Intro:

I would like to extend my warmest welcome to all and express my sincere gratitude for your presence. Our topic is Use of AI in Operational Technology Networks and packet-based attacks detection.

About us:

Our Ph.D. team principally engages in research endeavours at Széchenyi István University. I would like to introduce our team members to you.

First, Head of Team is Dr Timot Hidvegi PhD. He is an associate professor at our University and IT security expert. The second member of our Team would be Szilard Laszlo Takacs PhD. student. The last member is me; my name is Zoltan Dobrady, also PhD student. Currently, I work as a software developer at Swarco Limited at Vienna. The current project is in line with our main research objectives. Our primary focus lies on cybersecurity, which we aim to enhance through the utilization of artificial intelligence.

Network overview:

Before we commence, it would be beneficial for everyone to possess a common understanding of what OT networks are.

As you can see on the picture on the right-side is an OT network. It is a network connection, that connects production devices such as robots, transfer bands, pumps, packaging machines, and other similar devices. The machines are usually controlled by PLC-s and they use this network to communicate with each other.

The picture on the left, shows an example of an IT network. The main difference between the two is, that IT networks are primarily local area networks and typically include PC-s, laptops, and server equipment. Neither modbus nor CAN bus protocols are used, and there is no PLC communication presence on the network.

Problem:

As you are aware from your personal experiences, it is imperative to note that any component that is connected to a network is also susceptible to vulnerability.

What is the meaning of 'vulnerable'? It can be attacked by someone outside of the organization. Unlike IT systems, these systems were not specifically designed, to safeguard against cyberattacks.

This is a main problem.

The second problem as we know recently, a prominent automobile manufacturer acknowledged the occurrence of a targeted cyberattack that resulted in the complete stop of production lines across Europe. Is just happened two weeks ago.

During my work on machine development, I have firsthand knowledge of the potential complications and danger that can arise when sending incorrect data packets to the peripherals. When someone maliciously sends manipulated data packets, the same thing happens.

Data packets that are travelling on the OT network are currently analysed manually. This is done by humans, and the analysis is only done after the attack has already happened.

Possible solution:

We will require a real-time data packet analysis in order to mitigate the threat. In this study, we attempted to employ artificial intelligence (AI) to identify unusual requests. By that, I mean requests that are not usual, or anything that is considered out of the ordinary.

Attacking mechanism:

The attack mechanism used essentially floods the Modbus server with a large amount of data, resulting in little to no resources left for the communication on the Client side.

The impact of this suboptimal execution environment is that the peripherals controlled by the Client slow down or stop altogether.

We monitored the system processes during the attack mechanism using the network packet analyser software called Wireshark, and the data streams were archived for each peripheral.

Virtual testing environment:

We used three virtual machines with standard Modbus Server/Client communication. A fuzzer was used in addition between the two devices. So, the third virtual machine was allocated to the fuzzer. Fuzzers are generally used for examining and testing applications/protocols. Fuzzers can be used to discover vulnerabilities and weaknesses in applications, making the implementation process easier. Therefore, signs of fuzzer usage should be monitored in an industrial network

A.I.:

It is a branch of computer science that aims to create smart machines capable of performing tasks that typically require human intelligence, such as visual perception, speech recognition, decision-making, and language translation. We used ai for data packet analysis.
We used two methods: Statistical learning, and Natural Language processing.

Preparing generated data for A.I.:

First, we needed to prepare data for training the A.I. After the virtual network was created, we wrote the software's for the communication between the server, the client, and the fuzzer. This generated the needed data packets which we used to train the AI. The generated data packets had to be labelled, and Irrelevant columns for the A.I. have been removed. For the natural learning model, we used word-based tokenization on the dataset. For the neural network tokenization was not needed. On the picture you can see the edited data, on the top is the before, and on the bottom is after the edit

Statistical learning mode results:

On this slide you can see the results, that the statistical learning model provided. which could be processed by the language models. Applied word-based tokenization on the 'data' column. Created embeddings to construct the training dataset.
You can see left on the table the different statistical model what we used, and on the right side is the accuracy score. After the cross validation the best model were Logistic regression, Support Vector Machine.

Naturel learning mode results:

As previously mentioned on the slide, here we have implemented the word-based tokenization on the dataset. We tested two naturel learning models, LSTM and 1D Convolution. These methods are no longer statistical learning models, they are called neural networks. We trained the models for over 20 epochs. We may have overfitted the systems, as you can see from the results. The data suggests that the system operates with an accuracy of over 99 percent; however, our experience tells us, that this is not feasible

Conclusion:

Finally, we have reached the conclusion page. Our investigation suggests that machine learning could offer a means of detecting cyberattacks. After conducting a thorough evaluation of various statistical learning techniques, it was determined that the S*upport Vector Machine, Naive Bayes, Logistic Regression,* exhibited the highest level of accuracy, averaging approximately 70 percent. Statistical learning algorithms may not possess sufficient accuracy to detect attacks on their own; however, when utilized in conjunction with other algorithms, they can enhance protection and enhance attack identification. The detection of data packets in neural networks requires substantial research to test and validate its performance in diverse environments. The final and most significant point is that cybersecurity is a significant concern that requires continual enhancement.

Thank you:

Thank you for your time. I appreciate the opportunity to speak with you today. I'll now answer any questions you have about topic. If you need any further information, feel free to contact me at (contact information).