RSAConference2020

Learning Labs

HUMAN ELEMENT

Pentesting ICS 102

Write-up

In this workshop delivered at RSA Conference 2020, the goal of attendees was to learn how to attack PLCs by attacking ICS protocols: Modbus and OPC-UA. The session started by defining ICS and key vulnerabilities, then focused on PLCs and discovering how they communicate in order to learn the methods and tools that can used to p*wn them. Attendees experienced real-world scenarios by attacking PLCs on a dedicated setup featuring robot arms and a model train!

Arnaud SOULLIE – Manager – @arnaudsoullie

Alexandrine TORRENTS – Senior Consultant – @DrineTorrents

WAVESTONE

Table of Contents

Introduction to ICS

Industrial control systems (ICS) can be found in many places, across different industries.

An ICS interacts with the physical world and is composed of the production network (with sensors, actuators, PLCs and HMIs) and the supervision network (with SCADA servers, operators and engineering consoles).

In the IT vs. OT speech, it is better to leverage OT specificities that can be used to improve cybersecurity instead of blaming OT security: strong culture of quality and change management, safety often helps security.

What’s wrong with current ICS security?

There are 6 families of risks and vulnerabilities:

- Organization and awareness
- Lack of patch management
- Inexistent network segmentation
- Lack of third-party management
- Lack of security mechanism in equipment and protocols
- Lack of security supervision

However, the level of security is slowly evolving, and we tend to see some good improvements for most mature sites in some industries: creation of ICS cybersecurity sector, dedicated security equipment, systems patched on a regular basis for Windows environment, security requirements communicated to third-parties, etc.

ICS protocols and lab sessions

Modbus

Modbus is one of the standards for industrial communications. But there is no security: no authentication and no encryption.

The specificity of Modbus is that there is no object description. You will only get raw values to your requests, without any context.

Different functions are used by the Modbus protocol, the most used ones being the read and write requests on different types of parameters.

Lab session 1a

The goal of this session was to analyze a Modbus pcap file, understand the Modbus requests and responses and find the value of a specific register.

There are only a few requests, so it is easy to find values, however, there is no way of finding what the value represents for the industrial process.

Lab session 2a

The goal of this session was to discover the **mbtget** tool, a Perl script allowing to send Modbus read and write requests in command line.

In one line, you can specify the action (read or write), the register address, the number of values and the IP address of the PLC.

OPC-UA

OPC-UA is probably the future of ICS communications. Several security levels exist and allow signature and/or encryption. However, current implementations of this standard are mostly weak and only support the “None” security level.

OPC-UA uses a service-oriented architecture, with a node’s hierarchy and it is often simple to understand what is controlled by the node based on its name.

To get information on specific values, it is possible to subscribe to a node and receive updates on data change automatically.

Lab session 1b

The goal of this session was to analyze an OPC-UA pcap file, understand the OPC-UA traffic and find the node value that has been modified.

Compare to Modbus, there are a lot of packets and it can be hard to find what you are looking for. However, as names are used for nodes, you can look for packets that have an interesting name in the payload and then dig into the details of the packet to find the relevant information. Here, we could see a write request on Light@RobotController and by analyzing the value, we could figure out the light was turned off.

Lab session 2b

The goal of this session was to discover the **opcua-client** tool, a graphical tool allowing to connect to OPC-UA servers, browsing the hierarchy, subscribing to nodes and changing value on writable nodes.

Capture the flag

Once the tools (mbtget and opcua-client) had been tested on mock PLCs and SCADA servers, it was time to connect to the setup. The goal was to stop the train and capture the flag with the robot arm.

The first step was to identify the targets using nmap to scan the network on port 502 (for Modbus) and 12403 (for OPC-UA).

Once identified, mbtget could be used on Schneider PLCs to make the robots move and OPC-UA could be used to stop the train.

Takeaways

ICS are vulnerable and some vulnerabilities will never be patched. Indeed, protocols are insecure by design and once you get a network access, it can be relatively easy to compromise systems and mess with the industrial process.

Appropriate organizational and technical security measures are necessary to improve ICS security level.

But where to start?

- Know your ICS
- Limit your exposure
- Patch wisely
- Ensure business continuity