SoK: A Taxonomy for Contrasting Industrial Control Systems Asset Discovery Tools

https://doi.org/10.1145/3538969.3538979

Motivation

- ICS are large interconnected sites with thousands of assets
- Asset discovery, first step in securing industrial networks
- No information for asset scanning tools capabilities, features
- Manually created asset inventories, less visibility
- Vendor based tools not enough as multivendor settings exist
- Collection of assets information is a hard and tedious task

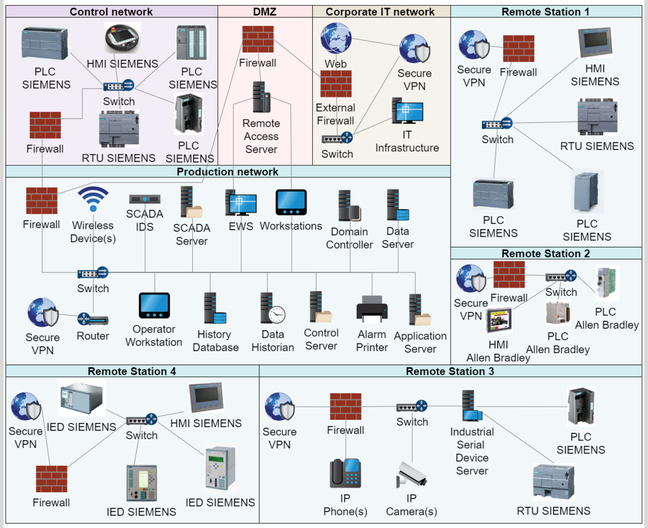
We provide in this work

- The first systematic feature comparison of free-to-use asset scanning tools
- An ICS scanning taxonomy
- Experimental results of testing 28 free-to-use asset scanning tools in University of Bristol testbed

Industrial Control Systems (ICS) characteristics

- Focus on safety, reliability, robustness and maintainability
- Responsible to control and monitor physical processes
- Large complex systems with old and new devices
- Unlike IT, ICS devices have real-time requirements

ICS/SCADA Architecture



Introduction to ICS asset scanning

Passive scanning	VS	Active scanning
Traffic collected and analyzed		Accurate scanning, more properties
No extra traffic but not accurate		Potential disruption from misuse

Asset scanning ICS devices using communication protocols

Identifying active IPs → Enumeration of ICS targets → Port scanning

ICS Active scanning method

Device Discovery → Service Identification → Vulnerability Identification

Taxonomy of ICS Asset Scanning Tools

Taxonomy mapping to scanning results

		SIMATIC	Modscan	Nmap	Plescan	Grassmarlin	NetworkMiner	Sophia	Lansweeper	SCADA-CIP	Wireshark	Nessus	OpenVAS	scada-tools	s7scan	Redpoint	ETTERCAP	OWASPNettacker	Unicornscan	nmap-scada	icsmaster	Modbusdiscover	scadascan	s7-info	plc-scanner	ICS-Hunter	ModbusScanner	ICSY	cyberlens
Specification	Bundled	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✗	✓	✗	✓	✗	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗
	Standalone	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓	✗	✓	✓	✓	✗	✗	✓	✓	✗	✓	✗	✓	✓	✓
	Commercial	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	Open source	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	Shareware	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	Freeware	✗	✗	✗	✗	✓	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
	Single target	✗	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✓	✗	✗	✗	✓	✓	✓	✓	✓	✓	✗	✓	✗	✗
	Wide target	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✓	✓	✗	✓	✓
	Single	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✓	✗	✓	✗	✓	✓	✗	✓	✓	✗
	Multiple	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	✓	✓	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✓
Execution	Passive	✗	✗	✗	✗	✓	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
	Active	✓	✓	✓	✓	✗	✗	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗
	Manual	✓	✓	✓	✓	✗	✗	✓	✓	✓	✗	✗	✗	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Automatic	✗	✗	✗	✗	✓	✓	✗	✓	✗	✓	✓	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	Interactive	✗	✓	✓	✓	✗	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗
	Point and click	✓	✗	✗	✗	✓	✓	✓	✓	✗	✓	✓	✓	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓
	Offline	✗	✗	✗	✗	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
	Real-time	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Port scanning	✗	✓	✓	✓	✗	✓	✗	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	ICMP scanning	✗	✗	✓	✗	✗	✓	✗	✓	✗	✓	✗	✓	✓	✗	✓	✗	✓	✗	✓	✗	✓	✗	✓	✗	✗	✗	✗	✗
	ARP scanning	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	Banner grabbing	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	Fingerprinting	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
	Automation protocols	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓
	Internet protocols	✗	✗	✓	✗	✓	✓	✗	✓	✗	✓	✓	✓	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
Output	1 Active IP address	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	2 Listening ports	✓	✓	✓	✓	✗	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✓	✗	✓	✗
	3 Protocol and service identification	✓	✗	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓
	4 Static device info	✓	✗	✗	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✗	✓	✗	✗	✗	✓	✓	✓	✗	✗	✓
	5 Deployment specific info	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗
	6 Vulnerability identification	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

✓ –> applicable | ✗ –> non-applicable

Industrial scanning insights

- Nmap based scanning scripts return more information for legacy devices vs newer models
- Passive traffic analysis tools provide less information about ICS devices in comparison with active scanning
- Many tools can reach output level 1-2 but few level 3-4 or 5-6
- Active scanning potentially can cause a failure state to devices, especially for legacy

Scanning Tools Overview

	EtherNet/IP	Profinet	Profibus	Modbus	Bacnet	S7comm	FINS	DNP3	FF	OPC UA	SNMP	Ethercat	HART	Version	Last Update
SIMATIC	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	v04.00.03	08-27-2021
Modscan	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	v0.1	06-01-2021
Nmap	✓	✗	✗	✓	✗	✓	✓	✗	✗	✗	✓	✗	✗	v7.9	03-10-2020
Plcscan	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	v0.1	06-01-2021
Grassmarlin	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	v3.2.1	27-06-2017
NetworkMiner	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	v2.7	15-06-2021
Sophia	✓	✗	✗	✓	✓	✓	✗	✓	✗	✓	✗	✗	✗	v3.5	03-01-2019
Lansweeper	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗	v9.0.10.2	30-09-2021
SCADA-CIP	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	v.1.0	06-03-2016
Wireshark	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	v3.4.9	06-10-2021
Nessus	✓	✓	✗	✓	✓	✓	✗	✓	✗	✓	✓	✗	✗	v8.15.0	15-06-2021
OpenVAS	✓	✗	✗	✓	✗	✓	✓	✓	✗	✗	✓	✗	✗	v21.04.0	16-04-2021
scada-tools	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	v1.0	26-04-2014
s7scan	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	v1.03	28-12-2018
Redpoint	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	v1.0	08-03-2016
ETTERCAP	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	v0.8.3.1	01-08-2020
OWASPNettacker	✓	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	v2.0	12-08-2021
Unicornscan	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	v0.4.7	30-05-2013
nmap-scada	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	v1.0	16-12-2013
icsmaster	✓	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	v1.0	04-01-2019
Modbusdiscover	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	v0.3	06-09-2018
scadascan	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	v1.0	26-10-2011
s7-info	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	v1.0	10-09-2020
plc-scanner	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	v1.2.1	06-07-2020
ICS-Hunter	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	v1.0	23-03-2020
ModbusScanner	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	v1.0	06-08-2017
ICSY	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	v1.0	19-04-2017
cyberlens	✓	✓	✗	✓	✗	✓	✗	✓	✗	✗	✓	✗	✗	v1.4	03-01-2019

✓ –> applicable | ✗ –> non-applicable

Key takeaways

- We establish the knowledge of the ICS scanning depths and the quality of information each tool can reach
- We created a Taxonomy is the basis for comparison and decision upon tools usage
- We demonstrated which tools are capable to be used in OT settings safely
- Identified the need for more OT-centric tools to cover the plethora of ICS protocols and devices
- Need for vulnerability scanner with respect on critical properties (safety, reliability)
- We hope that this study will help researchers and practitioners to have a means to contrast asset discovery tools before use against critical infrastructure
- We are in the process of performing a more detailed evaluation of these tools in a much more complex environment, utilizing the full OT network and a wider range of devices.

Manolis Samanis manolis.samanis@bristol.ac.uk
Joseph Gardiner joe.gardiner@bristol.ac.uk
Sridhar Adepu sridhar.adepu@bristol.ac.uk
Awais Rashid awais.rashid@bristol.ac.uk

AIRBUS

University of BRISTOL
Bristol Cyber Security Group