black hat®

EUROPE 2017

DECEMBER 4-7, 2017

EXCEL / LONDON, UK

#BHEU / @BLACK HAT EVENTS

EXFILTRATING RECONNAISSANCE DATA FROM AIR-GAPPED ICS/SCADA NETWORKS

David Atch & George Lashenko

CyberX

Trusted. Industrial. Cybersecurity.

Introduction

Introduction

David Atch

- VP/Research for CyberX
- Military service as the Team Leader in the IDF CERT
- Focused on reverse engineering & malware hunting

George Lashenko

- Security Researcher at CyberX
- Military service in the intelligence unit of the IDF
- Focused on reverse engineering & uncovering ICS zero-day vulnerabilities

Tal Kaminker

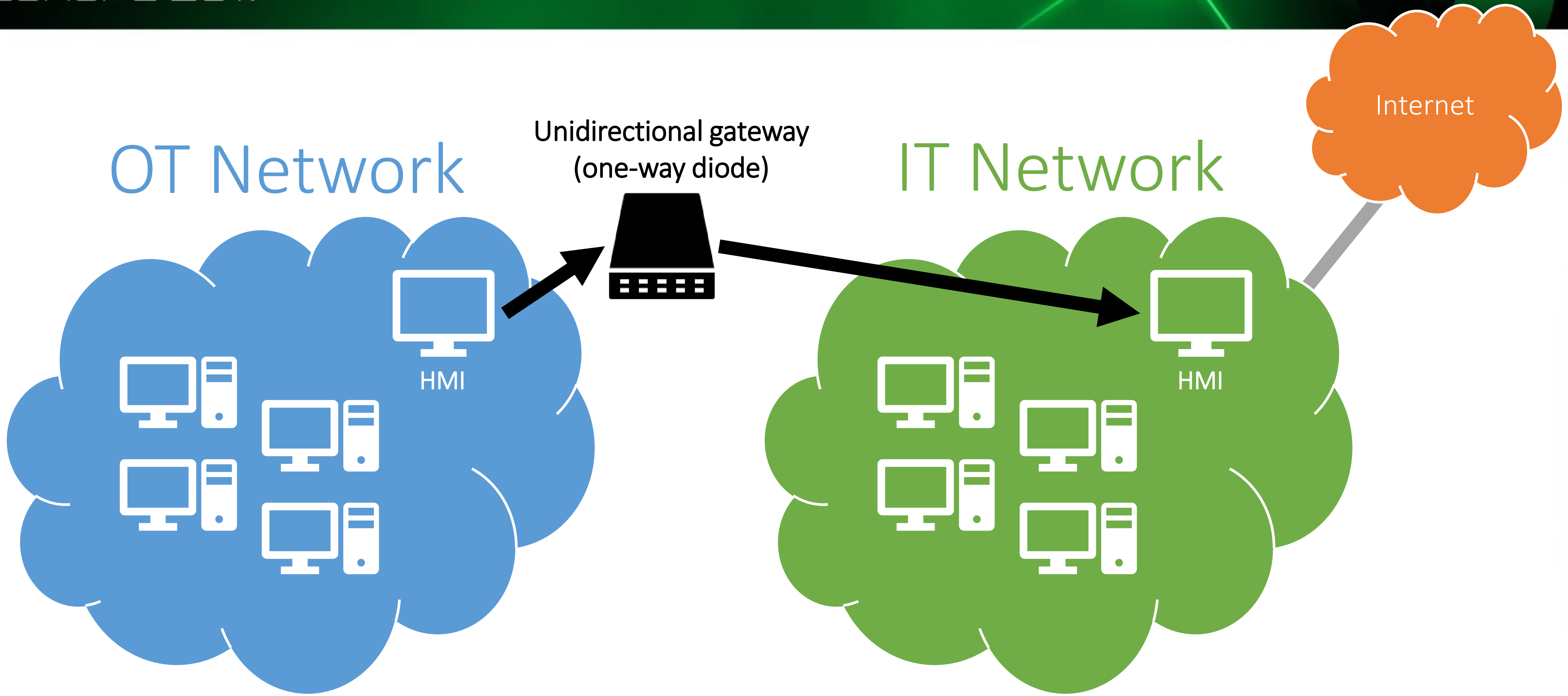
- ML Researcher at CyberX
- PhD student in Computer Science
- Focused on Machine Learning & modeling ICS behavior

Agenda

- Ways to get inside OT networks
- Challenges in exfiltrating data from air-gapped networks
- A few words about Ladder Logic
- Our method for exfiltrating data
- How we achieved it
- Demo

OT networks and how to get inside them

Air-Gapped Industrial Network



Air-Gapped Networks from the Attacker's Perspective

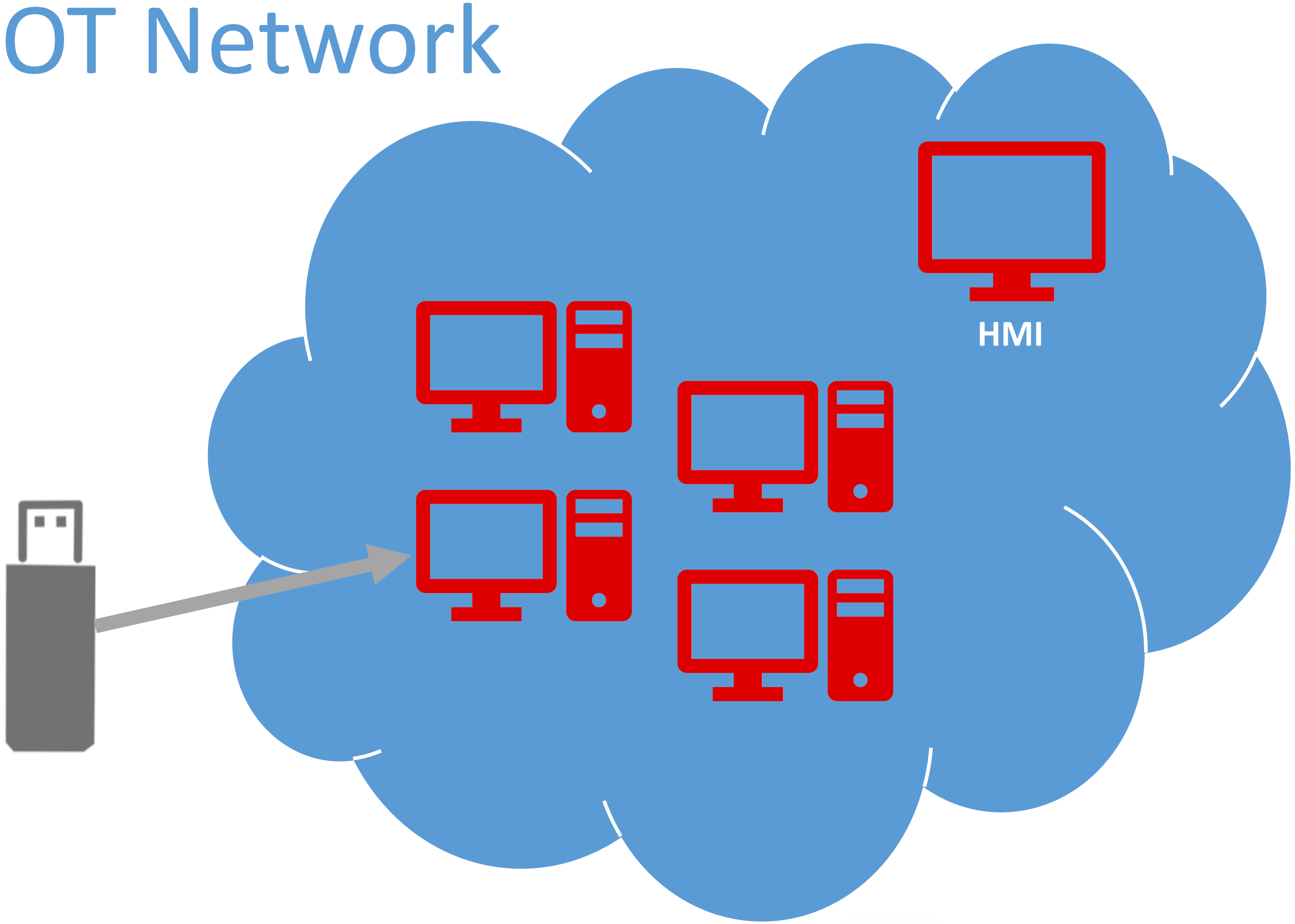
- Hard to get in
  - Not impossible
- Harder to get out
  - Also not impossible

Air-Gapped Networks from the Attacker’s Perspective

- First reconnaissance stage has to collect these things:
  - Network device mapping
  - Security product mapping
  - Device types and firmware versions
  - Ladder Logic programs
  - Schematics and design documents to understand device importance
  - Overall working patterns of the users/devices

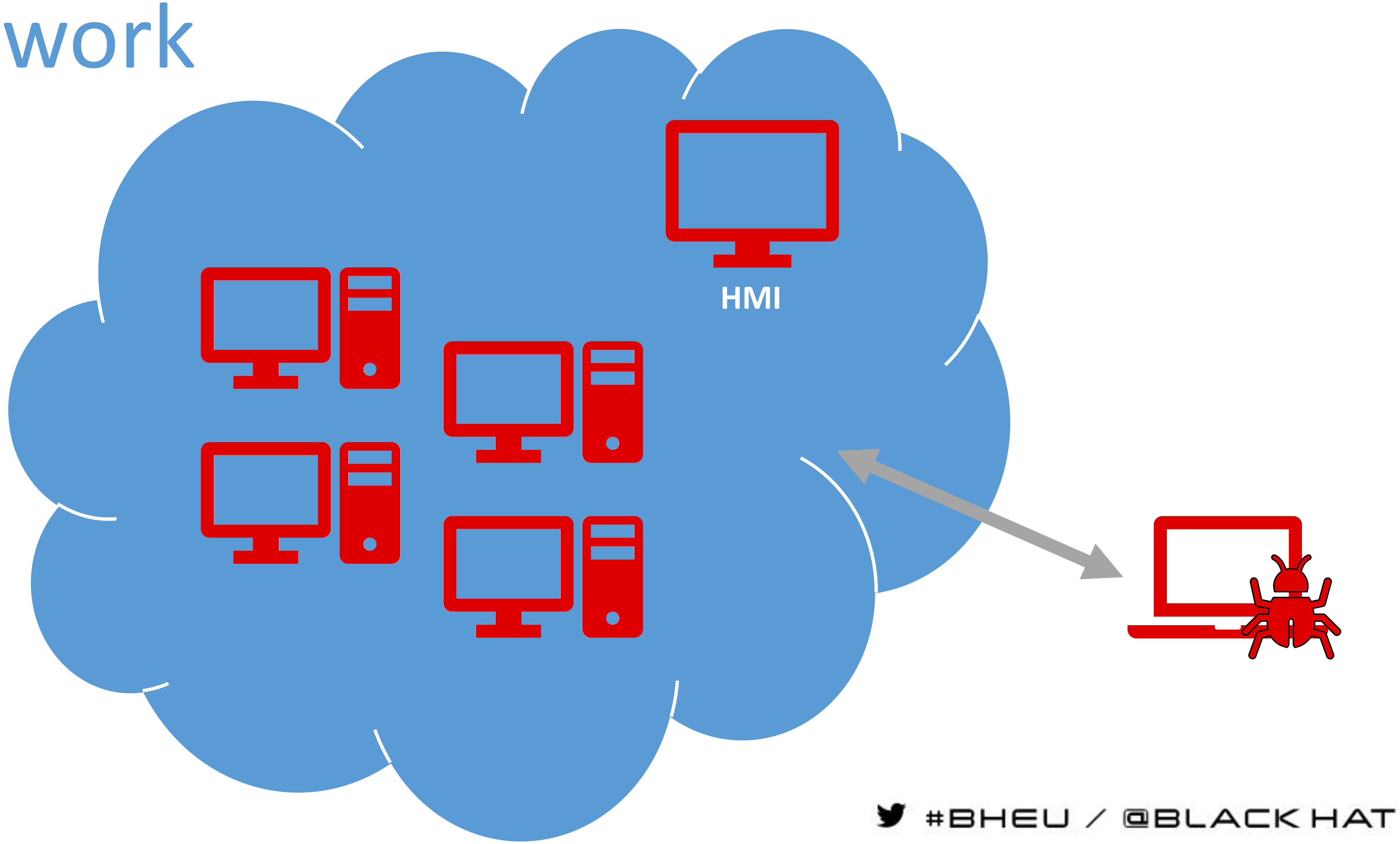
What are the attack vectors?

Attack Vectors: Malicious USB



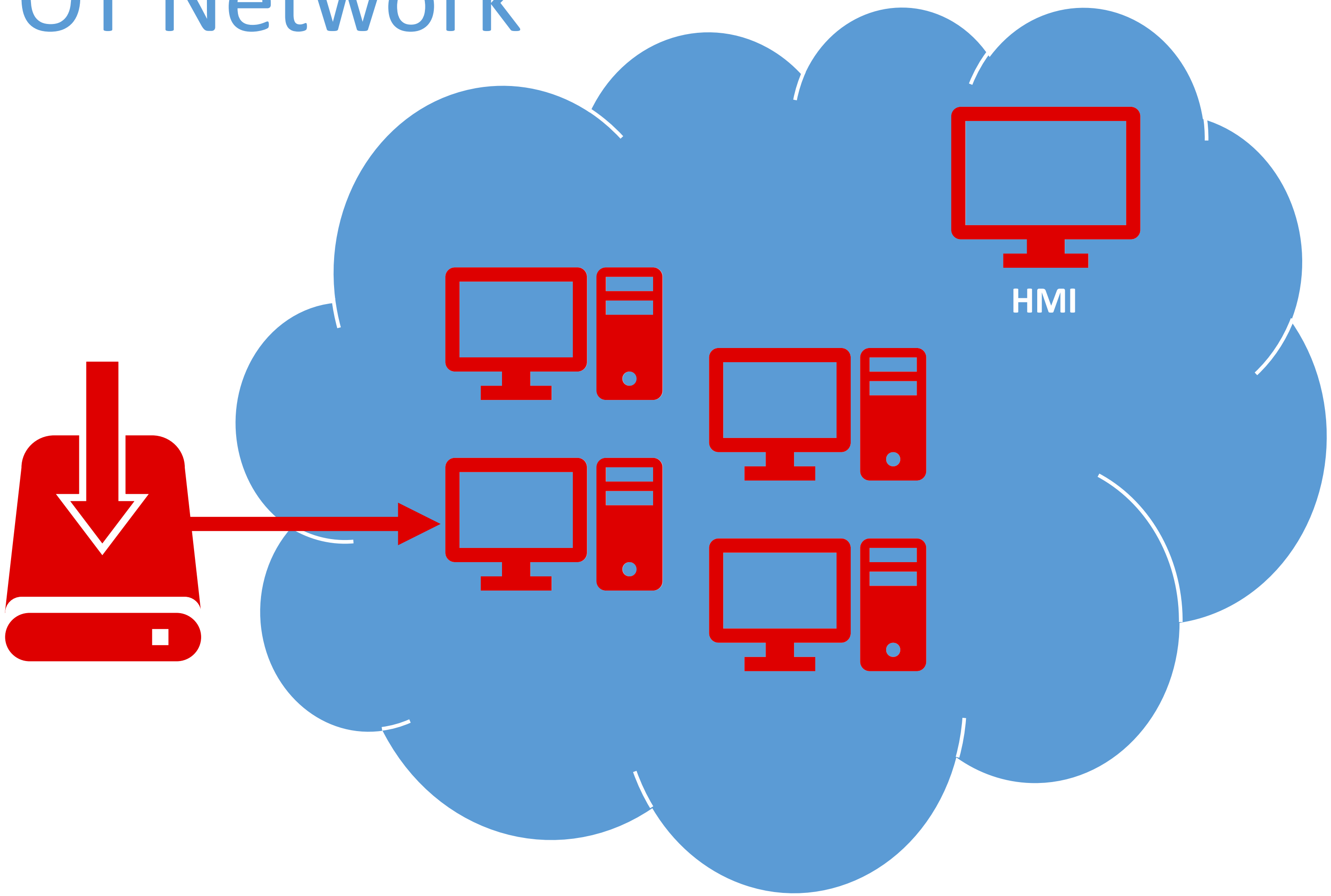
- autorun.inf – Enabled by default on Windows XP (still widely used in OT networks)
- LNK exploits – Used also by Stuxnet
- DLL Search Order Hijacking

Attack Vectors: External Engineering Laptop



Attack Vectors: Infected Vendor Updates

OT Network



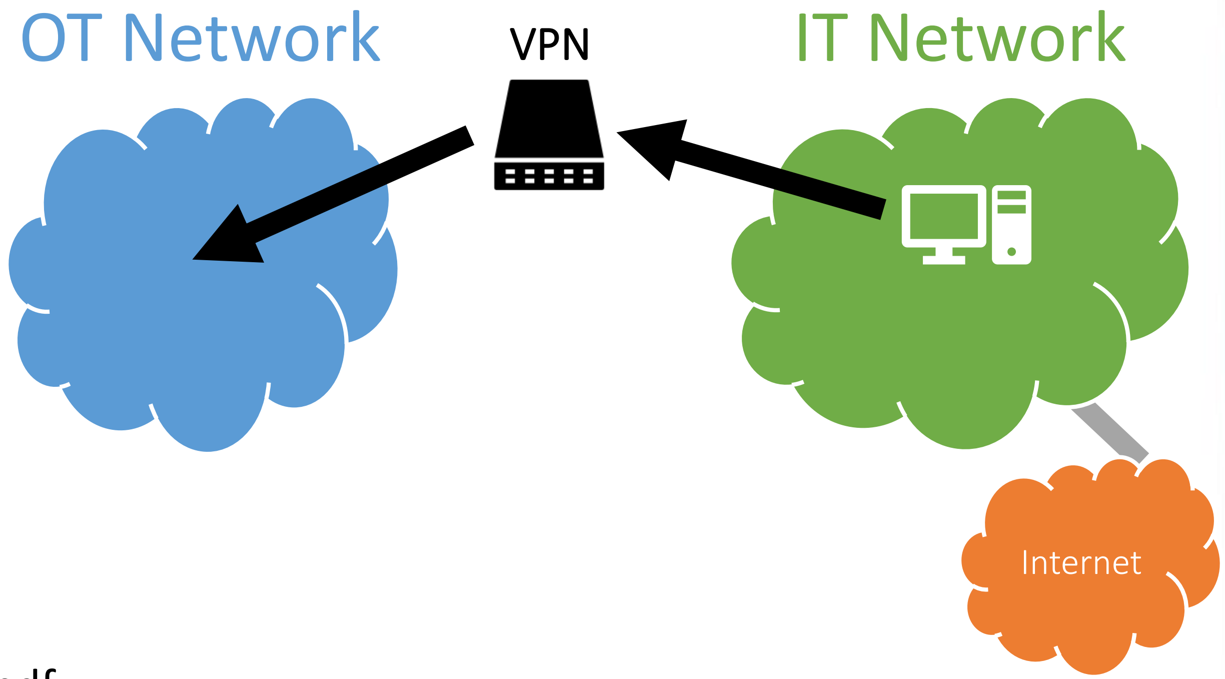
- NotPetya – Malicious update of Ukrainian financial software
- Dragonfly/Energetic Bear – Malicious updates (containing Havex Trojan) of ICS software from three separate ICS vendors

https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A

Attack Vectors: Stolen Remote Access Credentials

1st attack on Ukrainian electric grid (Dec. 2015)

- Phishing attack via IT network
- RAT installed on engineer's PC
- Theft of privileged credentials
- Entered OT network via trusted VPN connection



https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Exfiltrate Collected Data

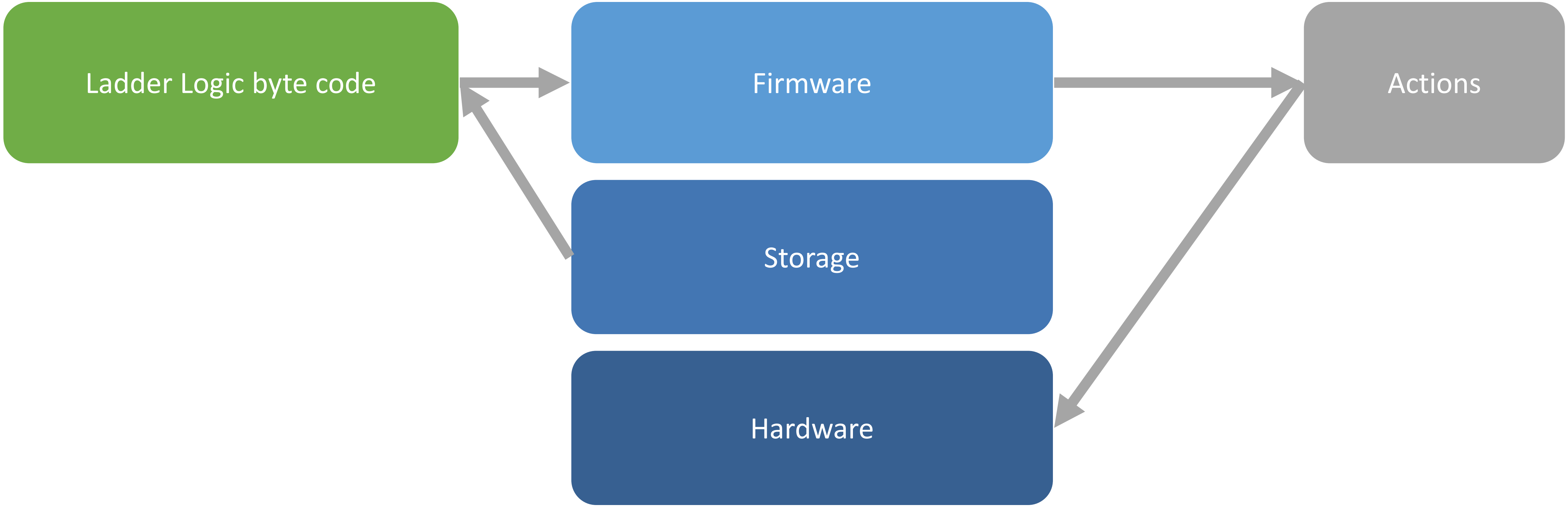
- Wait for the laptop to come back and communicate with the malware
- Wait for same/other USB to connect back to the network and exfiltrate through it

Exfiltrate Collected Data: Challenges

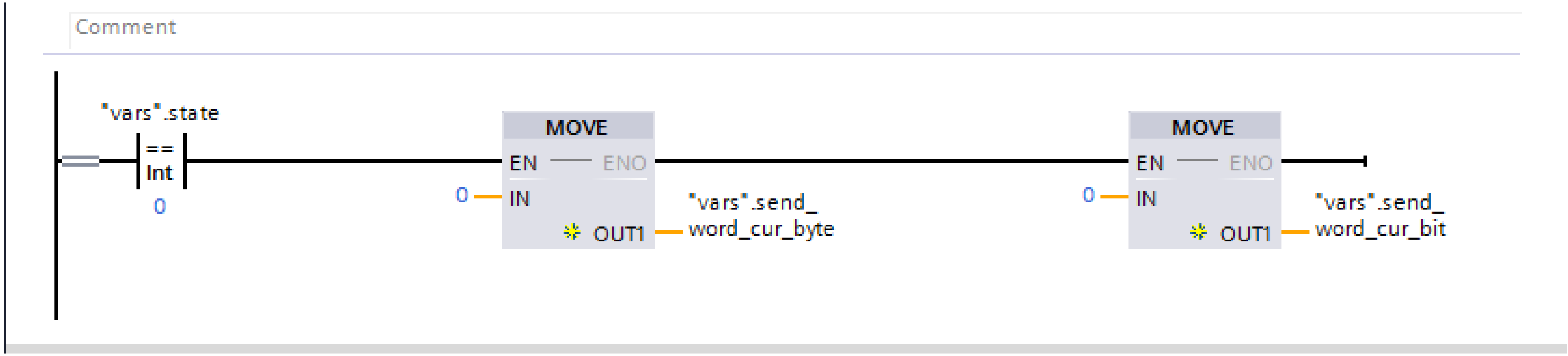
- Might take a long time for the malicious relay to connect back
- Increases risk that operation will be detected

Ladder Logic

PLC Structure



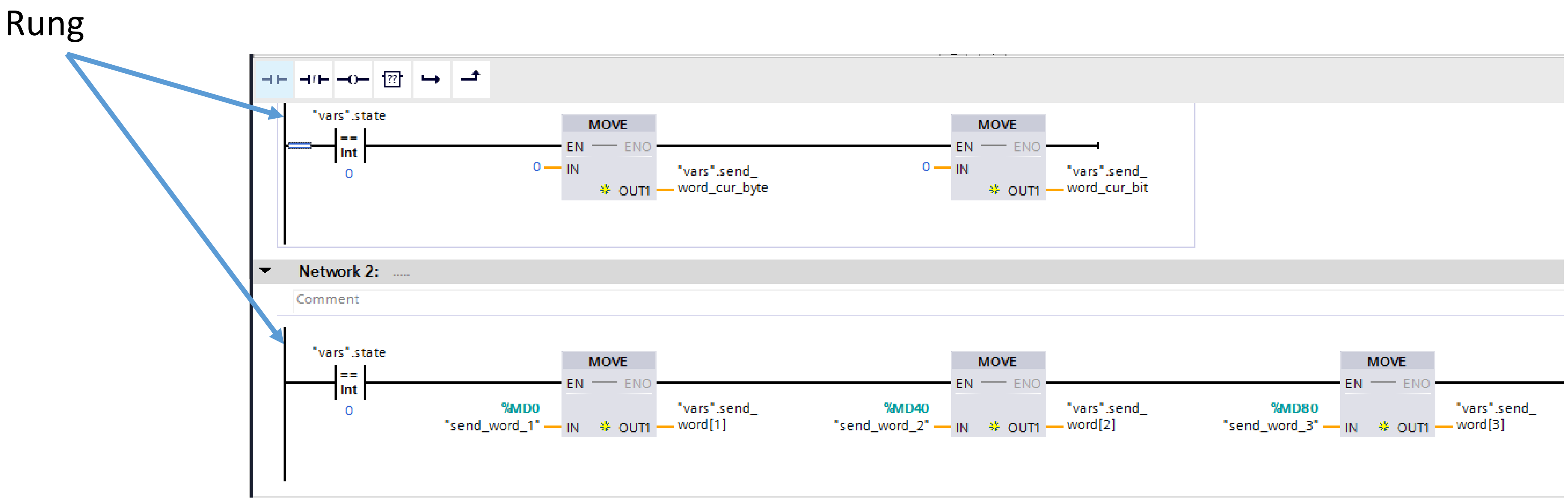
Ladder Logic Example



```
If vars.state == 0:
    move(0, vars.send_word_cur_byte)
    move(0, vars.send_word_cur_bit)
```

black hat EUROPE 2017

Multiple Rungs Example

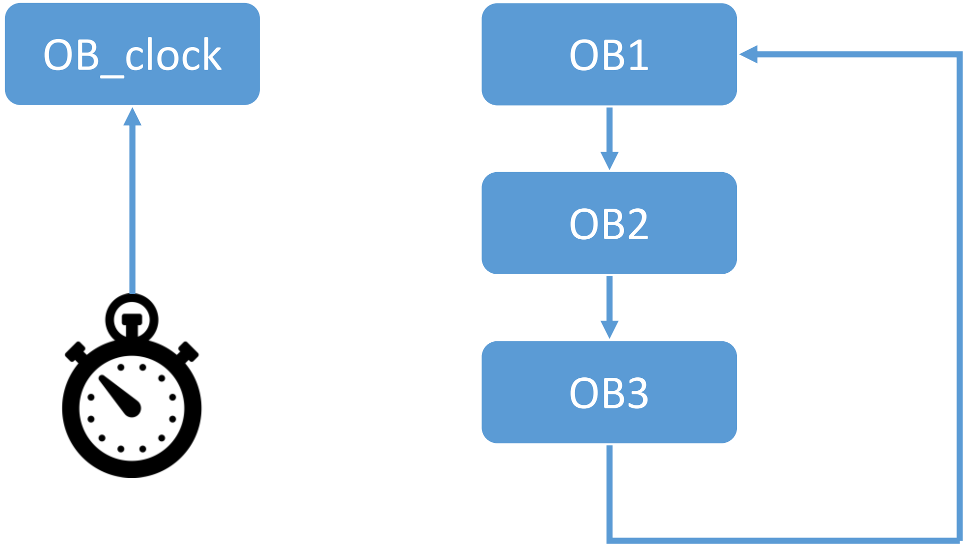


Block Types

- Ladder logic is organized in blocks
- Block types:
  - Organization Block (OB)
    - Main
    - Executed cyclically
  - Function Blocks
    - Code reuse
  - Data Blocks
    - Variables

OB Blocks

- OB Blocks
  - Cyclic execution (“parallel”)
  - Execution by event
    - Network error,…
  - Execution in a timer
    - Every x seconds

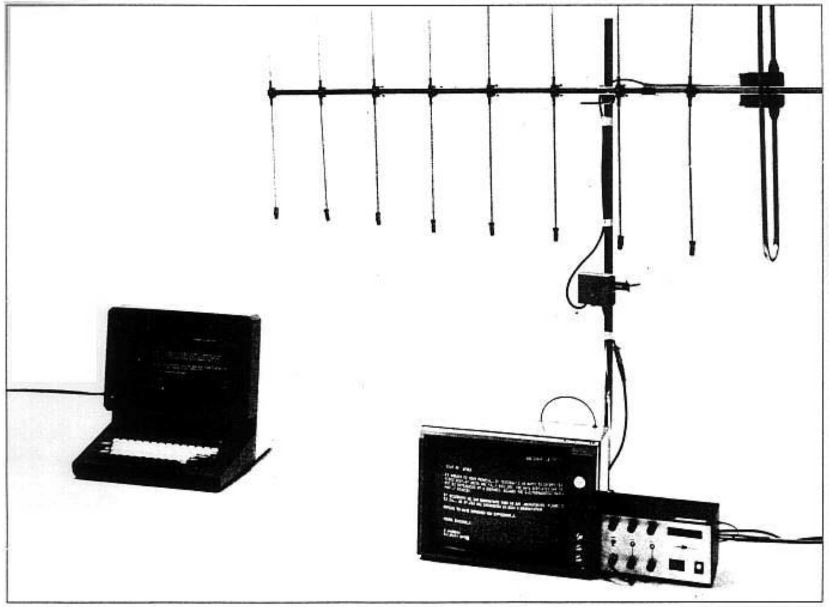


Why exfiltrate with ladder logic ?

- Why exfiltrate with ladder logic ?
  - Detection
    - Antivirus don’t examine ladder logic
  - Persistency
  - Previous research showed that Ladder Logic may act as reconnaissance malware
    - Scan the network, gather other ladder logic, gather configurations
    - Look for security products
    - Monitor work hours
  - Exploits
    - EthernalBlue, ..

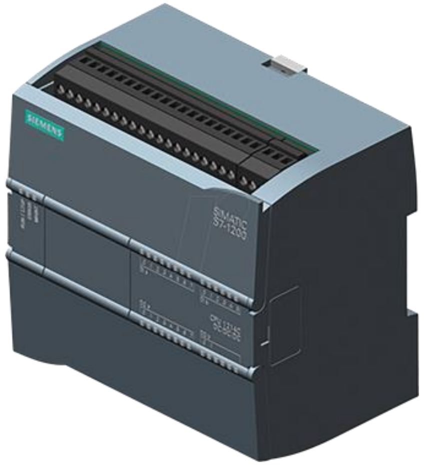
Previous research

- TEMPEST (1982)
  - NSA paper
  - Leaking data through electromagnetic emissions
- system-bus-radio
  - «Mary had a little lamb»

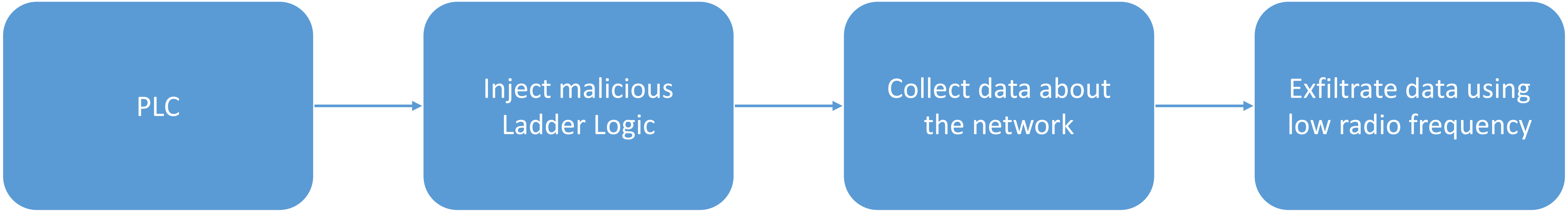


Setup

- SDRPlay 2
  - Antenna to USB
  - ConsoleSDR
- TV antenna
- S7-1200
  - Default configuration
  - POC is tested on this device but may be implemented for other vendors as well
  - It’s not a unique feature to this model/vendor



Our Method of Exfiltration



PLC

Inject malicious Ladder Logic

Collect data about the network

Exfiltrate data using low radio frequency

Challenges

- Frequency used by the PLC
  - Every device transmits electro magnetic waves
  - The frequency is different

PLC Processor Behavior Default Frequency

320Khz

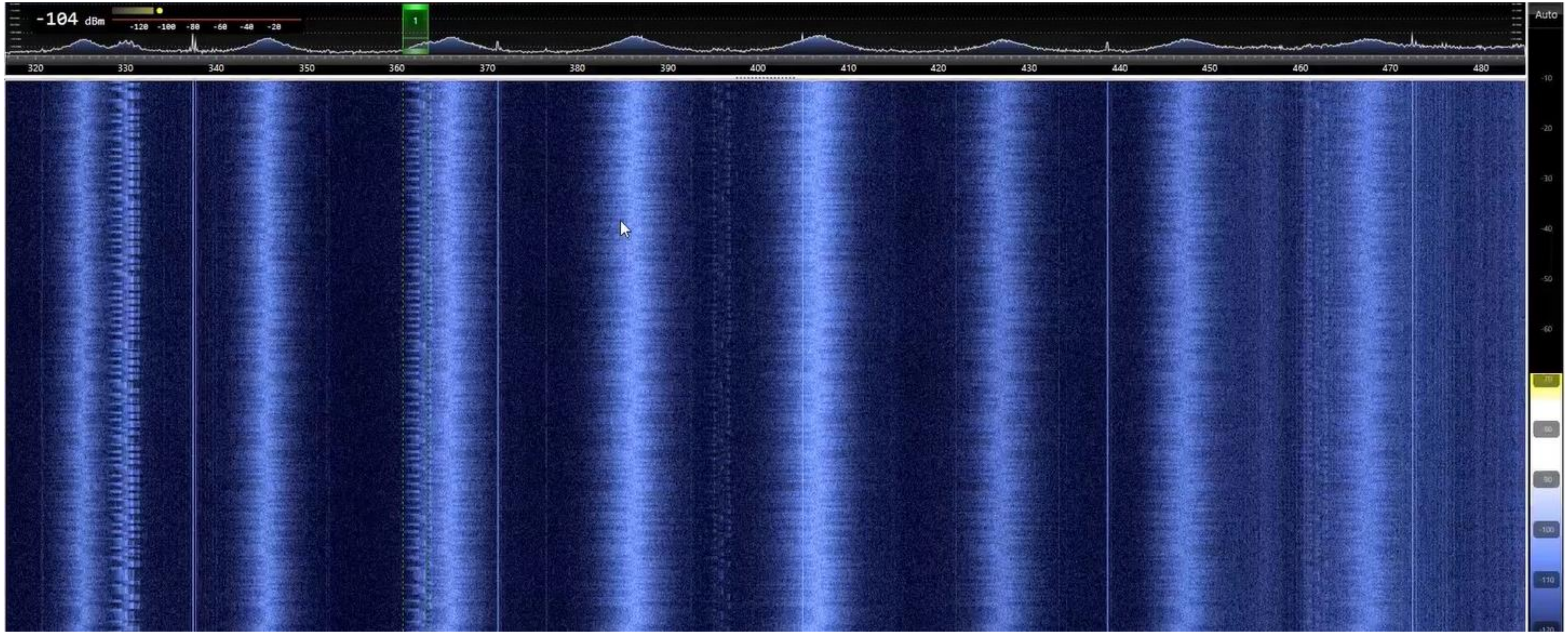
400Khz

Frequencies

Now

Time

-60



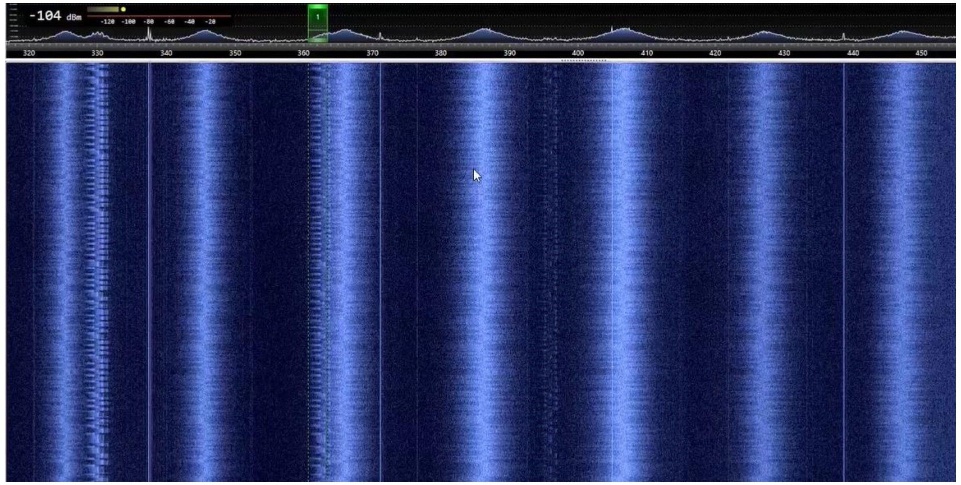
Challenges

- Frequency used by the PLC
- Create changes in EM waves
  - Through the ladder logic
  - Encoding data with changes

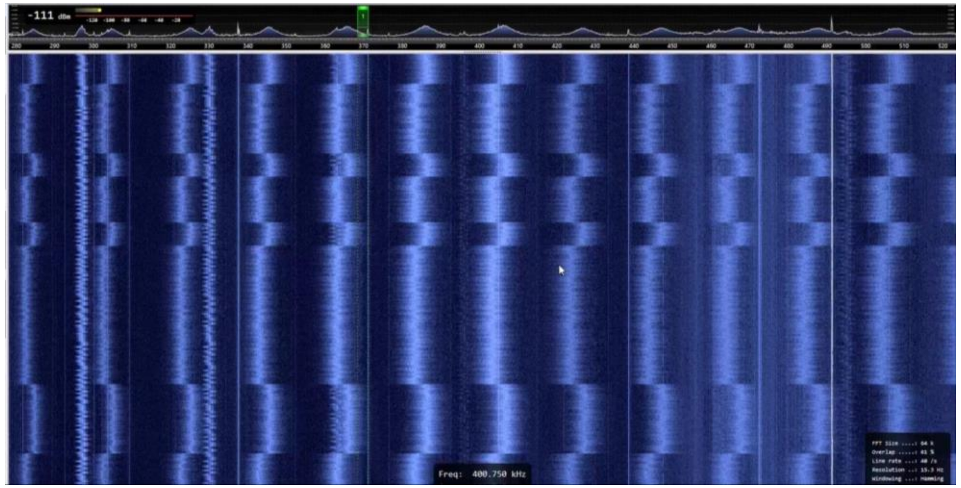
PLC EM behaviors

- Mathematical calculations
  - Mul, mod,..
  - No effect on the strength of the EM emission
- Ethernet cable
  - Has effect on frequency
  - Requires physically access
- Send/Receive network traffic
  - No change on the strength or the frequency
- Copying large memory blocks
  - No effect on the strength of the emission
  - But changes the frequency -> success

PLC Emission Writing to Memory



memcopy

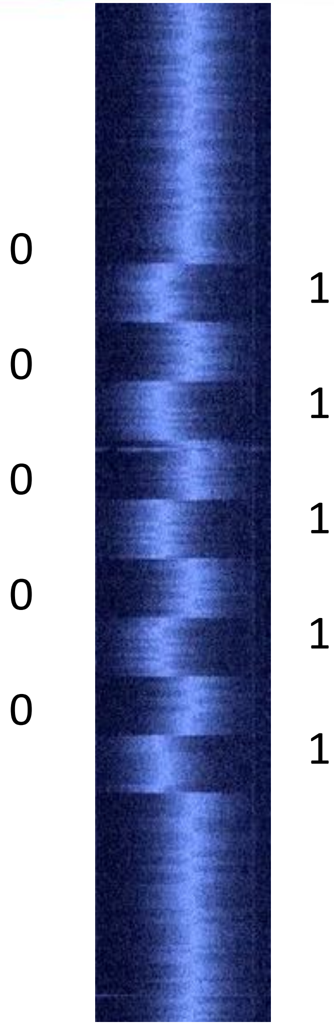


Challenges

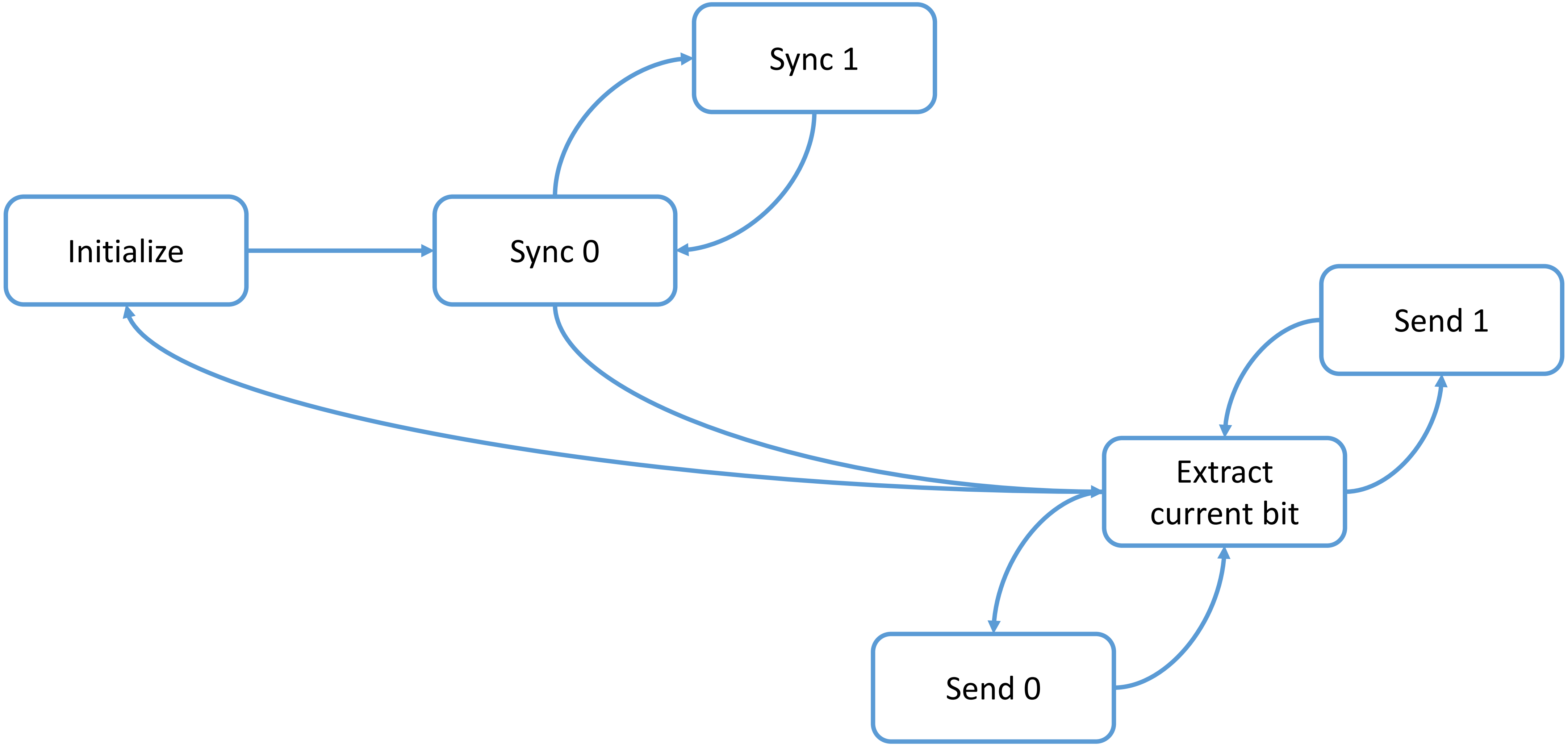
- Frequency used by the PLC
- Create changes in EM waves
- Ladder logic that send data

Ladder Logic to Exfiltrate Data

- Decide on an encoding
- Synchronization pattern
  - Sync the PLC clock to PC clock
- Send the data



Ladder Logic State Machine



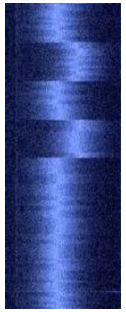
Ladder Logic
Rungs

Ladder Logic rungs

send_bit

Controls the current frequency, the rest of the program will manipulate "**bit**" variable to encode data

- If **bit** == 1:
  - Memcopy(dummy_src, dummy_dst, 10000)
- Else:
  - Dummy_var = dummy_var * 123

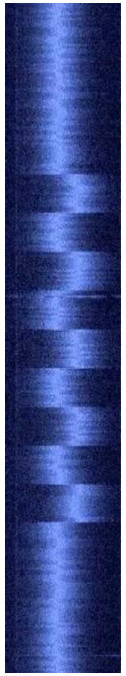


Ladder Logic rungs

sync

A sync pattern is needed to detect the signal on the listening side

```
• If sync_start <= state <= sync_end:
    • If state % 2 == 0:
        • send_bit(1)
    • Else:
        • send_bit(0)
```

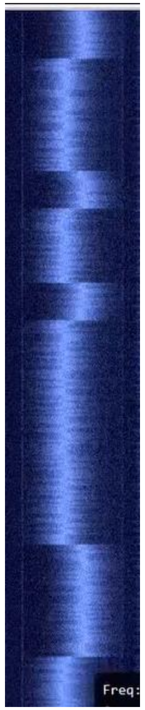


Ladder Logic rungs

send_cur_bit

We send the current bit

- If sync_end <= state <= data_end:
  - cur_bit = get_cur_bit(data_arr, state)
  - If cur_bit == 1:
    - send_bit(1)
  - Else:
    - send_bit(0)

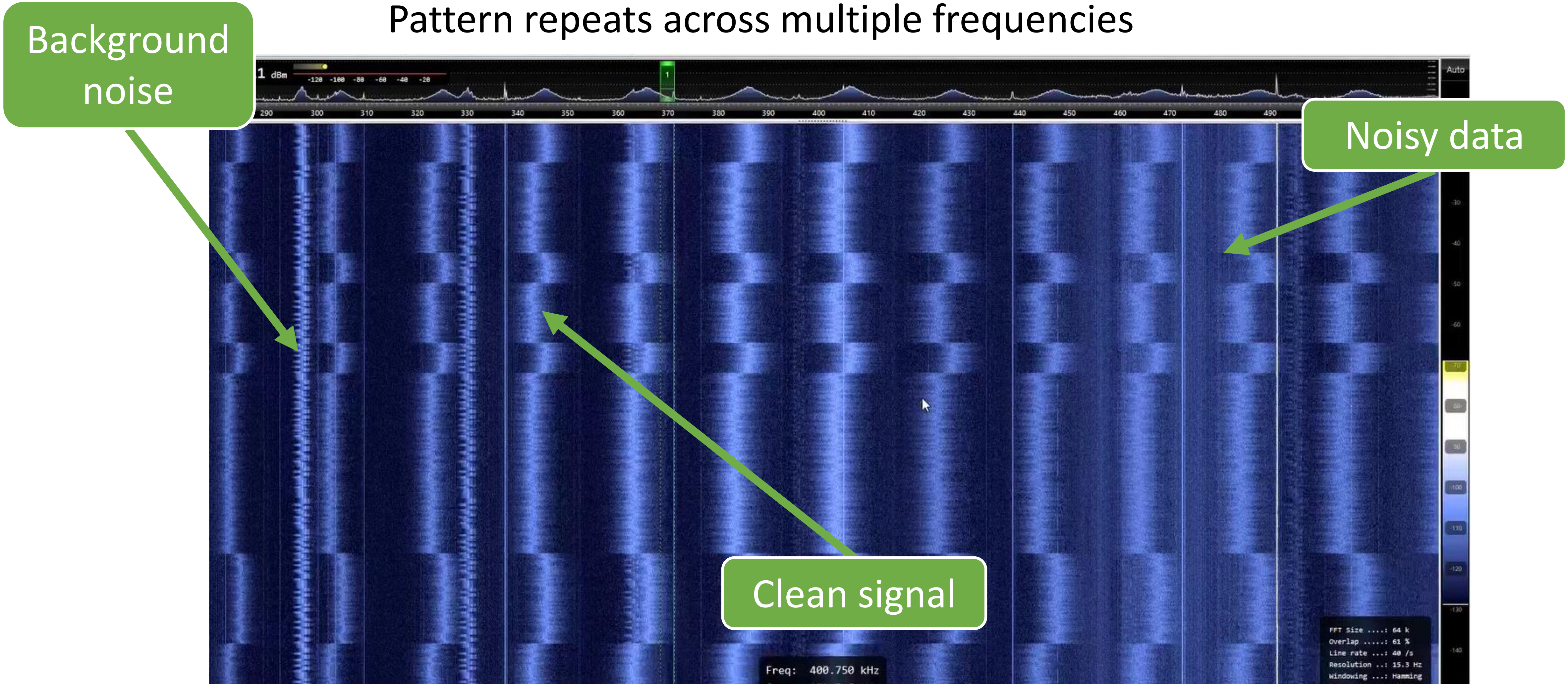


Challenges

- Frequency used by the PLC
- Create changes in EM waves
- Ladder logic that send data
- Code that receives the transmission
  - Find transmission frequency

Detecting transmission frequency

Pattern repeats across multiple frequencies



Background noise

Noisy data

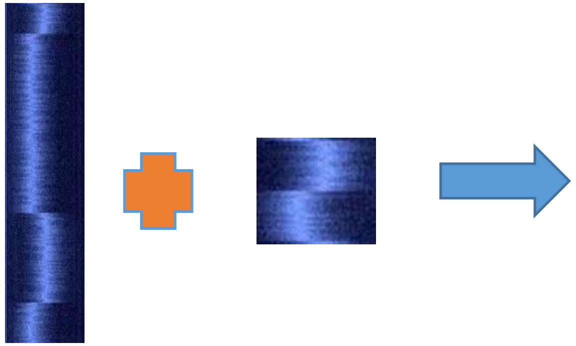
Clean signal

```
Freq:  400.750 kHz
```

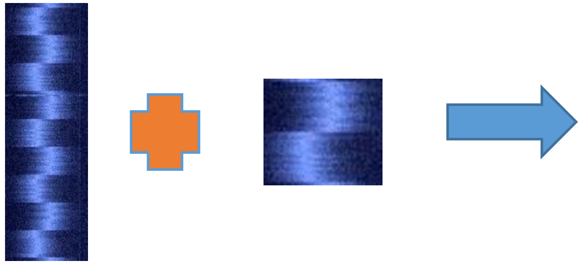
```
FFT Size ....: 64 k
Overlap .....: 61 %
Line rate ...: 40 /s
Resolution ..: 15.3 Hz
Windowing ...: Hamming
```

Detecting transmission frequency

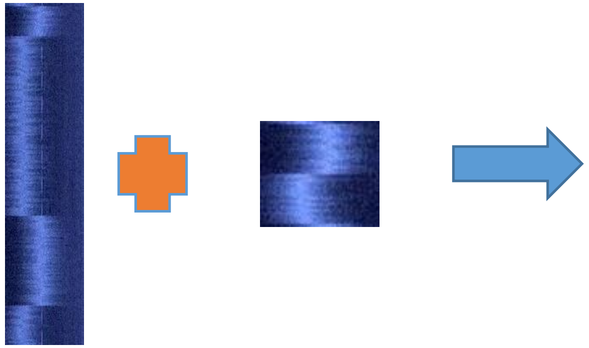
- Treat it like an image
- Correlate to a perfect mask
- Sync will be easiest to detect



Strong correlation



Strongest correlation



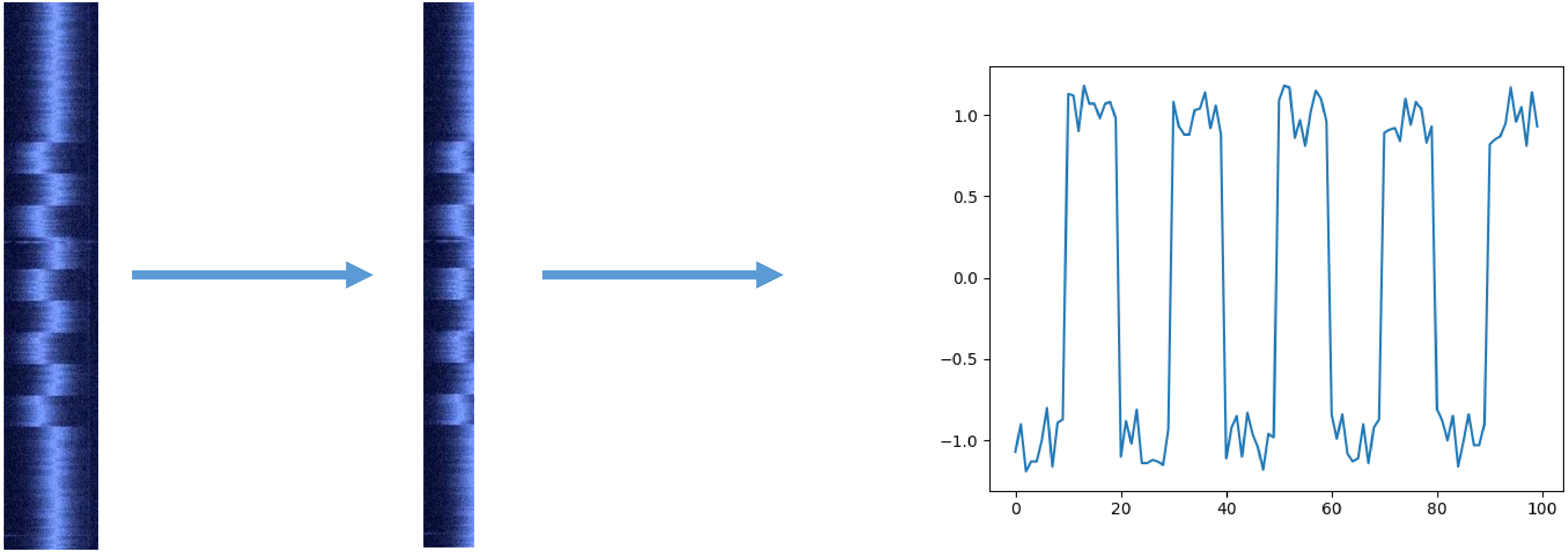
Weak correlation

Challenges

- Frequency used by the PLC
- Create changes in EM waves
- Ladder logic that send data
- Code that receives the transmission
    - Find transmission frequency
    - Detect a synchronization
        - sync to PLC clock

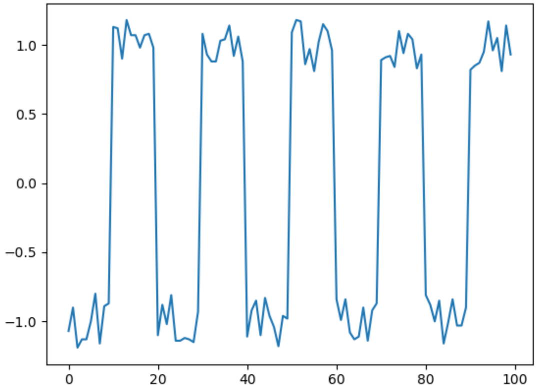
Detecting a sync

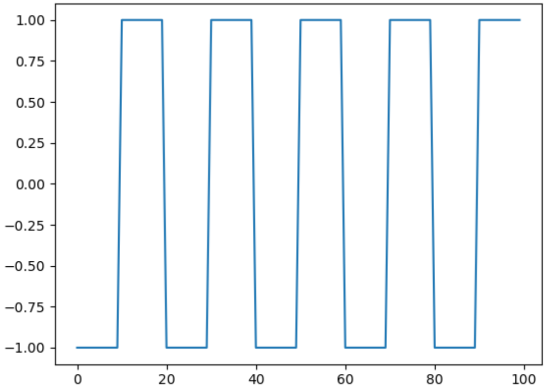
- Work with optimal frequency
- Transform the frequency into a 1D array



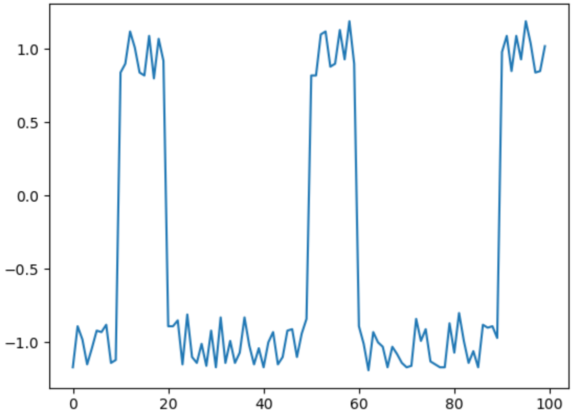
Detecting a sync

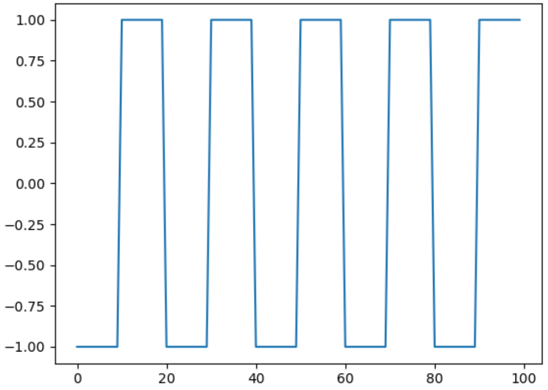
- Correlate to perfect signal





Strong correlation





Weak correlation

Challenges

- Frequency used by the PLC
- Create changes in EM waves
- Ladder logic that send data
- Code that receives the transmission
  - Find transmission frequency
  - Detect a synchronization
  - Receive data

Receiving the data

- We are synchronized to the PLC clock
- The PLC send a bit every second
- We all the data received in the last second

Statistics

- Distance
  - Up to 1 meter
  - A better antenna -> better range
- Bandwidth
  - 1 bit per second
  - Better algorithm + better antenna -> faster
- Exfiltration techniques
  - Antenna could be mounted on a drone to get to sufficient receiving range
  - Portable antenna could be concealed in a portable device

Demo

Black Hat Sound Bytes

- Use continuous monitoring with anomaly detection to detect cyber reconnaissance phase preceding data exfiltration
- Detect unwanted Ladder Logic programming
- Detect suspicious traffic originating to/from ICS devices
- Discover new devices on the network

CyberX

Trusted. Industrial. Cybersecurity.

Thank You!

david@cyberx-labs.com
george@cyberx-labs.com