A Taxonomy for Contrasting Industrial Control Systems Asset Discovery Tools

Emmanouil Samanis
Bristol Cyber Security Group,
University of Bristol
Bristol, UK
manolis.samanis@bristol.ac.uk

Joseph Gardiner
Bristol Cyber Security Group,
University of Bristol
Bristol, UK
joe.gardiner@bristol.ac.uk

Awais Rashid
Bristol Cyber Security Group,
University of Bristol
Bristol, UK
awais.rashid@bristol.ac.uk

ABSTRACT

Asset scanning and discovery is the first and foremost step for organizations to understand what assets they have and what to protect. There is currently a plethora of free and commercial asset scanning tools specializing in identifying assets in industrial control systems (ICS). However, there is little information available on their comparative capabilities and how their respective features contrast. Nor is it clear to what depth of scanning these tools can reach and whether they are fit-for-purpose in a scaled industrial network architecture. We provide the first systematic feature comparison of free-to-use asset scanning tools on the basis of an ICS scanning taxonomy that we propose. Based on the taxonomy, we investigate scanning depths reached by the tools' features and validate our investigation through experimentation on Siemens, Schneider Electric, and Allen Bradley devices in a testbed environment.

1 INTRODUCTION

Asset scanning is the process of discovering and collecting information about all physical and logical assets connected to a network, often implemented with the use of scanning tools. Recommended as a practice in the *identify* stage of the NIST Framework [1], it is a key element of risk assessments – discover which assets are connected to the organization's network in order to identify known vulnerabilities and put in place mitigating actions. It is also the stepping stone for a defense strategy. Security teams require effective asset scanning tools to understand the potential attack surface as new devices connect to the network or, existing ones are updated or modified in response to particular business needs. It is a well-established practice in IT networks with many commercial and free/open-source tools available for the purpose. In recent years, as industrial control systems (ICS) responsible for running critical national infrastructures, such as water treatment, power systems, manufacturing and other industrial environments have expanded in use, specialist asset scanning tools have emerged for this new setting. This is particularly driven by increasing network connectivity of such systems, including to the wider internet (traditionally, such systems were air-gapped for security). Some of these are bespoke solutions for Operational Technology (OT) – a term often used to describe the controllers, sensors and actuators deployed in industrial settings.

Whilst a traditional IT system is largely responsible for handling the flow of information, an OT system is responsible for controlling and monitoring a physical, real-world process, with potentially catastrophic consequences if something goes wrong. OT systems can be vast and complex, consisting of thousands of specialized devices and numerous pieces of software, used for monitoring and interacting with such devices that grow over the years as new equipment is added. For these complex critical infrastructure architectures, asset scanning tools not only help with the auditing process for the industrial devices and identify where security improvements are needed (e.g., firmware updates) but also assist in the commissioning process of new equipment [18].

Reconnaissance is an important step for an attacker as described in ATT&CK matrix for enterprise which includes a knowledge base of adversary tactics and techniques [13].This step is the first in the planning phase of the ICS cyber kill chain, where adversaries actively or passively gather information to identify potential targets or exfiltrate abundant information (device properties or vulnerabilities) [9]. Asset scanning tactics and techniques are included in the discovery stage of the MITRE ATT&CK matrix for ICS, which shows, at various stages, the potential actions of an attacker's intrusion into an ICS network [14].

Furthermore, an ICS environment will often contain legacy devices (ICS equipment is designed to operate for decades with minimal interruption), which can experience issues when exposed to scanning activities, in particular, the packet-heavy approaches that are used in IT environments. For example, an older programmable logic controller (PLC) with a low powered CPU or poorly implemented network stack could be overloaded by the high rate port and service scanning behavior from a common tool such as Nmap, if used without due regard to such considerations [8]. Further, the use of real-time industrial communication protocols that expect a steady stream of data from ICS devices can be interrupted by the heavy network traffic communications caused by active scanning of such devices. Due to these issues, as well as the use of specialized communication protocols used in ICS settings, eg., S7comm, DNP3, Profinet, etc., asset scanning for ICS cannot simply be achieved by transposing IT asset scanning tools to OT environments [19]. This is particularly critical because the requirements in ICS are different than IT systems and focus on safety, reliability, robustness, and maintainability [3]. A violation of these attributes could result in human causalities, physical damage to the industrial process or large scale societal disruption of critical services. Therefore, asset scanning tools must not only support the specialized equipment and protocols but also account

for critical properties such as safety, reliability and real-time requirements.

Unlike IT environments where comparative analyses have been conducted [2], and despite the growing number of ICS asset scanning tools, there lacks an analytic framework to help understand and contrast the full spectrum of asset scanning techniques and methods for OT environments. The lack of such a framework – and systematic investigations based on such a framework – makes it difficult for asset owners to decide which tools may be suitable to their particular ICS environment, whether the suitable tools afford the required scanning depths and other features such as active or passive scanning (with the former having potential for disruption to legacy environments). This paper addresses this gap by:

- Introducing a taxonomy for ICS asset scanning tools, their various features and scanning depth levels. To our knowledge, ours is the first taxonomy proposed to date that enables systematic mapping, characterization and classification of the features offered by ICS asset scanning tools. The taxonomy – and the capacity to contrast tools afforded by it – will enable users to garner a more objective understanding of the potential applicability of tools within their infrastructures and suitability to requirements and safety considerations (e.g., potential disruption of industrial processes due to active scanning);
- Contrasting the features and functionality – as depicted in their documentation or implementation – of twenty eight free-to-use and shareware tools on the basis of the taxonomy. We choose free-to-use tools mainly because they are a better fit for small infrastructure operators who have limited resources. As investment in expensive commercial tools may not be an option for such resource stretched smaller companies [15];
- Evaluating these features in a realistic ICS testbed (See Section 5.1) to both establish the effectiveness of the tools' features and investigate their safe operation within real industrial networks. The experimental evaluation does not only provide an insight into the scanning depth and quality of each tool but also the risk it may pose due to active scanning and the effects of such scans on the production.

To our knowledge, we are the first to propose a taxonomy to compare and contrast ICS asset scanning tools and use it as a basis to compare (both analytically and experimentally) twenty-eight tools. Our analysis also provides a first baseline comparison of the features of the 28 tools we studied, enabling future analysis with regard to the baseline as these tools evolve or new tools come on the scene (as well as comparisons with commercial offerings in future studies).

2 ICS SYSTEM ARCHITECTURE

In Figure 1 we provide an example of a "typical" ICS deployment architecture. Often, the Purdue model is used to hierarchically categorize the architecture of an ICS [6], and does indeed map to our architecture. However, we provide a much more

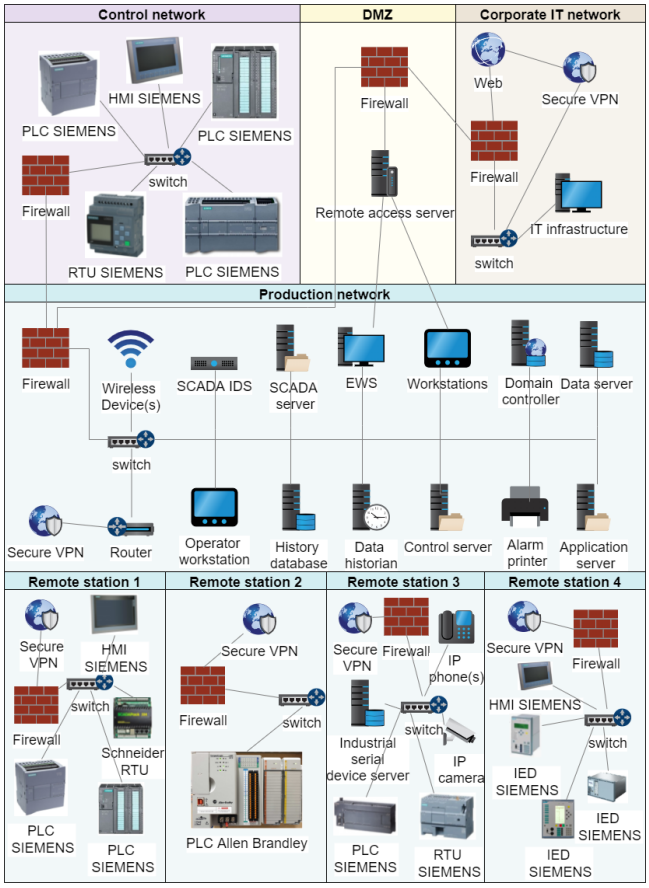

Figure 1: ICS/SCADA Architecture

detailed and realistic representation of the specific devices and systems within a typical ICS deployment compared to the high-level view of the Purdue model. Our example architecture highlights the challenges of asset scanning in industrial environments which would typically be even more complex and more connected—with hundreds of sites holding thousands of OT assets [10], both old and new. A typical ICS architecture includes several types of networks:

(1) Corporate IT network for management of basic plant functions; this includes a demilitarized zone (DMZ) where firewalls filter outgoing or incoming network traffic between corporate and ICS networks.
(2) The production network which offers overall monitoring and communication between supervisory control and data acquisition (SCADA) systems and industrial devices [19]. It collects information from field site devices in remote stations and is responsible for controlling the industrial processes through communication links which vary from telephone or power-lines to radio, microwave, cellular and satellite wide area networks. The production network includes SCADA systems, engineering workstations and data historians.