Vulnerability scanners in OT networks: a quick overview

Jaime Souto Casares
jaime.souto@inprosec.com
InprOTech *(www.inprotech.es)*

The field of cybersecurity has a well deserved relevance into the operational design of any company or organization nowadays. While this is unanimously the case for Information Technology (IT) environments, the case is more complex when dealing with industrial settings, in what is called Operational Technology (OT). In this short overview, we illustrate this with a quick dive into the topic of vulnerability scanners in the context of OT networks.

I. INTRODUCTION

It is clear now, with one fifth of the XXI century already in our backs, that cybersecurity has become a critical aspect of the everyday life of companies, governments, organizations, and even citizens. Cyberthreats are clearly on the rise, with 2021 seeing an increase of 68 percent in data breaches with respect to 2020[1], and malicious users now having even more vectors of attack with the ever-expanding digitalization that the world is still experiencing. Compromising private data or hijacking devices, to name a few examples, are major threats that can potentially target everyone and cause great harm in the form of economic loss or personal distress, but they pale in comparison with an attack aiming to halt the normal operation of a water treatment plant, or a power station. When we move up to the industrial plane, even a single successful attack could in fact destabilize societies.

This worrisome realization goes in hand with the arrival of the Fourth Industrial Revolution, that is turning factories into networks of agents interconnected via the Internet Protocol (IP), also accessible from the outside for monitoring and control. This breaks the main protection of traditional industrial control systems (ICS) in two ways: isolation and the usage of proprietary control protocols[2]. In this regard, industrial plants are now vulnerable to the plethora of attacks known in IT environments, and oftentimes the typical solutions are not so easily implemented due to the more complex nature of OT networks.

And the trend is, in fact, that cybercriminals are widening their focus to include OT targets. Since 2010, when the infamous and highly sophisticated *Stuxnet* worm infected an Iranian nuclear facility in Natanz, damaging the centrifuges and delaying the national nuclear program, the number of cyberattacks on OT systems are far from an extraordinary occurrence. In fact, according to the *2021 State of Operational Technology and Cybersecurity Report* by Fortinet, more than 6 out of 10 organizations experienced three or more intrusions in their systems in 2021, and only 7% reported none[3].

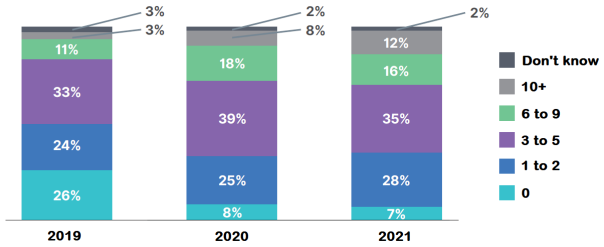

FIG. 1. Number of intrusions in the last three years as reported by OT managers. Data extracted from Ref. 3.

II. VULNERABILITY SCANNERS

As we mentioned before, the methods applied to protect an OT environment are different from the ones designed for IT, which is somehow conflicting with the current path of OT/IT integration driven by the Industrial Internet of Things (IIoT). Despite the endless possibilities that this technology enables (in terms of efficiency, security, and self-management), it is also undeniable that under this framework every OT element is a potential liability.

Last 2019, the Cyber Independent Testing Lab (CITL)[4], a non-profit organization with *"the mission of advising software consumers through expert scientific inquiry into software safety"*, presented a survey finding that more than 6,000 firmware versions from 18 vendors showed little to no improvement in security in the span of more than a decade (2003-2018)[5]. Moreover, there are several other ways in which OT/IT integration might be problematic[6]: (i) lack of communication between IT and OT manufacturers and developers, (ii) large lifespan of OT systems, without proper security updates, (iii) most OT systems are required to function on a 24/7 cycle, making it extremely cumbersome and/or expensive to stop them in order to perform security updates.

The strategy is, then, to use those security tools developed for IT systems but tailoring them so that they become useful (or, at least, not harmful) when given the task of looking at a modern ICS network. One of the main cybersecurity tools used in IT are vulnerability

scanners, a set of computer programs designed to test systems against known weaknesses, such as those collected in the CVE list (*Common Vulnerabilities and Exposures*) by MITRE[7]. Roughly speaking, one can split these scanning techniques in two categories: passive or active, depending on the level of engagement between the scanner and the scanned device.

A. Active Scanners

Active scanners are a staple in the IT-security toolkit, and some are routinely used in all kind of systems as SaaS (Software as a Service). Nmap, and its faster alternative Zmap, are two ubiquitous and open-source network scanner tools. Some other bulkier options with more options and functionalities are Nessus, OpenVAS (an open-source fork of Nessus), or Metasploit. In their core, they relay on sending packets and monitoring the response. The problem when applying them on OT elements, such as Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisiton (SCADA) systems, or Process Control Systems (PCSs), is that they can interact unexpectedly with the scanning packets, causing all sorts of malfunctioning behaviour, compromising the operation of the network and even the integrity of such devices. Some techniques consist on sending on purpose corrupted data to the devices, and while an IT network can easily recover from such an interference, that is not the case in an average OT facility. Moreover, many industrial protocols are very sensitive to latency and require precise synchronization, so just a simple network scan can be enough to disrupt the system. Some real-life examples drawn from Ref.8:

- A SCADA network operating on an array of robotic arms was subjected to a ping sweep while the controllers were on standby mode, causing one of them to perform a quick 180 degree turn. Fortunately, no one was on the 2.5 m reach of the arm.
- A similar ping sweep was trying to identify all hosts on a PCS network, halting a system responsible for the creation of integrated circuits, with an estimated loss of £50k.
- In a gas facility, an IT penetration test spilled into the SCADA system, resulting in the blockage of all gas pipelines for several hours.

Unfortunately, there is still a notable level of scarcity in the knowledge of how these industrial protocols actually work and interact with the scanners, making it impossible to draw predictions[9].

All these points illustrate why active scanners are considered inappropriate options for OT vulnerability management in general, and why many industrial companies decide to skip them altogether and use passive listening tools instead.

B. Passive Scanners

Passive scanners consist of a set of techniques of listening (*sniffing*) to the network, by mirroring a port in a switch or a Terminal Access Point (TAP), and extract or infer information just by looking at the packets being transferred, like version fingerprints or hints that reveal the operating system running on a device.

Being a much safer option for the stability of the network, it also comes with the price of a much more limited scope. Silent devices cannot be analyzed -as the adage says, *you cannot secure what you cannot see*[10]. It will require more time to gather enough information to make a picture of the situation, and more data will be generated that will need a larger filtering effort. It is also very hard to create a template applicable to any system; rather, one has to depend on the OT-administrator's expertise on actual the network, the devices running on it, its protocols, etc[11].

A common way to perform a passive scanner is with the combined usage of NetworkMiner, a packet analyzer, and p0f and FingerBank, two databases where one can map OS with several parameters of a TCP/IP connection and several implementations of DHCP, respectively. For some of the standard open industrial protocols, like Modbus or EthernetIP, one could directly read the exchanged frames after capturing them with tools such as tcpdump or Wireshark.

In the midst of the discussion of active and passive scanners in OT networks, some voices expressed their concerns about the actual passivity of the latter, claiming that the term was being using euphemistically and that it had evolved into something more akin to *asset visibility*. A quick list of some of the reasons:

- Not every switch is capable of mirroring the OT traffic. Even in those scenarios where it is indeed possible, it is not uncommon that the switch presents other severe technical limitations.
- Activating some protocols required for the passive scanner might enable vulnerabilities on the OT network.
- Some of the information given to the scanner has to be generated somehow because OT agents normally perform just the task that they were designed to perform, and not something unnecessary for the operation of the network like giving away their vendor, or serial number. The system has to create "fake traffic" in order to get some of this information.
- The scanner has to be able to read the traffic, but this might be challenging when almost everything is encrypted. Lifting the encryption would solve the issue, but for a heavy prize.

In summary, in order for a passive scanner to be somewhat useful some compromise has to be made, and strictly speaking the passiveness might be left behind in the process[12].

III. SUMMARY

In this short overview, we have offered a first dive into the topic of vulnerability scanners in the context of OT networks, stating the need for them in the first place, and going through the dangers and weakness of active and passive techniques, respectively.

As the field of cybersecurity in the industrial world evolves and matures, some narratives trying to break from the limited perspective of "active *versus* passive" are starting to see the light[13]. The path for such a transcendence move would be to cook, thanks to the accumulated experience, the right mix of techniques together with the application of fail-safe designs. After a couple decades, that some might label as *lost* in ICS security, it seems like the field is ready to take up the challenge of planning a balanced way to optimize the usage of every scanning techniques available.

[1] https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises.

[2] Guide to Industrial Control Systems (ICS) Security, http://dx.doi.org/10.6028/NIST.SP.800-82r2 (2015).

[3] https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-2021-ot-cybersecurity.pdf.

[4] https://sarah-zatko.squarespace.com/.

[5] https://securityledger.com/2019/08/huge-survey-of-firmware-finds-no-security-gains-in-15-years/.

[6] https://searchitoperations.techtarget.com/definition/IT-OT-convergence.

[7] https://mitre.org/.

[8] D. P. D. et al., Penetration Testing of Industrial Control Systems, Sandia National Laboratories (2005).

[9] E. Samanis, J. Gardiner, and A. Rashid, A taxonomy for contrasting industrial control systems asset discovery tools (2022), arXiv:2202.01604 [cs.CR].

[10] https://www.caba.org/wp-content/uploads/2020/11/IS-2020-150.pdf.

[11] K. C. et al., Vulnerability analysis of network scanning on scada systems, Security and Communication Networks (2018).

[12] http://www.industrialdefender.com/why-passive-network-monitoring-isnt-passive/.

[13] https://www.securityweek.com/active-vs-passive-monitoring-no-longer-either-or-proposition.