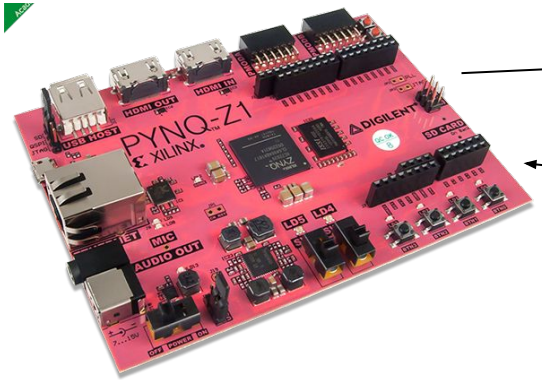
cybereason®

Boston University
Electrical & Computer
Engineering

Who Are We?

A group of 5 Computer Engineering Seniors just trying to graduate that hope you like this presentation

What is CyberTap?



A network tap that provides a way to continuously generate and store metadata from Industrial Control System (ICS) network traffic.

Boston University
Electrical & Computer
Engineering

Why Does CyberTap Matter?

Cyberattacks are becoming more and more prevalent

CyberTap provides a clear and lossless traffic record for security analysis in the event of a malicious attack

CyberTap

What's the Point?

Our client - a cybersecurity company with limited accessibility and visibility into their customers' network traffic

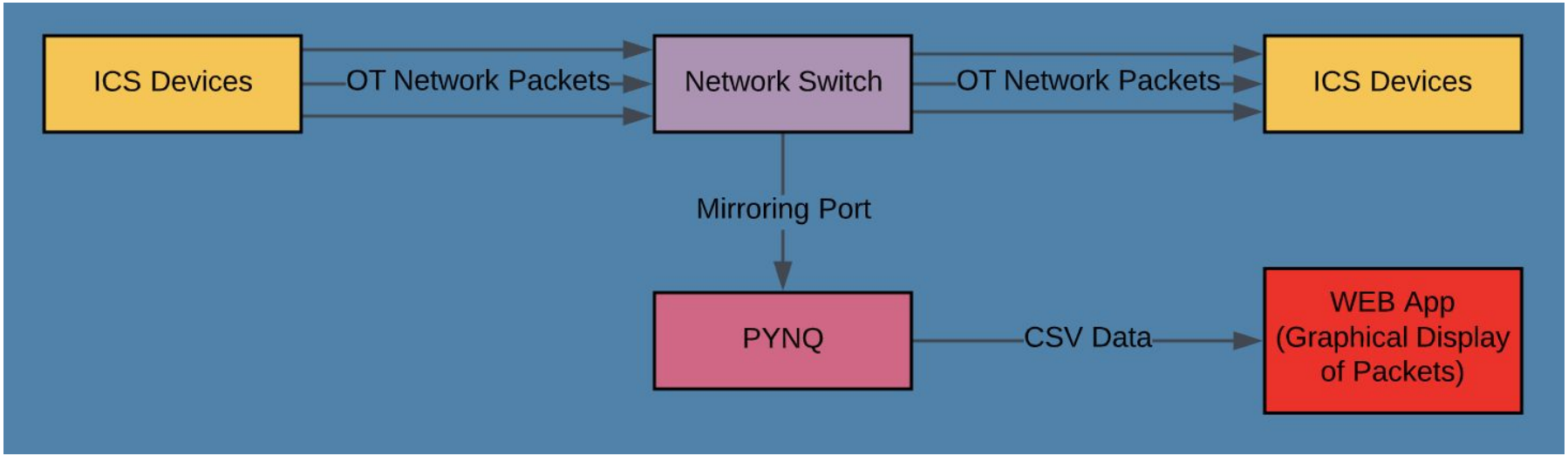
CyberTap comes in and can be used by

1. Mirroring a dedicated port on the network switch to receive directed traffic
2. Plug CyberTap into the port
3. Start main application via bash script
4. View network traffic via web app

CyberTap

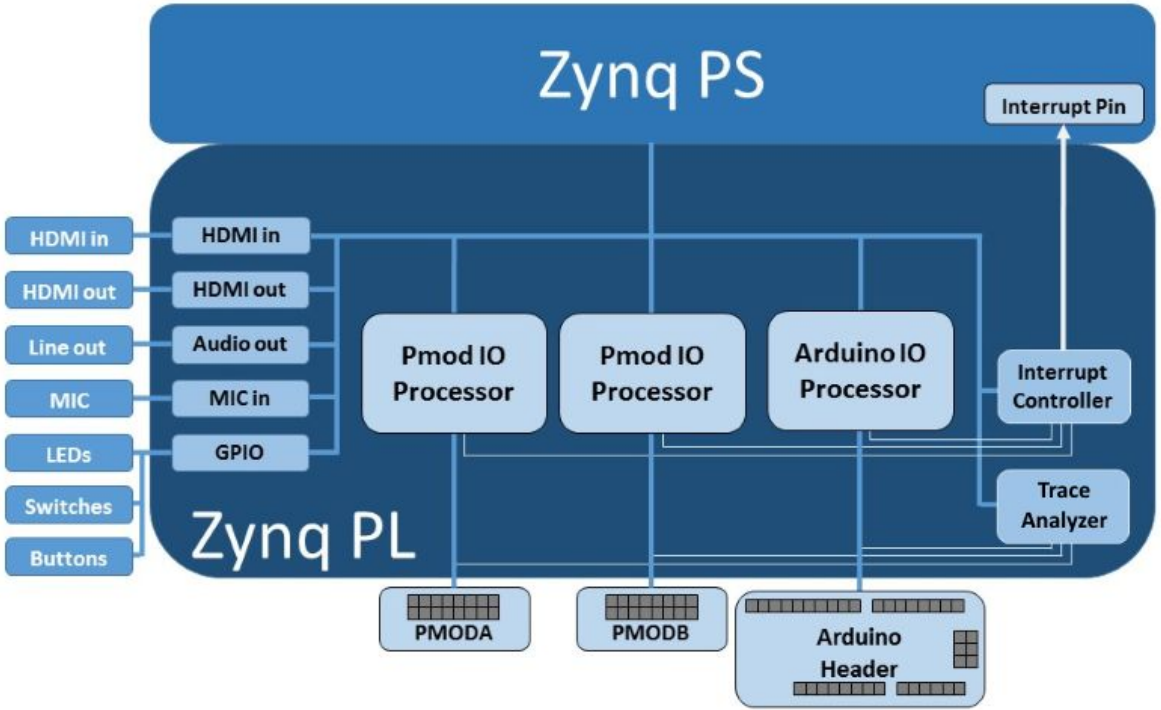
Boston University
Electrical & Computer
Engineering

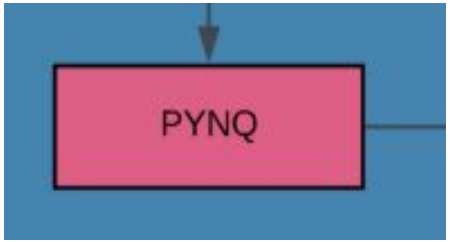
How Does It Work?



CyberTap

Our Board: PYNQ

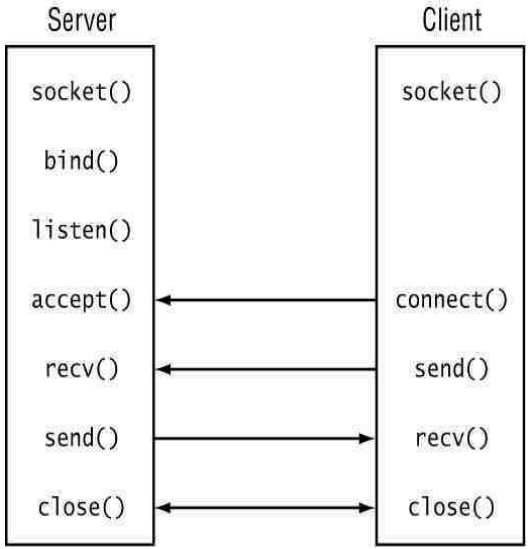




PYNQ's Python overlay allows for easy interaction between software and hardware elements of the system

How Do We Receive the Packets?

"A **socket** is one endpoint of a two-way communication link between two programs running on the network"

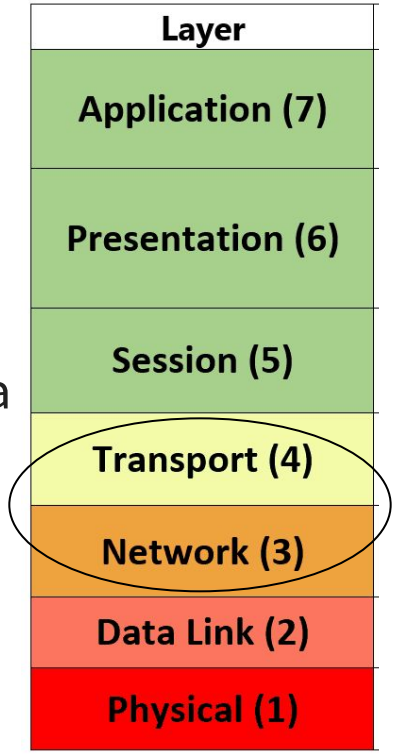


Raw Socket Sniffing

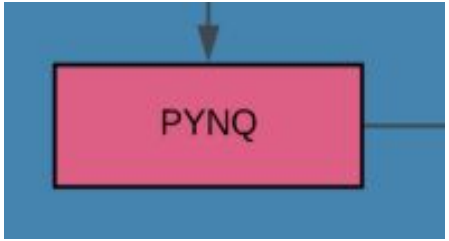
By opening a socket all data sent to the PYNQ from the switch will be seen

Socket == Doorway

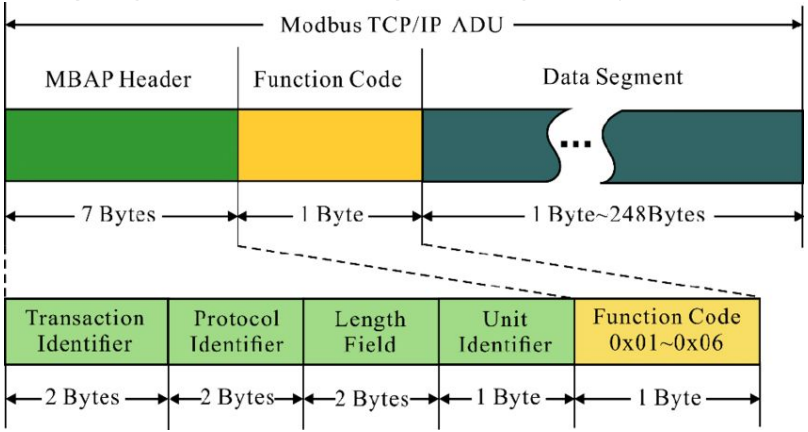
All data received in hexadecimal values

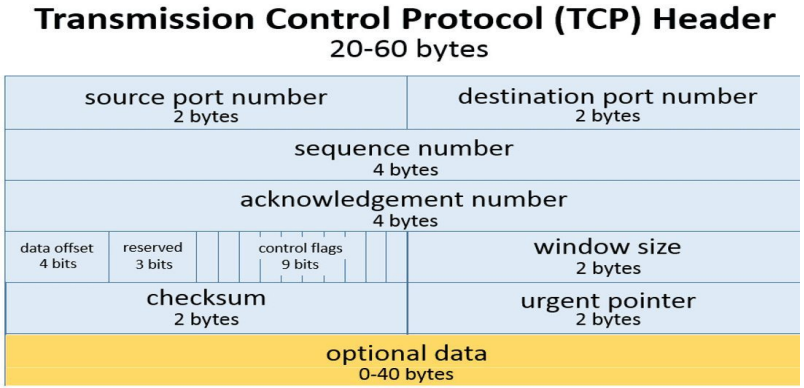


How Do We Parse the Packets?



Accomplished by converting the header data of the packets received in the raw socket (from hex) to the needed metadata (source, destination, etc). Payloads remain in hex form.





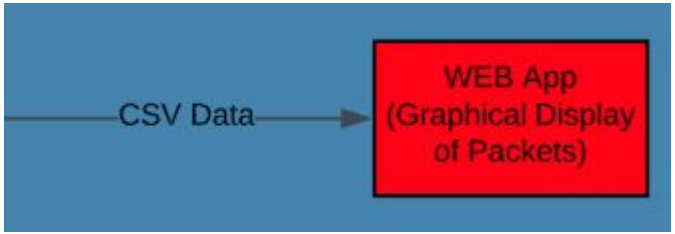
CyberTap

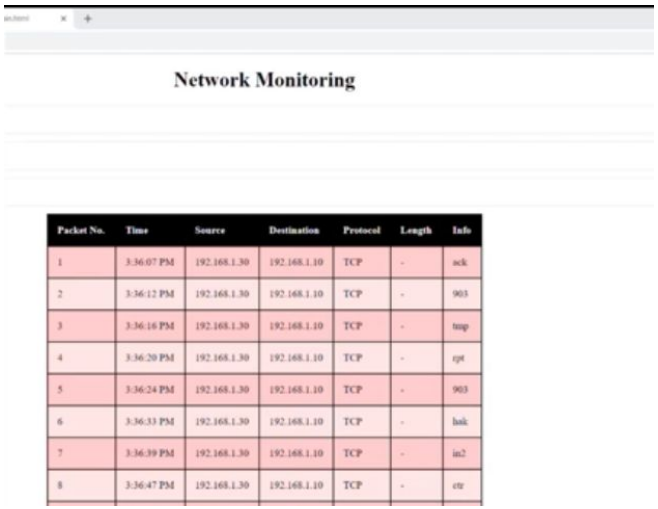
How Does the Web App Work?

Provides a soft real time look into the network activity

Reads from a CSV file and users can search through their packets

Hosted off board

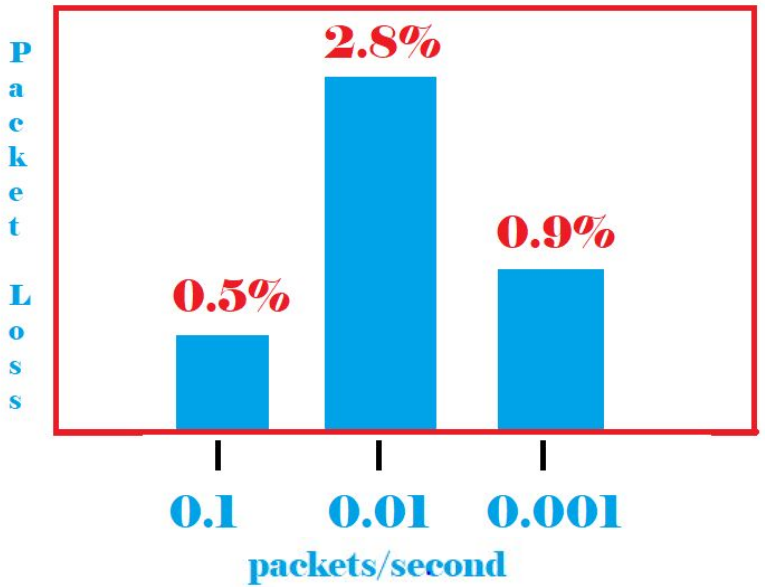




What Were Our Results?

The following results are from 2/20/2020:

Test 1:
3 trials pinging 1000 packets at different intervals



Web App:
Are the packets and their information corrected displayed?
Yes.

Test 2: Modbus
Does the web app correctly label the packets as TCP packets? Yes.

What Do We Want You To Remember?

The **purpose** of CyberTap is to provide a long-term solution to enable retroactive network data analysis.

Cyberattacks may be planned months in advance – prevent the next stuxnet!

Boston University
Electrical & Computer
Engineering

The End.

CyberTap