Real time asset inventory in ICS

Research Project 1, 2021

Supervised by:
Michel van Veen
Pavlos Lontorfos

Research project by:
Artemis Mytilinaios
Industrial Control Systems (ICS)

➔ Combination of control systems

➔ Used to operate and automate industrial processes.

➔ Types: SCADA/DCS
Identify an ICS asset

➔ Active scanning
   ◆ Probing the targeted device

➔ Passive scanning
   ◆ Collecting and analyzing information by sniffing network traffic

➔ Hybrid scanning
   ◆ Combination of Active and Passive
The Problem!

➔ Outdated network diagrams

➔ ICS components are fragile

➔ Active scanning can cause a lot of problems (e.g. Putting targeted devices out of service)

➔ Passive scanning collects small part of the device information
Research Questions

What are the added benefits of hybrid scanning compared to passive?
Research subquestions

➔ What are the problems that can occur by using hybrid scanning in ICS environments?

➔ How certain types of ICS devices behave under hybrid scanning and what are the problems that may arise in relation to these specific devices?
Components of ICS

➔ Programmable Logic Controller (PLC)
➔ Human Machine Interface (HMI)
➔ Remote Terminal Unit (RTU)
Related Work

➔ Adam Wedgbury et al.(2015)
  ◆ Problems that exist during an identification process on ICS.

➔ Mohammed Abdulrazzaq et al.(2018)
  ◆ Definition of asset identification in ICS.
  ◆ Introducing Hybrid scanning.

➔ Sergei Bantseev et al.(2003)
  ◆ Available tools for network scanning.
  ◆ No available tools that can do it all.
Methodology(1)

Created an ICS environment with the help of:

- OpenPLC
- Scada Br
- VMware Workstation
- Kali Linux

Conducted experiments using passive tool.
- Grass Marlin
Methodology(2)

Conducted experiments using hybrid approach, with the following combination of active and passive tools.

- Nmap
  - Modbus-discover
- Plcsan
- Scadascan
- Grass Marlin

Analyzed incoming information and document the state of the devices.

- Performance
- Availability
- Responsiveness
OpenPLC is an open source tool developed by Thiago Alves.[3] Aiming to **emulate** PLC programs in different environments.

Supports multiple programming languages.
- Ladder Logic (LD)
- Instruction List (IL)
- Function Block Diagram (FBD)
- Sequential Function Chart (SFC)
- Structured Text (ST)
Background: Scada Br

→ Open source tool.
  ◆ Aiming for development of Automation, Data acquisition and Human Machine Interfaces (HMI).

→ Useful tool for:
  ◆ Universities
  ◆ Automation professionals
  ◆ Technical schools
Background: Scanning tools(1)

➔ Grass Marlin
◆ Open source tool.
◆ Passively sniff network traffic.

➔ Plcscan
◆ Developed by Dmitry Efano[4]
◆ Discovers PLCs by scanning for Modbus/TCP protocol.
Background: Scanning tools (2)

➔ ScadaScan
   ◆ Written in Perl
   ◆ Identifies Modbus slaves
   ◆ Identifies Distributed Network Protocol 3 (DNP3) slaves

➔ Nmap
   ◆ Modbus-discover
Setup

→ Test environment

→ Scanning OpenPLC and Scada Br

→ Collected information and necessary results
Results(1)

➔ OpenPLC and Scada Br remained stable during the hybrid scan, using Plcscan and Grass Marlin.

➔ Hybrid scanning with Scadascan script and Grass Marling, also resulted to a stable operation.

➔ Modbus-discover script and Grass Marling (hybrid scanning) confirmed the continuous availability of the devices.
Passive scanning provided information regarding:
- Manufacturer
- ICS Protocol (Modbus)
- Role (Master/Slave)
- Operating System

Hybrid scanning also provided the above information with the following additions:
- Open port number, Unit ID (Plcscan)
- DNP3 slaves (ScadaScan)
- Slave ID data (Nmap: Modbus-discover)
Discussion

➔ The results indicate that
◆ Hybrid approach did not arise any fragility on the targeted devices.
◆ Hybrid scanning offered more information of the targeted devices compared to passive scanning.

➔ Limitations of this research:
◆ This approach was not tested on physical devices due to COVID-19 restrictions. → The results may differ when the experiments are conducted on physical devices.
◆ Only specific devices included in the research
What are the added benefits of hybrid scanning compared to passive?

➔ Collection of more details for the targeted devices.
➔ Variety of tools can be chosen for scanning.
  ◆ Flexibility to choose appropriate tools depending on the targeted devices.
Conclusion(2)

What are the problems that can occur by using hybrid scanning in ICS environments?

➔ Based on the virtualized environment that hybrid scanning was tested, no problems arose regarding
  ◆ Performance
  ◆ Availability
  ◆ Responsiveness
How certain types of ICS devices behave under hybrid scanning and what are the problems that may arise in relation to these specific devices?

➔ OpenPLC and Scada Br
   ◆ Stable operation
   ◆ No interruptions
Future Work

➔ Expand the scope of the research using physical equipment, like Siemens or ABB PLCs.

➔ Investigate what is the methodology of scanning that vendor’s tool use, and what are the possibilities of integrating these methods to the hybrid approach.
Thank you!

Research project by:
Artemis Mytilinaios

Supervised by:
Michel van Veen
Pavlos Lontorfos
Questions
References


