecting *Siemens S7-300 PLCs*. It was employed before *Stuxnet*, but was found later due to a different propagation mechanism. *Havex* [62] was a malware infecting the European energy industry and spying on confidential information. *BlackEnergy* and *Industroyer* [71] were aimed at Ukrainian power plants. Major blackouts in December of 2015, respectively December of 2016 in the Ukraine are said to result from *BlackEnergy* and *Industroyer*.

VI. Lessons Learned

We used *Shodan* [72], an internet search engine that specialises on the *Internet of Things (IoT)* and industrial applications. Specifically, we grouped our search by ports and only looked for ports that are the default for several industrial protocols. The results of this survey is shown in table III. It can be seen that there still is a huge amount of industrial devices to be found, directly connected to the internet. Since all of the entries in table III are fieldbuses, their connection to the internet is risky. They were never designed for security as one of the paradigms in their development was the physical separation of industrial network and internet [9]. This assumption does not hold for about 1.45 million fieldbuses, that, depending on their configuration, can be accessed - and probably tampered with - by an attacker via internet access. We introduced some concepts for botnets in our previous works [10], [11], and there are other projects that develop industrial honeypots, such as the *Conpot* [73]-project and the *IoT-pot* [74]. One could assume that some of the entries in table III originate in honeypots. We found that 137 of the above entries definitely stem from honeypots by comparing the banners found with the default banners of *Conpot*. Even though it is plausible that we missed several honeypots, we deem it probable that a majority of the entries is from productive systems. Despite the fact that security flaws in industrial applications have been a critical issue for quite some time, there still are devices and protocols used in insecure ways.

VII. Conclusion

The trend in figure 1 shows that *PLC*-exploitation is becoming more relevant. At the same time, our findings in section VI point out that many operators do not employ their industrial networks in a physically separated way to at least provide basic security. In this work, we showed that the kill chain for *ICS* is rather easy to use. There are tools to identify vulnerable systems, as well as databases that contain information about vulnerabilities and sometimes also

TABLE II
A SELECTION OF ATTACK TOOLS AND CAMPAIGNS

Name	Year	Presumed Target	*TS*	Purp.	Affected *ICS*	Exploited *CVE*
Slammer	2003	untargeted	1	Sabot.	Nuclear Power Station	CVE-2002-0649
Conficker	2009	untargeted	1	Sabot.	French & German Air Force	CVE-2008-4250
Stuxnet	2010	Iranian Nuclear Enrichment Facilites	4	Sabot.	Siemens S7-300	CVE-2010-2568 CVE-2008-4250 CVE-2010-2729 CVE-2010-2772
Duqu / Duqu 2.0	2011/2015	Industrial Project Documents	3	Esp.	-	-
Shamoon / Shamoon 2.0	2012/2017	Saudi-Arabian Oil Industry	2	Sabot.	-	-
Regin	2012	GSM Base Stations	4	Esp.	-	-
Stuxnet 0.5	2013	Iranian Nuclear Enrichment Facilites	4	Sabot.	Siemens S7-300	CVE-2012-3015
Havex	2013	European Energy Industry	3	Esp.	-	-
BlackEnergy	2016	Ukrainian Power Plant	3	Sabot.	-	CVE-2014-4114 CVE-2014-0751
Industroyer	2017	Ukrainian Power Plant	4	Sabot.	Siemens SIPROTEC	CVE-2015-5374

TABLE III
DEVICES FOUND PUBLICLY ADDRESSABLE BY *Shodan*

Service	Port Numbers	Hits	Hit Percentage
EtherNet/IP	2222	1 015 093	69.78%
DNP3	20000	232 108	15.95%
OMRON	9600	51 911	3.57%
Niagara Fox	1911	46 806	3.22%
ENIP	44818	32 100	2.21%
Proconos	20547	19 761	1.36%
Modbus	502	18 732	1.29%
CoDeSys	1200, 2455	17 667	1.21%
PCWorx	1962	14 949	1.03%
Siemens	102	3368	0.23%
Fieldbus	1089-1091	924	0.06%
Profinet	34962-34964	809	0.06%
DNP	19999	300	0.02%
EtherCAT	34980	270	0.02%
Sum	-	1 454 798	100.00%

the corresponding exploits. This makes it simple also for non tech-savvy people to attack systems and cause damage. The rising importance of interconnectivity in industrial applications will lead to an increase in interest of attackers. As more and more industrial systems become accessible, get more complex software and are remotely configurable, the number of possibilities for exploitation and intrusion also increases. Many industrial operators maintain their production units for decades with little or no possibilities for software updates. This leads to a tremendous danger, as more exploits occur every year.

ACKNOWLEDGMENTS

This work has been supported by the Federal Ministry of Education and Research of the Federal Republic of Germany (Foerderkennzeichen KIS4ITS0001, IUNO). The authors alone are responsible for the content of the paper.

REFERENCES

[1] S. Thomson, “Is this the start of a fourth industrial revolution?” 2015. [Online]. Available: https://www.weforum.org/agenda/2015/09/fourth-industrial-revolution/?utm_content=buffer274c7&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

[2] B. Galloway and G. P. Hancke, “Introudction to industrial control networks,” *IEEE Communications Surveys Tutorials*, vol. 15, no. 2, pp. 860–880, 2013.

[3] Robert Bosch GmbH, “Can specification: Version 2.0,” 1991. [Online]. Available: http://www.bosch-semiconductors.de/media/ubk_semiconductors/pdf_1/canliteratur/can2spec.pdf

[4] MODICON Inc., 1996. [Online]. Available: http://www.modbus.org/docs/PI_MBUS_300.pdf

[5] Modbus-IDA, “Modbus messaging on tcp/ip implementation guide v1.0b,” 2006. [Online]. Available: http://www.modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf

[6] Modbus, “Modbus application protocol specification v1.1b3,” 2012. [Online]. Available: http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf

[7] PROFIBUS, “Profinet specification,” 2017. [Online]. Available: http://www.profibus.com/nc/download/specifications-standards/downloads/profinet-io-specification/display/

[8] OPC Foundation, “Unified architecture,” 2017. [Online]. Available: https://opcfoundation.org/developer-tools/specifications-unified-architecture/part-1-overview-and-concepts

[9] V. M. Igure, S. A. Laughter, and R. D. Williams, “Security issues in scada networks,” *Computers & Security*, vol. 25, pp. 498–506, 2006.

[10] D. Fraunholz, D. Krohmer, S. Duque Anton, and H. D. Schotten, “Investigation of cyber crime conducted by abusing weak or default passwords with a medium interaction honeypot,” in *International Conference On Cyber Security And Protection Of Digital Services(Cyber Security-17)*. IEEE, 2017.

[11] D. Fraunholz, M. Zimmermann, S. Duque Anton, J. Schneider, and H. D. Schotten, “Distributed and highly-scalable wan network attack sensing and sophisticated analysing framework based on honeypot technology,” in *7th International Conference on Cloud Computing, Data Science & Engineering (Confluence-2017)*, Amity School of Engineering and Technology. IEEE, 1 2017, p. 33.

[12] B. Zhu, A. Joseph, and S. Sastry, “A taxonomy of cyber attacks on scada systems,” *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, pp. 380–388, 2011.

[13] P. S. Motta Pires and Oliveira, Luiz Affonso H. G., “Security aspects of scada and corporate network interconnection: An overview,” *2006 International Conference on Dependability of Computer Systems*, pp. 127–134, 2006.

[14] J. Caswell, “A survey of industrial control systems security,” 2011. [Online]. Available: https://www.cse.wustl.edu/~jain/cse571-11/ftp/ics/

[15] B. Meixell and E. Forner, “Out of control: Demonstrating scada exploitation,” Las Vegas, July 2013. [Online]. Available: https://www.blackhat.com/us-13/

[16] R. Chandia, J. Gonzalez, T. Kilpatrick, M. Papa, and S. Shenoi, “Security strategies for scada networks,” *International Conference on Critical Infrastructure Protection*, vol. 253, pp. 117–131, 2007. [Online]. Available: https://www.researchgate.net/publication/221654717_Security_Strategies_for_SCADA_Networks

[17] A. Hildick-Smith, “Security for critical infrastructure scada

systems," 2005. [Online]. Available: https://www.sans.org/reading-room/whitepapers/warfare/security-critical-infrastructure-scada-systems-1644

[18] International Organization for Standardization, "Iso/iec 27001," 2013. [Online]. Available: https://www.iso.org/standard/54534.html

[19] M. Langfinger, S. Duque Anton, C. Lipps, A. Weinand, and H. D. Schotten, "Angriffe la carte - systematische bewertung von angriffsvektoren auf industrielle (funk-)netzwerke," in *17. VDI Automatisierungskongress (AUTOMATION-2016)*, VDI. VDI, 6 2016.

[20] S. Duque Anton, D. Fraunholz, and H. D. Schotten, "Angriffserkennung fuer industrielle netze innerhalb des projektes iuno," in *ITG-Fachtagung Mobilkommunikation - Technologien und Anwendungen (ITG-17)*, P. Roer, H. D. Schotten, R. Toenjes, and C. Westerkamp, Eds., Informationstechnische Gesellschaft im VDE (ITG). VDE Verlag GmbH, 2017, pp. 68–73.

[21] S. Duque Anton, D. Fraunholz, J. Zemitis, F. Pohl, and H. D. Schotten, "Highly scalable and flexible model for effective aggregation of context-based data in generic iiot scenarios," in *9th Central European Workshop on Services and their Composition (ZEUS-2017)*, O. Kopp, J. Lenhard, and C. Pautasso, Eds. CEUR Workshop Proceedings, 4 2017, pp. 51–58.

[22] Bundesamt für Sicherheit in der Informationstechnik, "Industrial control system security: Top 10 bedrohungen und gegenmaßnahmen 2016," 2016. [Online]. Available: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.pdf?__blob=publicationFile

[23] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," *Proceedings of the 20th USENIX Conference on Security*, 2011. [Online]. Available: http://dl.acm.org/citation.cfm?id=2028067.2028073

[24] M. Wolf, A. Weimerskirch, and C. Paar, "Sicherheit in automobilen bussystemen," 2014. [Online]. Available: https://www.researchgate.net/publication/228696907_Sicherheit_in_automobilen_Bussystemen

[25] T-Systems, "White paper: It-sicherheit für das vernetzte fahrzeug," 2016. [Online]. Available: https://www.t-systems.com/blob/454516/5dd711e8706ac91e48c291a4d02cf6a0/dl-wp-it-sicherheit-vernetzte-autos.pdf

[26] J. Wright, "Five wireless threats you may not know," 2007. [Online]. Available: https://www.sans.edu/cyber-research/security-laboratory/article/wireless-security-1

[27] MITRE, "Download cve," 2016. [Online]. Available: https://cve.mitre.org/data/downloads/index.html

[28] J. B. Lovins, "Development of a stemming algorithm," *Mechanical Translation and Computational Linguistics*, vol. 11, no. 1 and 2, 1968. [Online]. Available: http://mt-archive.info/MT-1968-Lovins.pdf

[29] M. Chaput, "stemming 1.0," 2010. [Online]. Available: https://pypi.python.org/pypi/stemming/1.0

[30] Rapid7, "Metasploit," 2010. [Online]. Available: https://www.metasploit.com/

[31] ——, "Vulnerability & exploit database," 2000. [Online]. Available: https://www.rapid7.com/db/

[32] Offensive Security, "Offensive security's exploit database archive," 2009. [Online]. Available: https://www.exploit-db.com/

[33] Inj3ct0r Team, "http://0day.today/," 2008. [Online]. Available: http://0day.today/

[34] Packet Storm Security, "Packet storm," 1998. [Online]. Available: https://packetstormsecurity.com

[35] N. Falliere, L. O. Murchu, and E. Chien, "W32.stuxnet dossier," Symantec Corporation, techreport, 2011. [Online]. Available: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[36] LIN Consortium, "Lin specification package revision 2.2a," 2010. [Online]. Available: https://www.cs-group.de/wp-content/uploads/2016/11/LIN_Specification_Package_2.2A.pdf

[37] MOST Cooperation, "Most specification rev. 3.0 e2," 2010. [Online]. Available: http://www.mostcooperation.com/publications/specifications-organizational-procedures/request-download/mostspecification-3v0e2pdf/

[38] FlexRay Consortium, "Flexray communications system protocol specification version 3.0.1," 2010. [Online]. Available: https://svn.ipd.kit.edu/nlrp/public/FlexRay/FlexRay%E2%84%A2%20Protocol%20Specification%20Version%203.0.1.pdf

[39] A. Porros, "Nuking and defending scada networks," 2010. [Online]. Available: https://www.noconname.org/files/presentaciones/2010/NocONName_2010-Nuking_and_defending_SCADA_networks.pdf

[40] Bluetooth SIG, "Specification of the bluetooth system," 2010. [Online]. Available: https://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiY76_but3UAhWDWBoKHXn_ARUQFggpMAA&url=https%3A%2F%2Fwww.bluetooth.org%2Fdocman%2Fhandlers%2Fdownloaddoc.ashx%3Fdoc_id%3D229737&usg=AFQjCNFY1IFeFAAWwimnoaWMsIRZQvPDSw&cad=rja

[41] ZigBee Alliance, "Zigbee specification," 2004. [Online]. Available: http://www3.nd.edu/∼mhaenggi/ee67011/zigbee.pdf

[42] ABR, NOBRIOT, JFR, and NTJ, "Z-wave networking basics," 2016. [Online]. Available: http://zwavepublic.com/sites/default/files/APL13031-2%20-%20Z-Wave%20Networking%20Basics.pdf

[43] etsi, "Etsi rfid," 2017. [Online]. Available: http://www.etsi.org/technologies-clusters/technologies/radio/rfid

[44] N. Sornin, M. Luis, T. Eirich, T. Kramp, and O. Hersent, "Lorawan specification," 2015.

[45] IEEE Computer Society, "Ieee standard for information technology - part 11: Wireless lan," 2016. [Online]. Available: http://standards.ieee.org/getieee802/download/802.11-2016.pdf

[46] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 2027–2051, thirdquarter 2016.

[47] IEEE 802.11, "Wep: The wired equivalent privacy algorithm," 1994. [Online]. Available: http://www.ieee802.org/11/Documents/DocumentArchives/1994_docs/1194249_scan.pdf

[48] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the key scheduling algorithm of rc4," *Selected Areas in Cryptography 2001*, pp. 1–24, 2001.

[49] T. Zillner and S. Strobl, "Zigbee exploited - the good, the bad, the ugly," 2015. [Online]. Available: https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly.pdf

[50] A. Francillion, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start system in modern cars," 2010. [Online]. Available: https://www.researchgate.net/profile/Srdjan_Capkun/publication/220333841_Relay_Attacks_on_Passive_Keyless_Entry_and_Start_Systems_in_Modern_Cars/links/541d6d520cf241a65a17df2d/Relay-Attacks-on-Passive-Keyless-Entry-and-Start-Systems-in-Modern-Cars.pdf

[51] S. L. Garfinkel, A. Juels, and R. Pappu, "Rfid privacy: An overview of problems and proposed solutions," 2005. [Online]. Available: https://pdfs.semanticscholar.org/41be/889e9949017ef8f0b360ff4e40c600d29c7a.pdf

[52] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," 2005. [Online]. Available: https://nslab.kaist.ac.kr/courses/2006/cs710/paperlist/security/35.pdf

[53] A. Abbasi and M. Hashemi, "Ghost in the plc: Designing an undetectable programmable logic controller rootkit via pin control attack," *Black Hat Europe 2016*, pp. 1–35, 2016.

[54] D. Urbina, J. Giraldo, N. O. Tippenhauer, and A. Cardenas, "Attacking fieldbus communications in ics: Applications to the swat testbed," *Proceedings of the Singapore Cyber-Security Conference (SG-CRC)*, vol. 14, pp. 75–89, 2016.

[55] Z. Basnight, J. Butts, J. Lopez, and T. Dube, "Firmware modification attacks on programmable logic controllers," *International Journal of Critical Infrastructure Protection*, vol. 6, no. 2, pp. 76–84, 2013.

[56] L. A. Garcia, F. Brasser, M. H. Cintuglu, A.-R. Sadeghi, O. Mohammed, and S. A. Zonouz, "Hey, my malware knows physics! attacking plcs with physical model aware rootkit," *NDSS Symposium 2017*, 2017.

[57] P. Wood, B. Nahorney, K. Chandrasekar, S. Wallace, and K. Haley, "Internet security threat report," Symantec Corporation, Tech. Rep., 2016.

[58] S. McClure, S. Gupta, C. Dooley, V. Zaytsev, X. B. Chen, K. Kaspersky, M. Spohn, and R. Permeh, "Protecting your critical assets - lessons learned from operation aurora," McAfee Inc., Tech. Rep., 2010. [Online]. Available: https://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf

[59] C. Wueest, "Targeted attacks against the energy sector," Symantec Corporation, Tech. Rep., 2014. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf

[60] E. Chien and G. OGorman, “The nitro attacks, stealing secrets from the chemical industry,” Symantec Corporation, Tech. Rep., 2011.

[61] J. DiMaggio, “The black vine cyberespionage group,” Symantec Corporation, Tech. Rep., 2015. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-black-vine-cyberespionage-group.pdf

[62] “Dragonfly: Cyberespionage attacks against energy suppliers,” Symantec Corporation, Tech. Rep., 2014, symantec Security Response. [Online]. Available: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf

[63] R. M. Lee, M. J. Assante, and T. Conway, “Analysis of the cyber attack on the ukrainian power grid,” *SANS Industrial Control Systems*, 2016. [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[64] “Threat landscape for industrial automation systems in the second half of 2016,” Kaspersky Lab, Tech. Rep., 2017. [Online]. Available: https://ics-cert.kaspersky.com/wp-content/uploads/sites/6/2017/03/KL-ICS-CERT_H2-2016_report_FINAL_EN.pdf

[65] B. Kesler, “The vulnerability of nuclear facilities to cyber attack,” *Strategic Insights*, vol. 10, no. 1, pp. 15–25, 2011.

[66] G. Sciacco, “Larmée de lair face à la menace dun ”cyber pearl harbor”,” *Res Militaris*, 2015. [Online]. Available: http://resmilitaris.net/ressources/10205/55/res_militaris_article_sciacco_arm_e_de_l_air_face___la_menace_d_un_cyber_pearl_harbor.pdf

[67] B. Bencsáth, G. Pék, L. Buttyán, and M. Félegyházi, “Duqu: A stuxnet-like malware found in the wild,” CrySyS Lab, Tech. Rep., 2011. [Online]. Available: https://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf

[68] B. Bencsáth, G. Ács-Kurucz, G. Molnár, G. Vaspri, L. Buttyán, and R. Kamarás, “Duqu 2.0: A comparison to duqu,” CrySyS Lab, Tech. Rep., 2015. [Online]. Available: http://www.crysys.hu/duqu2/duqu2.pdf

[69] C. Raiu, M. Amin Hasbini, S. Belov, and M. Sergey, “From shamoon to stonedrill,” Kaspersky Lab, techreport, 2017. [Online]. Available: https://securelist.com/files/2017/03/Report_Shamoon_StoneDrill_final.pdf

[70] G. McDonald, L. O. Murchu, S. Doherty, and E. Chien, “Stuxnet 0.5: The missing link,” Symantec Corporation, techreport, 2013. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf

[71] A. Cherepanov, “Win32/industroyer - a new threat for industrial control systems,” ESET, Tech. Rep., 2017. [Online]. Available: https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

[72] Shodan, “Shodan.” [Online]. Available: https://www.shodan.io/

[73] L. Rist, J. Vestergaard, D. Haslinger, and A. Pasquale, “Conpot.” [Online]. Available: http://conpot.org/

[74] Y. M. Pa Pa, s. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, “Iotpot: Analysing the rise of iot compromises,” *9th USENIX Workshop on Offensive Technologies (WOOT 15)*, 2015. [Online]. Available: https://www.usenix.org/conference/woot15/workshop-program/presentation/pa