S7comm-plus Anomaly Detection

Abstract

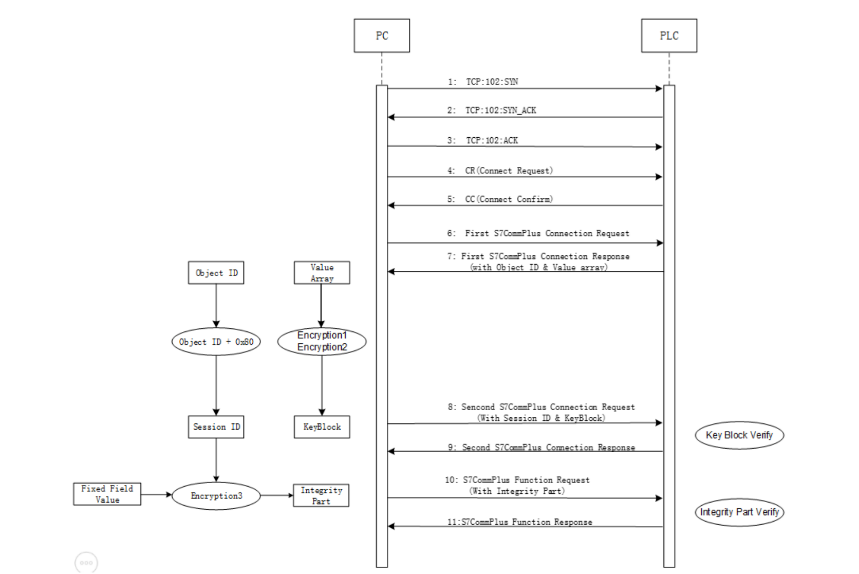
Cyber-physical systems are found in manufacturing and industrial systems, as well as critical infrastructures that play a crucial role in our society. The integration of standard computing devices and IP-based technology into cyber-physical systems increases the threat of cyber attacks. Also, traditional offensive defense strategies are often not feasible in industrial environments. This article focuses on the widely used Siemens S7 communication protocol and provides an approach for detecting anomalies in network packets by training a model with neural networks and applying the model to existing network traffic.

Introduction

We carried out our project by conducting tests at the Critical Infrastructures National Test Bed Center within Sakarya University. As we have stated, our aim is to reverse engineer s7comm and s7comm-plus, which are the communication protocol of Siemens Plc devices that are used at 50% of the world, and after making packet analysis, selecting the effective parameters and adding them to our data set, we will put them into machine learning, make various attacks and show the test results.

2. RELATED WORK

When we examine the S7comm-plus protocol, we see two main differences, unlike the s7comm protocol. First, in the s7comm protocol, all the information is uploaded and sent to a packet during communication, so that when the attacker analyzes the package, he has the chance to access and manipulate all the information. However, if it is in the s7comm-plus protocol, everything is carried in fragmented memory, cpu information, cpi information are all carried in separate packages. However, s7comm-plus encryption has an encryption system and we can summarize it with the following visual.

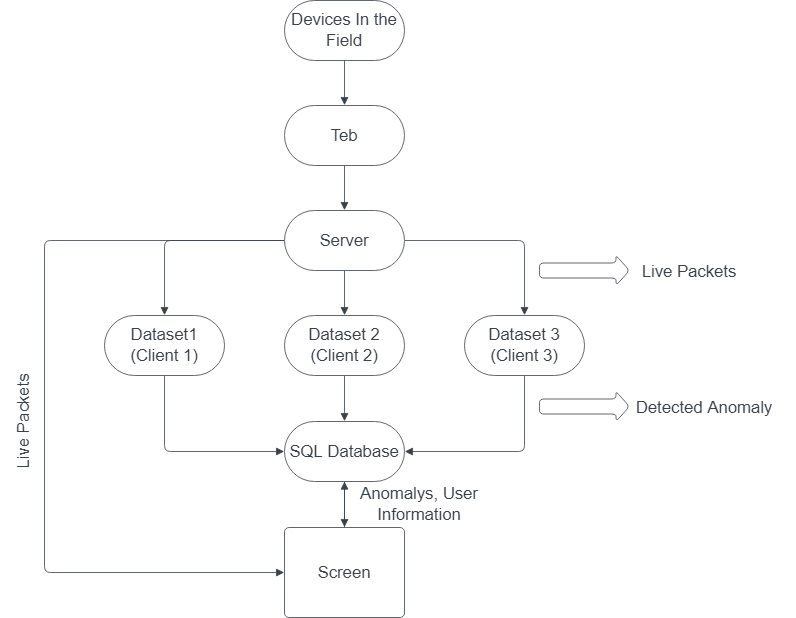


A vulnerability was identified on 05/2022 through the s7comm-plus protocol, which has become more secure in this way, and no vulnerability has been found at the moment.

3. EXPERIMENTAL SETUP

As the tools and libraries we use, we have installed SuperSimpleTcp, a c# nugget package for creating a server client, Microsoft.ML for machine learning, pcap nugget packages to listen to live packages, and completed our installations.

4. HOW DOES IT WORK?



As seen above, the server we have created collects packages and broadcasts live.

When each package arrives, it sends packets to port 9000 and c# programs where 3 different data sets are taught take the appropriate data to their own data sets and determine whether there is an anomaly in machine testing and record it in the SQL database. If an anomaly is recorded in the database in the Screen section, it shows it on the screen and shows the s7comm and s7comm-plus packages that are connected to the server and flowing live. A sample image of the program is as follows.

a picture with text, a screenshot, interior

Description automatically generated

In the right part, the Plc is pulled from the data in the relevant byte part of the functions in the request and response packets that the Plc flows are monitored live and discarded from the communication of the packets .

5. HOW DID WE DO IT?

Dos attack type detection data set:



Data set detected when sensors are manipulated:



Data set when counterfeit package is sent:



Microsoft.ml these data sets separately in C# projects, we added normal and anomaly states to the machine using the library.

And;

Dos attack accuracy rate : 98.35

Sensor intrusion accuracy rate : 96.36

Fake Packet attack type accuracy rate: 93. 87th

6. Conclusion

Securing of CPSs from cyber-attacks has highpriority for many industry facilities. While manyintrusion detection systems exist, they focus mainlyon network traffic behavior or perimeter security. Ourpaper proposes an supervised learning approach foranomaly detection in monitoring CPS network traffic.

References

* <https://attack.mitre.org/matrices/ics/>
* <https://www.blackhat.com/docs/eu-17/materials/eu-17-Lei-The-Spear-To-Break%20-The-Security-Wall-Of-S7CommPlus-wp.pdf>
* <https://media.defcon.org/DEF%20CON%2026/DEF%20CON%2026%20workshops/DEF%20CON%2026%20-%20Workshop-Alexandrine-Torrents-and-Arnaud-Soullie-Pentesting-ICS-101.pdf>