**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 níder at Széchenyi István University. I would like to introduce our team membörsz to you.

First, Head of Team is Dr Timot Hidvegi PhD. He is an asszosziate professor at our University and IT security expert. The second membör of our Team would be Szilard Laszlo Takacs PhD. student. The last membör 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 lájz on cybersecurity, which we aim to enhance through the utilization of ártifisöl intelidzsensz.

**Network overview:**

Before we commence, it would be beneficial for everyone to posszesz a komön 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, pekedzsing machines, and other similör devices. The machines are usually controlled by PLC-s and they use this network to komjunikét 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 szörvör equipment. Nájder modbus nor CAN bus protocols are used, and there is no PLC communication prezensz on the network.

**Problem:**

As you are aware from your pörszönöl experiences, it is imperative to note that any component that is connected to a network is alszó szászzeptiböl 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 áknolidzsd 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 melisöszli sends manipulated déta peketsz, the szém thing happens.

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

**Possible solution:**

We will require a real-time déta peket analysis in order to mitigate the fret. In this study, we attempted to employ artificial intelligence to ájdenifáj ánjúzsual requests. By that, I mean requests that are not usual, or anything that is konszided out of the ordinary.

**Attacking mekenizem:**

The attack mekenizem used, esszensöli floods the Modbus szörvör with a large amount of déta, rezalting in little to no ríszorszesz left for the communication on the Client side.

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

We monitored the system proszessz during the ettekk mekenizem using the network peket enelájzer software called Wireshark, and the déta streams were örkájvd for each peripheral.

**Virtual testing environment:**

We used three virtual machines with sztenderd Modbus szörvör-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 or protocols. Fuzzers can be used to discover vulnerabilities and weaknesses in applications, making the implementation process easier. dherfór, signs of fuzzer júzedzs should be monitored in an indásztriál network

**A.I.:**

It is a branch of computer science that éjmsz to kríét smart machines kéjpöböl of performing tasks that tipikli require human intellidzsensz, such as visual perception, speech recognition, disszizsön -making, and language translation. We used AI. for déta pecket ennelizisz.

We used two methods: Statistical learning, and Naturel Language processing.

**Preparing generated data for A.I.:**

First, we needed to prepare déta for training the A.I. After the virtual network was created, we wrote the software’s for the communication between the szörvör, the client, and the fuzzer. This generated the needed déta peketsz which we used to train the A.I. The generated déta peketsz had to be lébölld, and irrelevönt columns for the A.I. have been removed. For the natural learning modöl, we used word-based tokenization on the détaset. For the nyúröl network tokenization was not needed. On the picture you can see the edited déta, on the top is the before, and on the báddom is after the edit.

**Statistical learning mode results:**

This slide shows the results of the statistical learning model. Kindly take note that we utilized multiple statistical models for testing purposes, as evident from the above. The table's top-left corner displays the various statistical models we employed, and the right side displays the accuracy scores. Furthermore, it is important to note that the accuracy scores of the various statistical models exhibit significant variances. Upon completion of the cross validation, the most effective models were Logistic regression and Support Vector Machine.

**Naturel learning mode results:**

As priviöszli mencsönd on the slide, here we have implemented the word-based tokenization on the détaset. 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 szudzsesszt that the system operates with an accuracy of over nájti nájn percent; haoever, our experience tells asz, that this is not fíziböl.

**Conclusion:**

Finally, we have reached the conclusion page. Our investigation szudzseszt that machine learning could offer a means of detecting cyberattacks. After kondákting ö thöróv eváljuéjsön of veriösz statistical learning techniques, it was ditörmind that the S*upport Vector Machine, Naive Bayes, Logistic Regression,* exhibited the highest level of accuracy, avöredzsing approximately szeventi pörcent. Statistical learning algorithms may not pozesszesz száfisönt accuracy to detect attacks on der own; ; haoever, when utilized in kondzsáksön with other algorithms, they can enhance protection and enhance attack ájdenifikésön. The detection of data packets in nyúrol networks requires szábsztensöl research to test and validate its performance in dájvörsz 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 standing here today. I’ll now answer any questions you have about the topic. If you need any fördör information, feel free to contact me at the given contacts. I leave it here for seconds should you want to write it down.

Thank you again, and enjoy of the upcomming presentations. Good bye