RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: HTA-W04

MIND THE AIR-GAP: EXFILTRATING ICS DATA VIA AM RADIOS & HACKED PLC CODE

David Atch

VP of Research
CyberX

Introduction

David Atch

- VP/Research for CyberX
- Military service as Team Leader in IDF CERT
- Focused on reverse engineering, malware hunting, tracking ICS campaigns & adversaries

George Lashenko

- Security Researcher at CyberX
- Military service in DF intelligence unit
- 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 behaviors

CyberX

- Founded by military cyber-experts with nation-state expertise defending critical infrastructure
- Purpose-built platform for continuous ICS monitoring, vulnerability management, & automated threat modeling

INTRODUCTION

Agenda

- Many 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

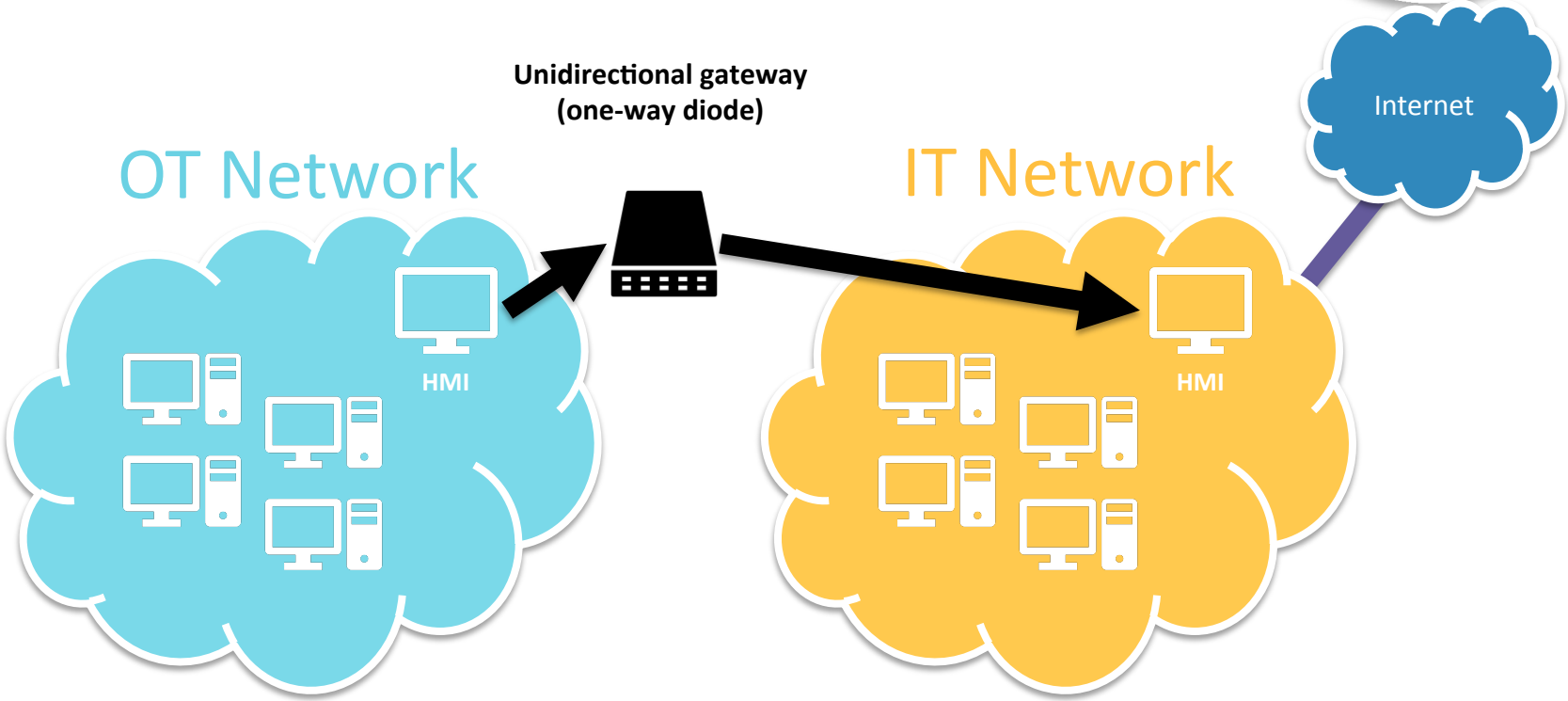
RSAConference2018

NOW MATTERS

#RSAC

OT NETWORKS AND HOW TO GET INSIDE THEM

Air-Gapped Industrial Network



Air-Gapped Networks from the Attacker's Perspective

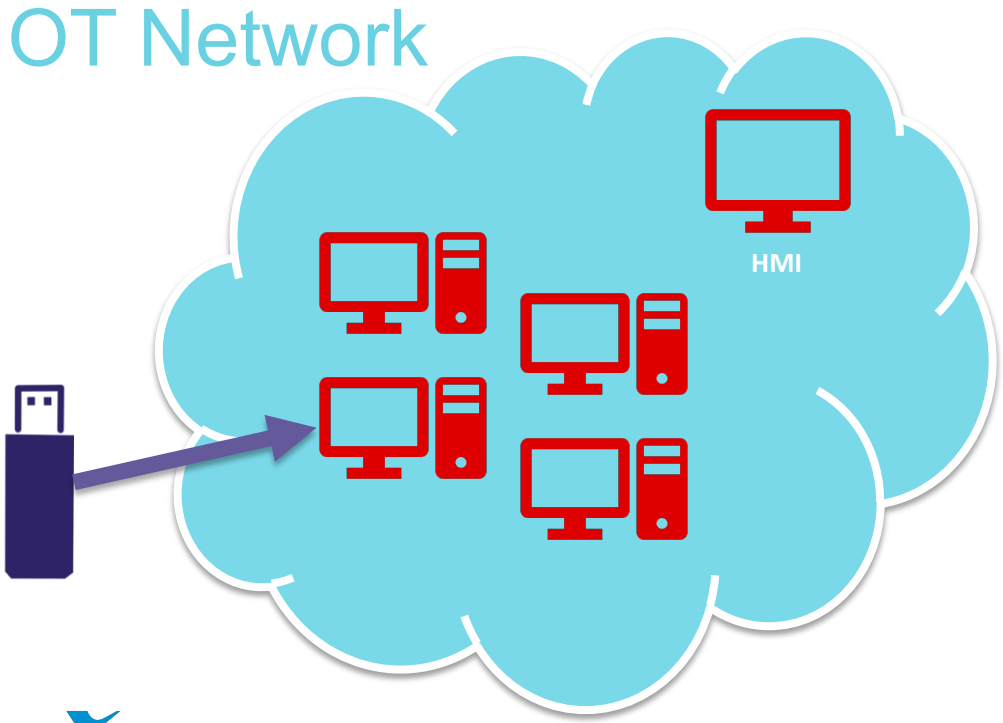
- Hard to get in
  - Not impossible
- Harder to get out
  - Also not impossible

Air-Gapped Networks from the Attacker's Perspective

- Initial 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

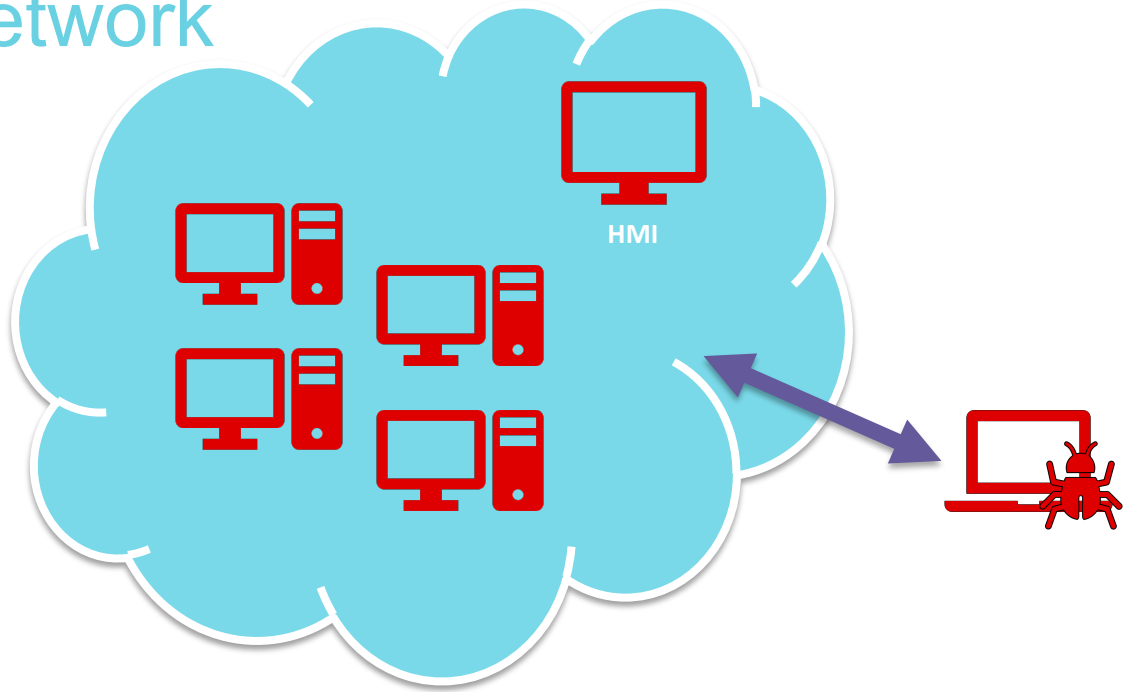
WHAT ARE THE ATTACK VECTORS?

Attack Vectors: Malicious USB

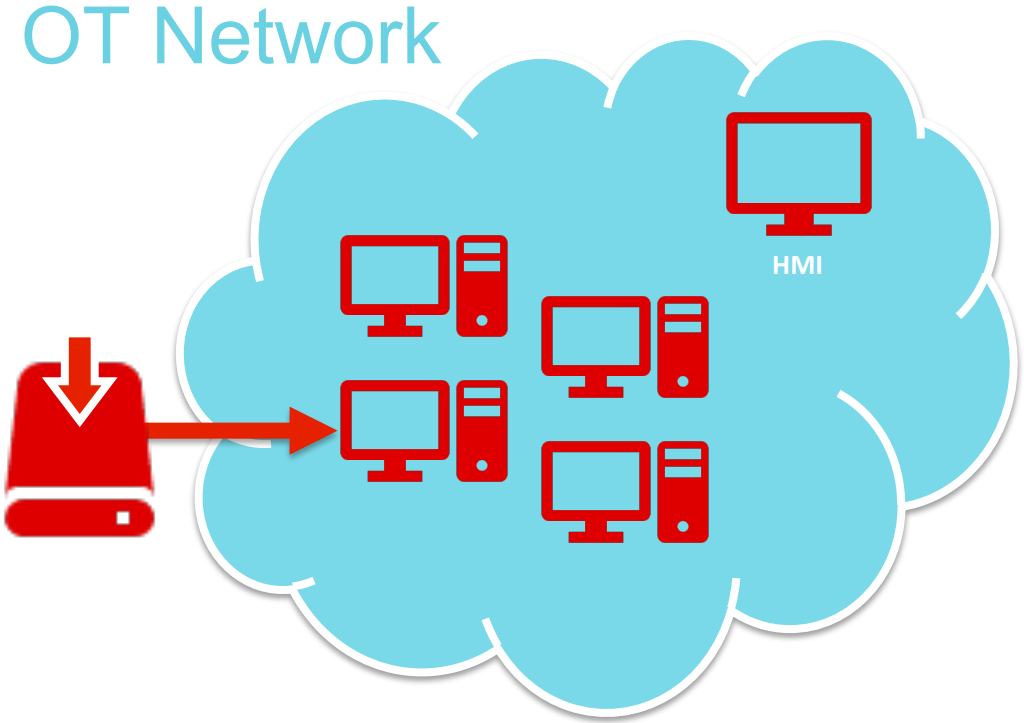


- autorun.inf – Enabled by default on Windows XP (still widely used in OT networks)
- LNK exploits – Used also by Stuxnet
- DLL Search Order Hijacking

Attack Vectors:
External Engineering Laptop



Attack Vectors: Infected Vendor Updates



- 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

Exfiltrate Collected Data

Approaches

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

Challenges

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

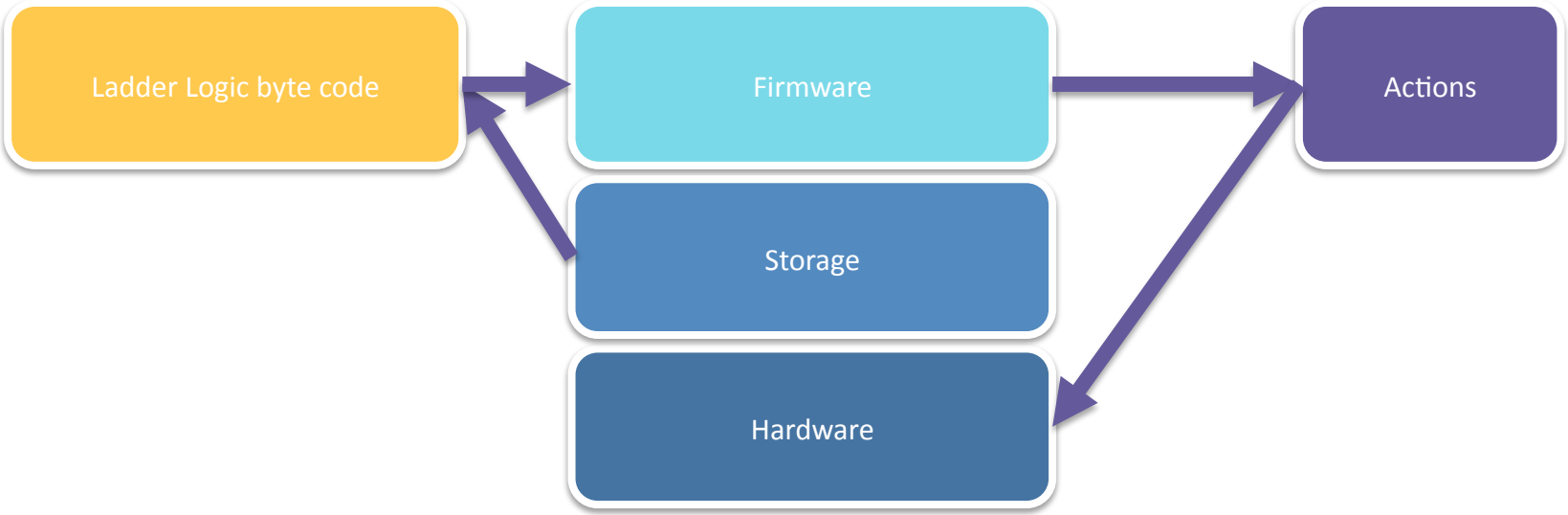
RSAConference2018

NOW MATTERS

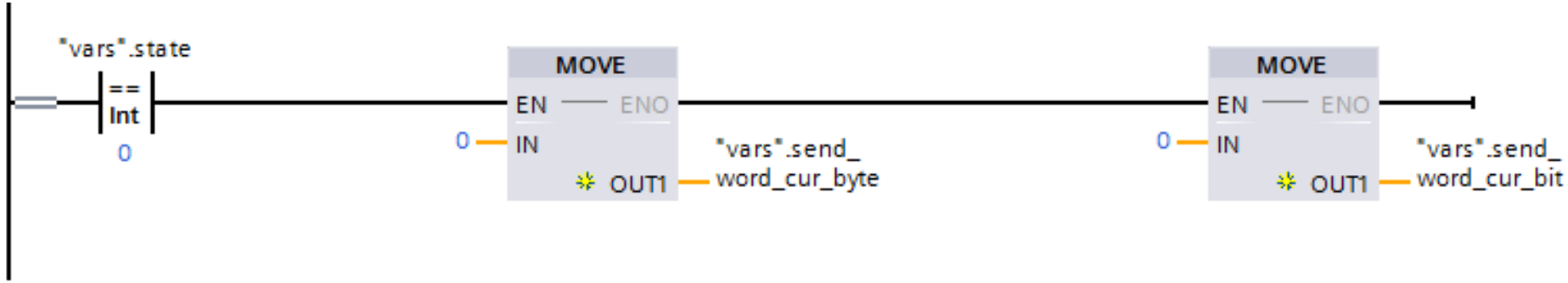
#RSAC

BRIEF OVERVIEW OF LADDER LOGIC

PLC Structure

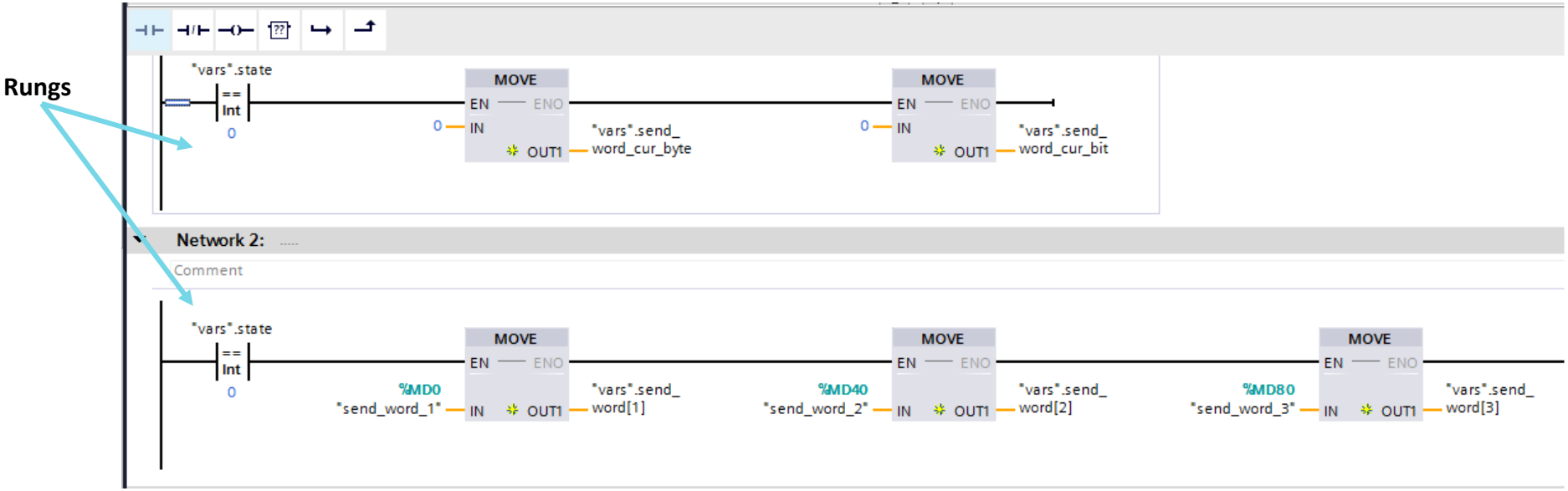


Ladder Logic Example



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

Multiple Rung Example

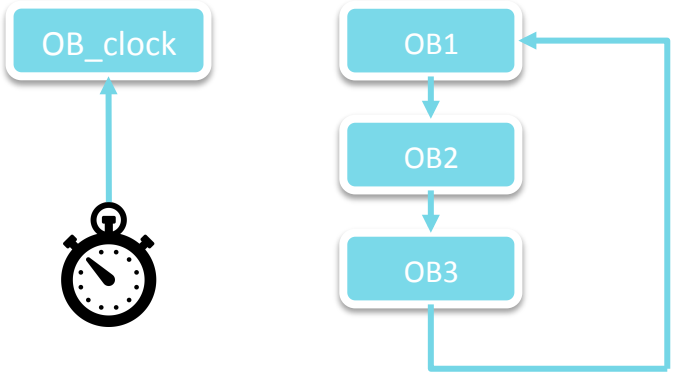


Block Types

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

Organizational Blocks (OB)

- Cyclic execution (“parallel”)
- Execution via event trigger
  - Network error, …
- Execution via a timer
  - Every x seconds

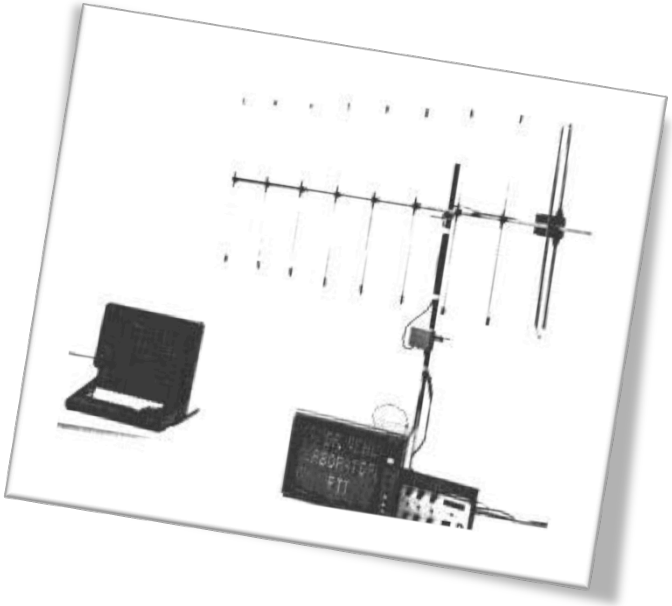


Why Exfiltrate with Ladder Logic?

- Avoid detection
  - Can't run antivirus programs in a PLC
- Persistency
  - Malicious code can be stealthily inserted into legitimate code (e.g., TRITON)
- Previous research shows Ladder Logic can also act as reconnaissance malware
  - Scan the network, gather other ladder logic, gather configurations
  - Look for security products
  - Monitor work hours
- Exploits can also be embedded in ladder logic (e.g., EternalBlue)

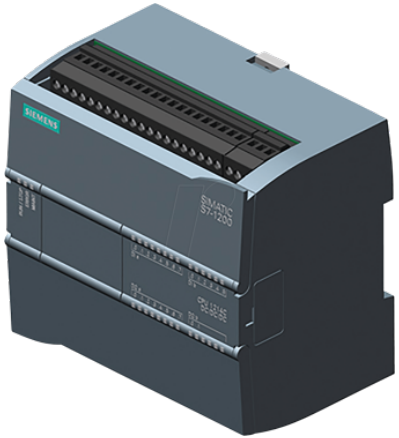
Previous Research

- TEMPEST (1982)
  - “Telecommunications Electronics Material Protected from Emanating Spurious Transmissions” (and other acronyms)
  - NSA paper
  - Leaking data through electromagnetic emissions
- system-bus-radio
  - «Mary had a little lamb»

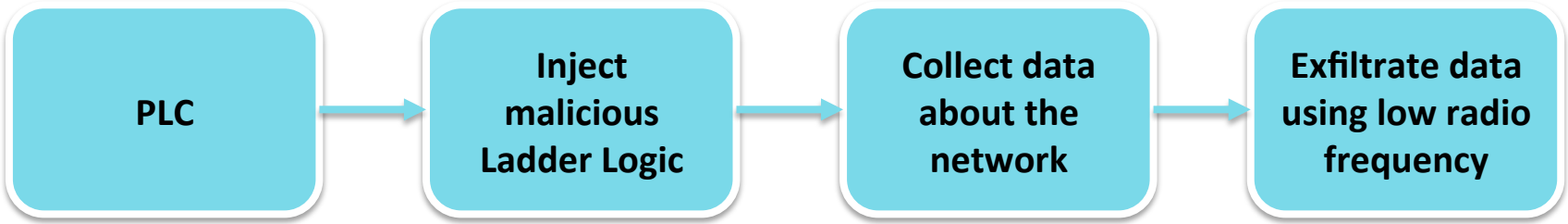


Setup

- SDRPlay 2
  - Antenna to USB
  - ConsoleSDR
- TV antenna
- Siemens S7-1200 SIMATIC Controller
  - Default configuration
  - POC tested on this device but can be implemented for other vendors as well
  - It's not a vulnerability or unique feature to this model/vendor



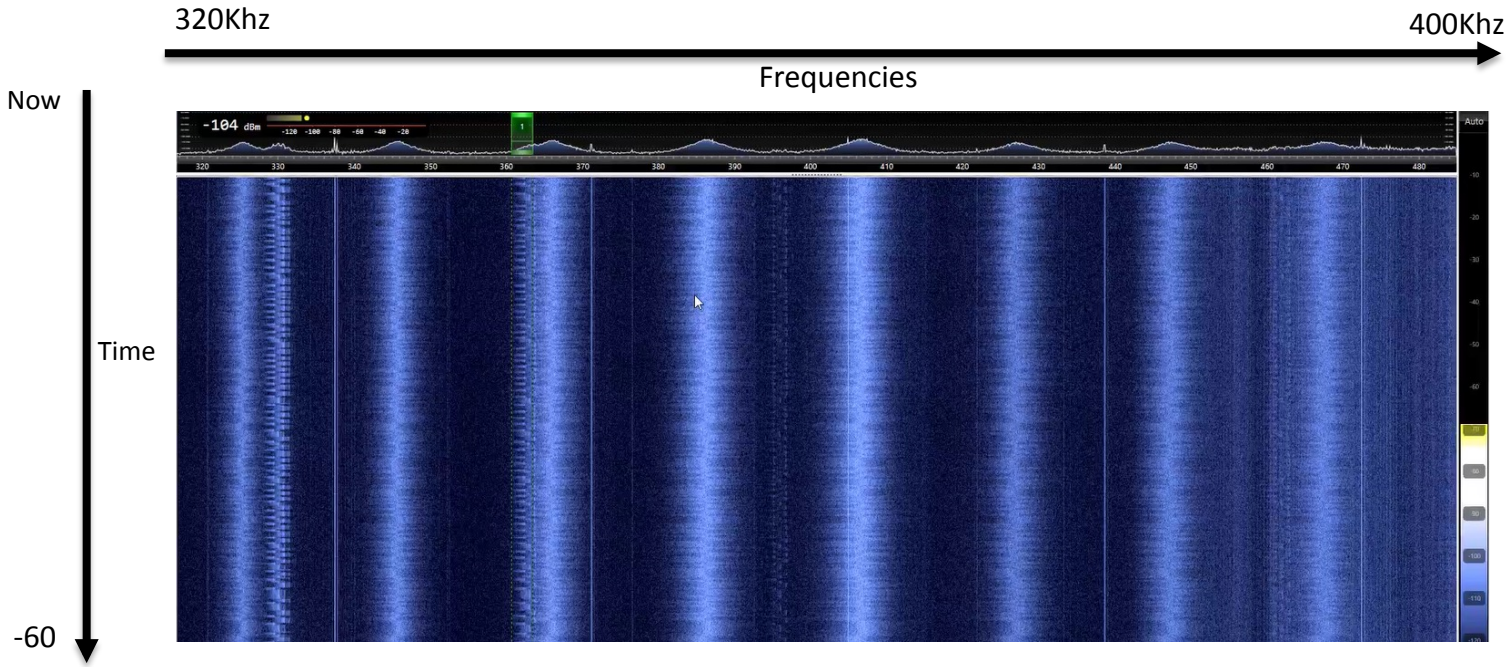
Our Method of Exfiltration



Challenges

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

PLC Processor Behavior
Default Frequency



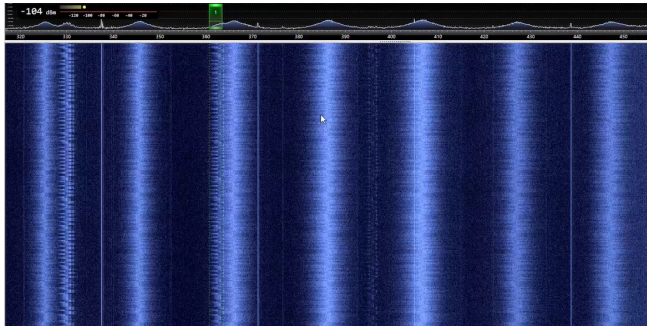
Challenges

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

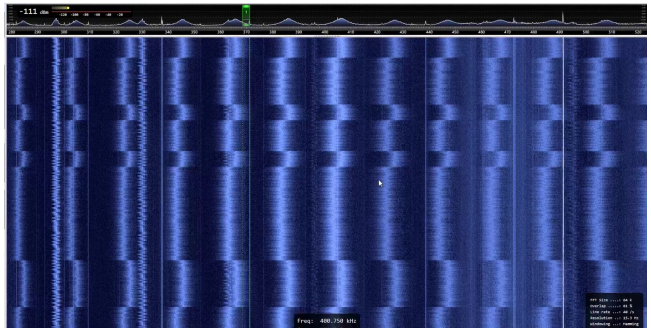
PLC EM Behaviors

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

PLC Emission
Writing to Memory



memcopy

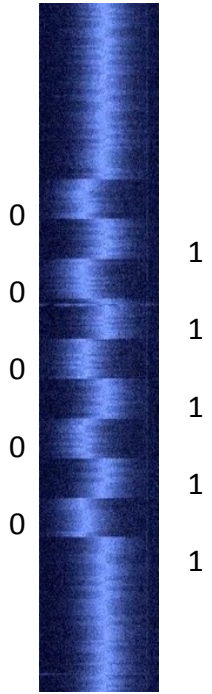


Challenges

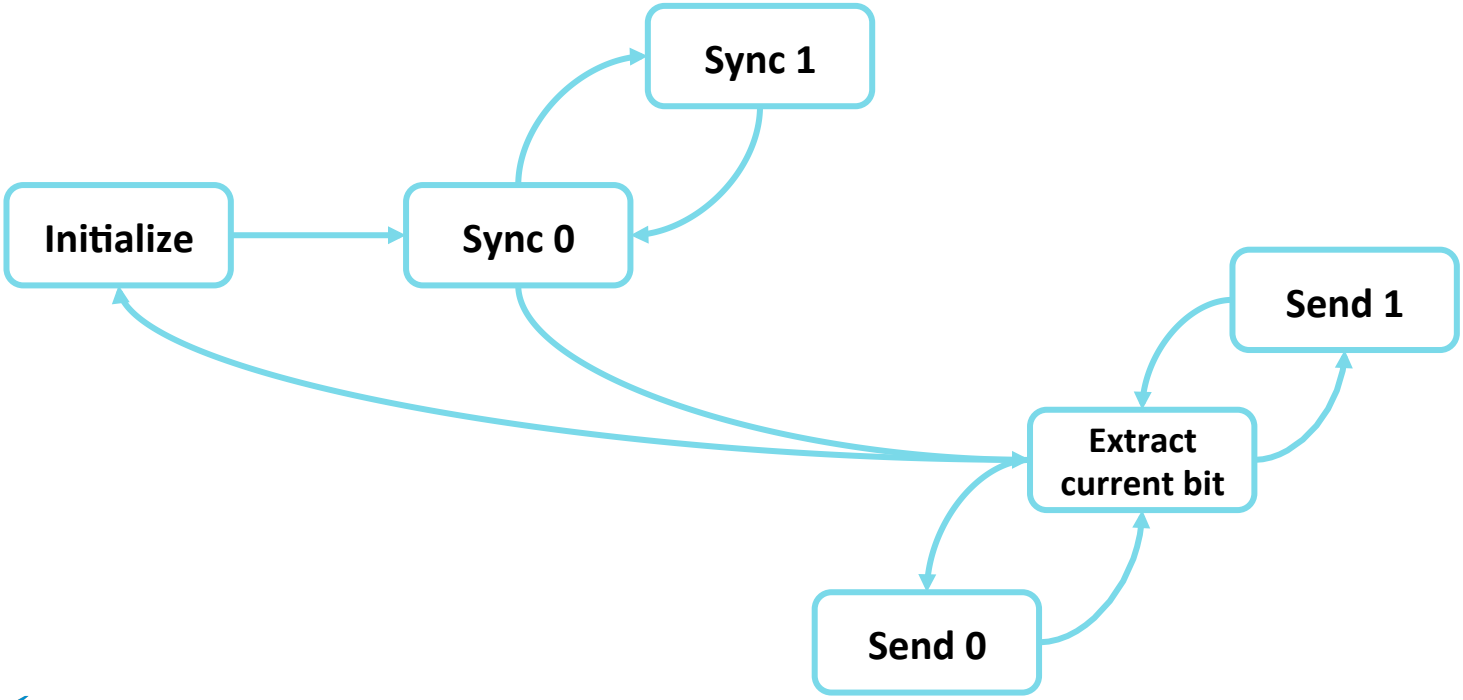
- Frequency used by the PLC
- Create changes in EM waves
- Ladder logic that send data

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



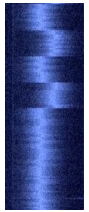
LADDER LOGIC RUNGS

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

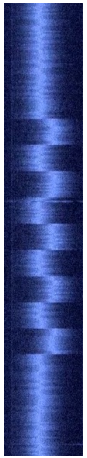


Ladder Logic rungs

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)

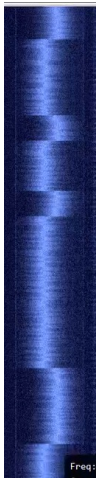


Ladder Logic rungs

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)

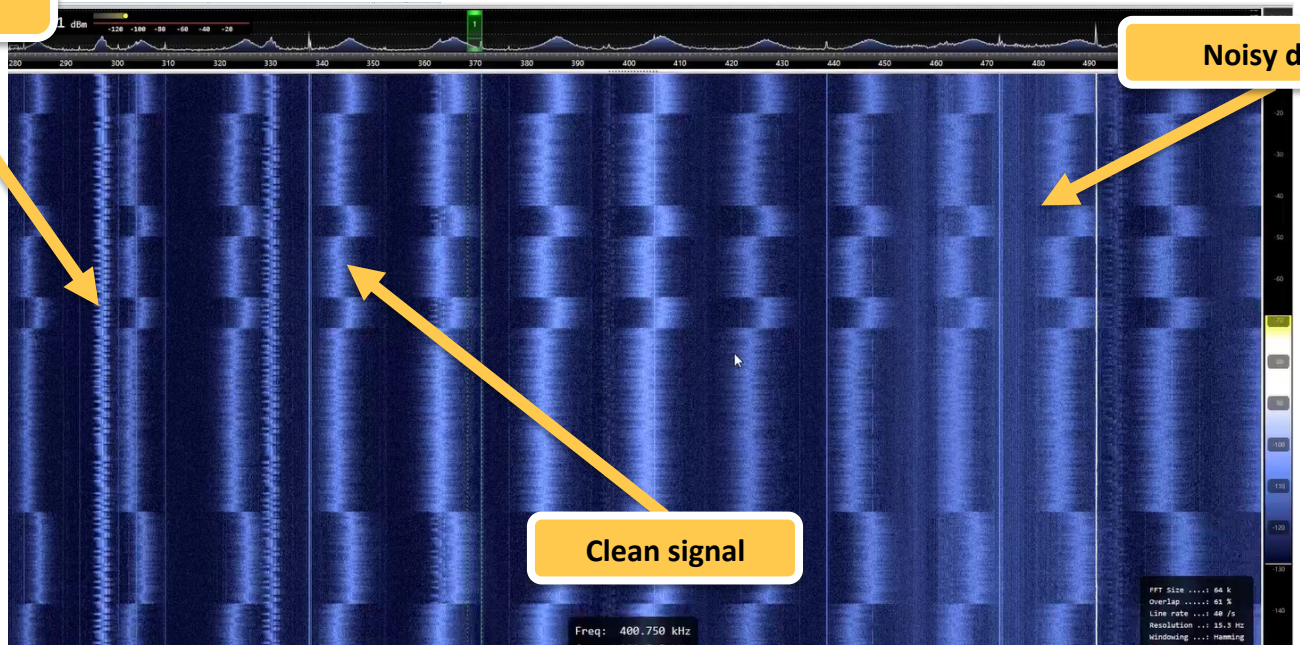


Challenges

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

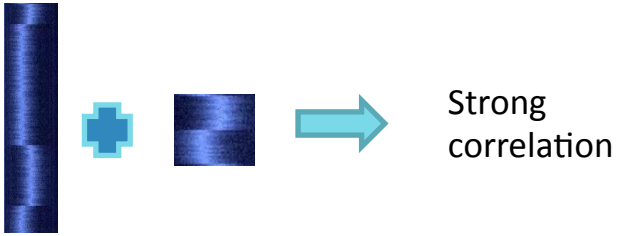
Detecting Transmission Frequency

Pattern repeats across multiple frequencies

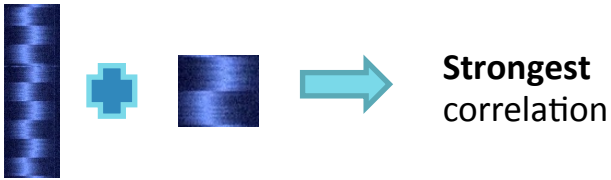


Detecting Transmission Frequency

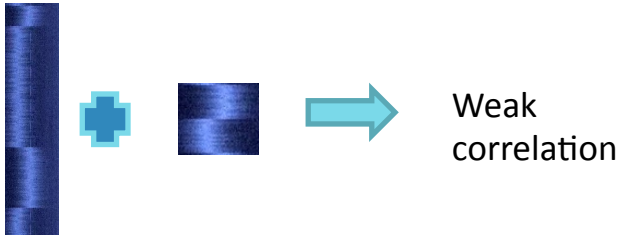
- Treat it like an image
- Correlate to a perfect mask
- Sync will be easiest to detect



Strong correlation



Strongest correlation



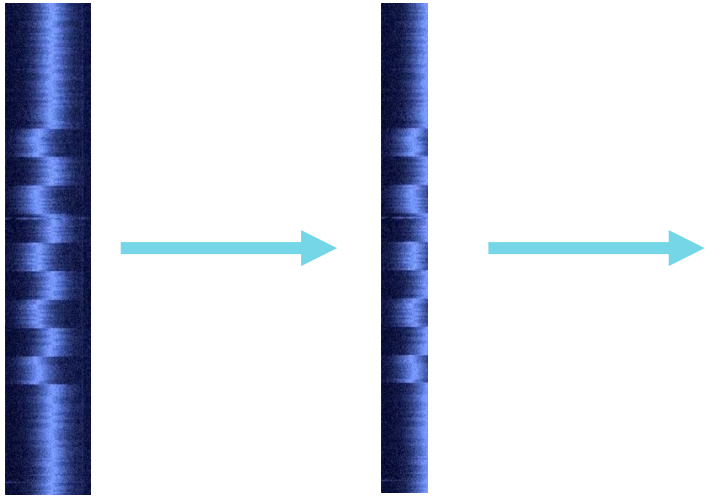
Weak correlation

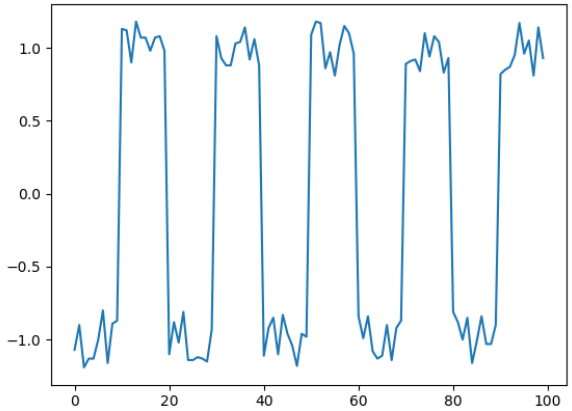
Challenges

- 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

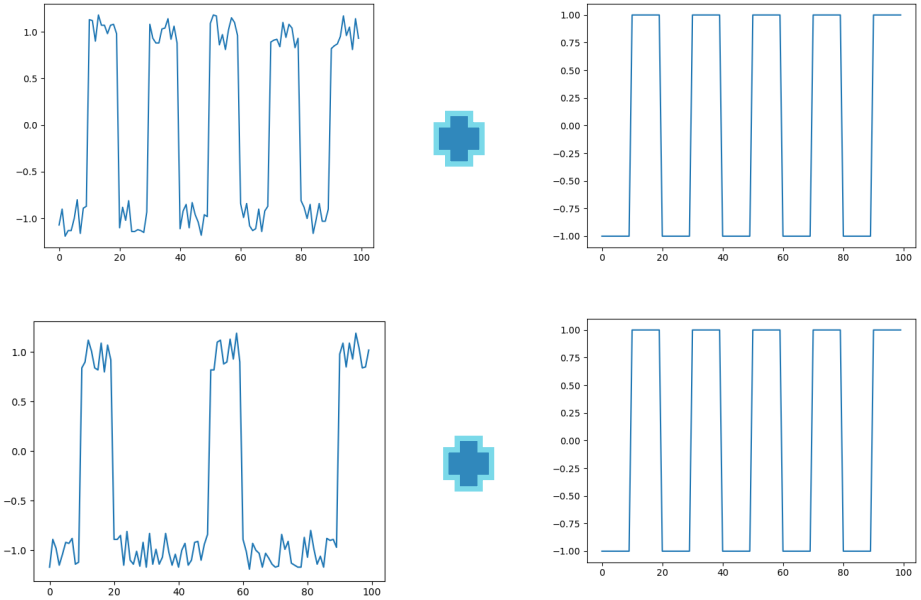
- Work with optimal frequency
- Transform the frequency into 1D array





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 sends 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

Conclusions — How to Defend

- Use continuous monitoring with behavioral anomaly detection to detect reconnaissance by adversaries prior to data exfiltration
- Detect unauthorized PLC programming
- Detect suspicious traffic originating to/from ICS devices
- Discover new devices on the network

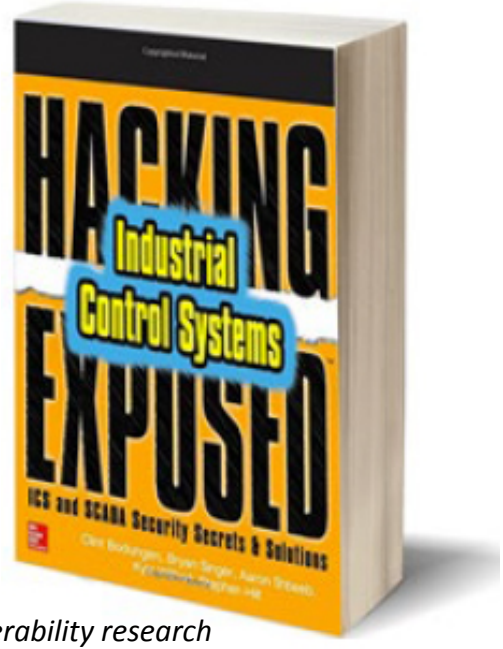
For More Information

Check out our ICS & IIoT Security Knowledge Base

- CyberX threat & vulnerability research (Black Energy, etc.)
- Transcripts from SANS webinars (TRITON, etc.)
- Free downloads of *ICS Hacking Exposed (McGraw-Hill)*
- CyberX "Global ICS & IIoT Risk Report" with vulnerability data obtained from 375 production ICS networks worldwide
- Research presentations from Black Hat & S4x18 conferences

Visit us at:

- **CyberX "Emerging ICS Threats"** seminar with CISOs from Teva Pharmaceuticals & Scotia Gas Networks (London, May 3)
- **Cyber Security for Oil & Gas** in Houston (May 21-22)
- **Gartner Security** & Risk Management in MD (June 4-7)
- **EnergySec** in Anaheim (August 27-29)
- **ManuSec** USA in Chicago (October 9-10)
- *More …*



CyberX vulnerability research featured in Chapter 7

CyberX
Trusted. Industrial. Cybersecurity.