Advanced Persistent Threat detection for Industrial Control Systems

Presenters: Dominika Rusek & Steffan Roobol

Supervisors: Tijl Deneut & Hendrik Derre

3rd July 2020

Why Industrial Control Systems?

- ICS = control systems, instrumentation used to automate/operate processes
- Energy grids, bridges, airports, manufacturing
- Strategic significance, potential serious consequences
- Rise in targeted attacks (APT) on ICS

Security in ICS

- Main ICS focus is safety, security very often not build in
- Vulnerability management proves difficult
- Monitoring:
  - Lack of visibility in the events on the network (81% according to Dragos)
  - IT monitoring not sufficient – ICS specific protocols
  - Commercial solutions available, but pricy
  - Scarce open-source solutions
- Research project at IC4

IC4 INDUSTRIAL CONTROL & COMMUNICATION COMPETENCE CENTER

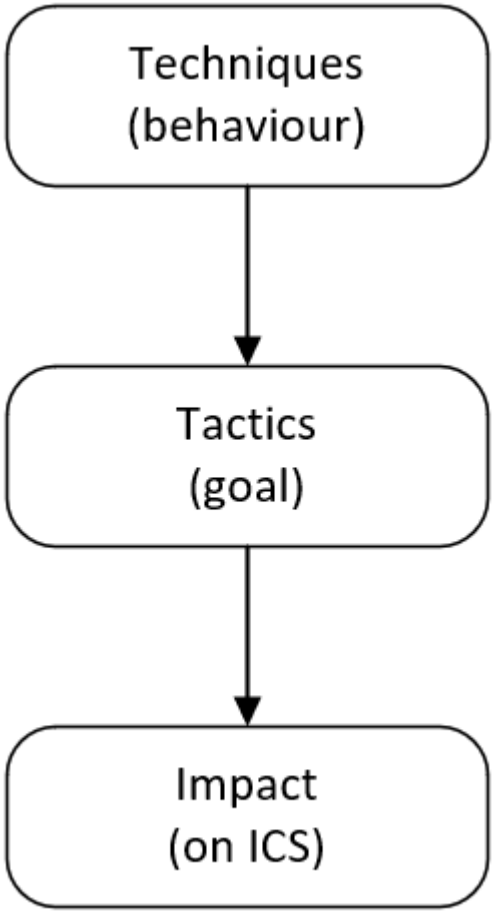
Research question

How can network analysis be used to discover the potential presence of Advanced Persistent Threats (APT) in Industrial Control Systems (ICS)?

- What are the network-based attack techniques used by APT groups documented in the ICS Mitre ATTACK framework?
- How can existing monitoring solutions be improved upon to automate the detection of APT techniques in ICS network?
- How can the detected techniques be mapped to the ICS Killchain to recognize the stage of adversary campaign?

Background - ICS Mitre ATT&CK

- Published in January 2020
- ICS specifics techniques
- Insights about adversary behaviours
- 23 selected network-based techniques

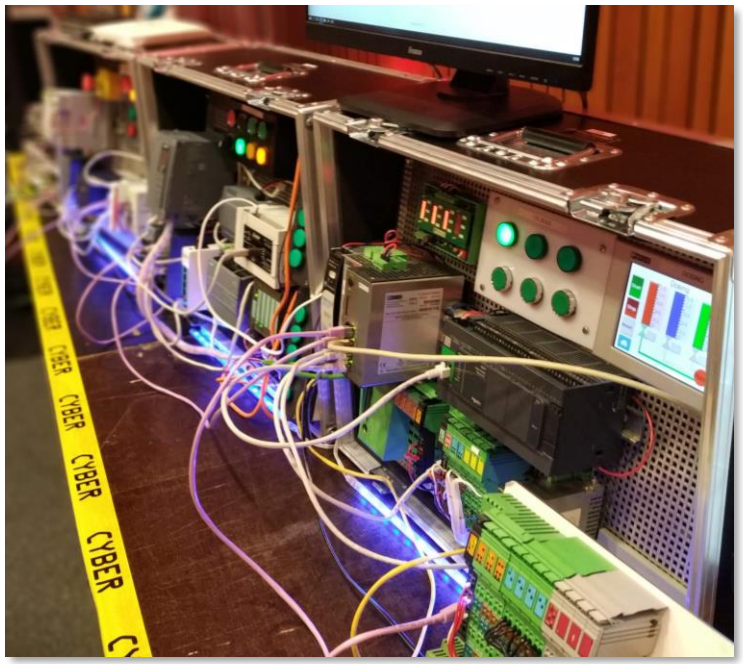


Background - ICS Killchain

- Stage 1
  - Cyber intrusion, management & enablement, sustainment, entrenchment, development & execution
  - Gaining knowledge and persistence
- Stage 2
  - Attack development & tuning, validation, ICS attack
  - Inflicting damage to control systems
- Not all adversaries reach Stage 2 capabilities
- Knowledge where adversary is in the killchain, helps with appropriate response actions

Manufacturing testbed

- IC4 – Industrial Control & Communication Competence Center
- Fictile tile manufacturing
- 3 industrial segments, 1 IT
- PLCs, HMIs, industrial routers etc.
  - Siemens, Phoenix, Beckhoff, Rockwell etc.



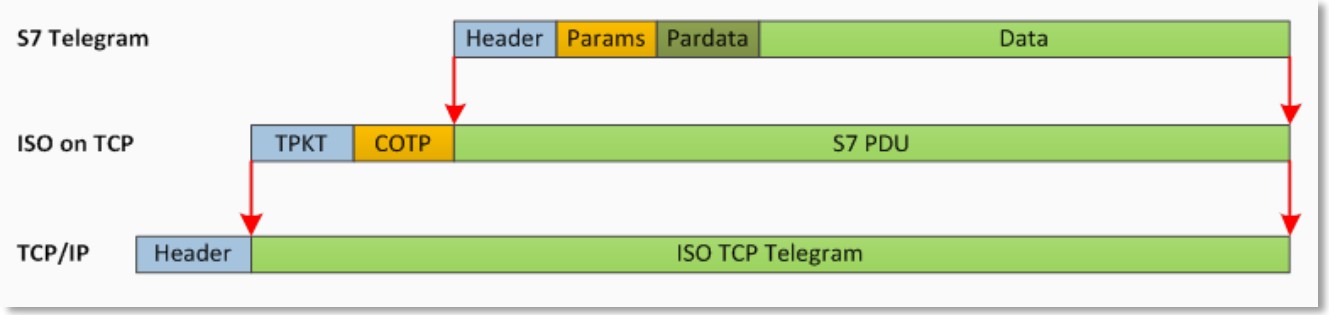
Datasets collected from the testbed

- Baseline pcap:
  - Getting familiar with ICS protocols
  - Used for creating the PoC and testing
- Adversary techniques pcap:
  - Using IC4 scripts
  - 12 techniques, 7 tactics
- Unbalanced data set
  - Many normal events (regular traffic)

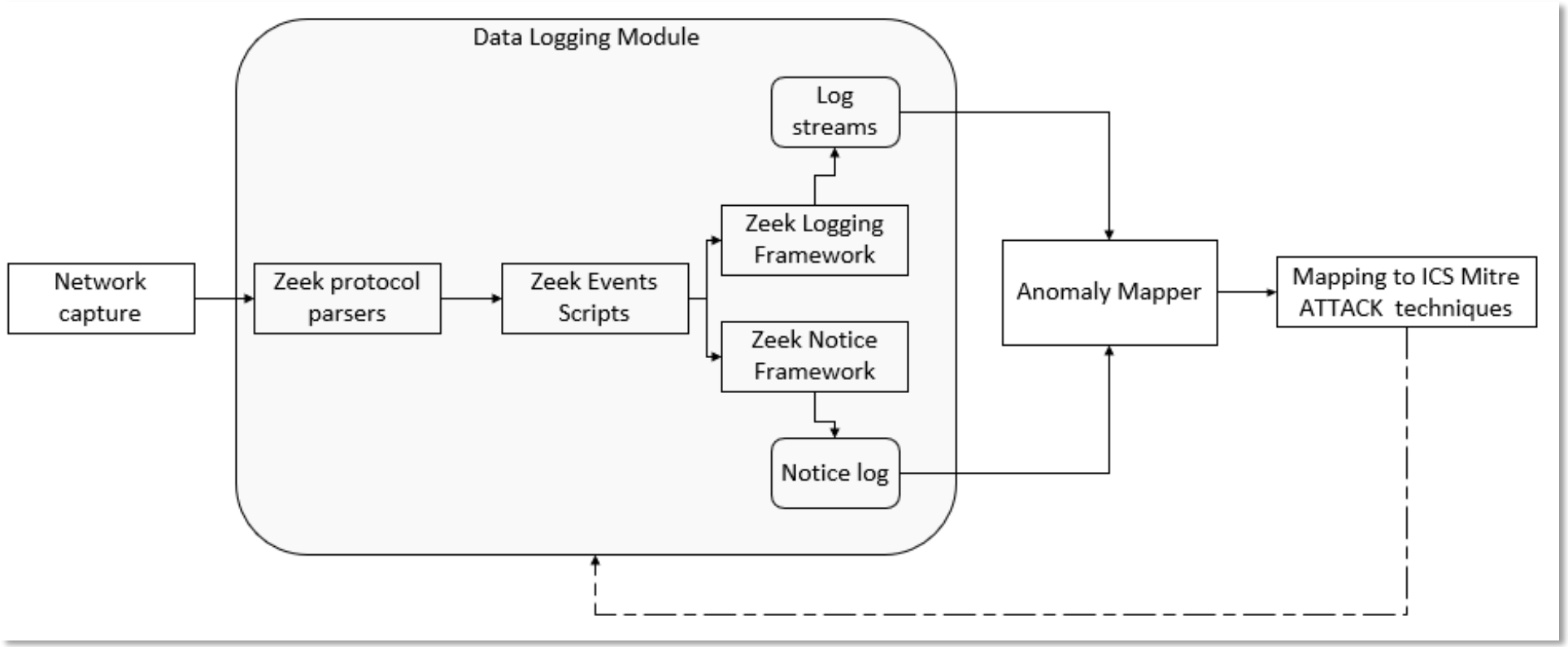
Action	Technique
ARP spoofing	MiTM
Establishing SSH session	Command Line Interface
Establishing RDP session	Command Line Interface
Altering outputs	Change Program State
Altering memory	Change Program State
Uploading executable file	Module Firmware, System Firmware, Remote File Copy
Stop/start CPU PLC	Utilize/Change Program Mode
TCP scan	Network scanning
WannaCry	Exploitation of Remote Services, External Remote Services, Remote File Copy
Device Scanning	Collection
DNS tunneling	Command and control

S7comm

- Siemens proprietary protocol
- Used for PLC programming, exchanging data between devices
  - Standard version ID 0x32, new version ID 0x72
- Interaction with devices with function codes in S7comm Data
  - Read/write
  - Stop/start
  - Upload/download



Proof of Concept application



Zeek (formerly Bro)

- Open-source network security traffic analyzer
- Inspects all traffic for signs of suspicious activity
- Wide protocol base support by default
  - Some ICS protocol parsers
- No hard coded analysis
- Scripting language allows for customization

Data Logging Module

- Protocol parsers:
  - Zeek common protocol parsers
  - ZKG plugins for ICS protocols (S7comm)
- Custom Zeek event scripts:
  - Save extra data while parsing pcap
  - Raising notices (alerts)


```
{
    "ts": 1593265918.13298,
    "uid": "Cc9Xcz23lSoBMQcFt4",
    "id.orig_h": "10.20.20.22",
    "id.orig_p": 37512,
    "id.resp_h": "10.20.2.10",
    "id.resp_p": 102,
    "proto": "tcp",
    "note": "S7CommLogging::IsoCotp",
    "msg": "An ISO COTP command has been issued (208)
        from 10.20.20.22 to 10.20.2.10.",
    "src": "10.20.20.22",
    "dst": "10.20.2.10",
    "p": 102,
    "actions": [
        "Notice::ACTION_LOG"
    ],
    "suppress_for": 3600
}
```

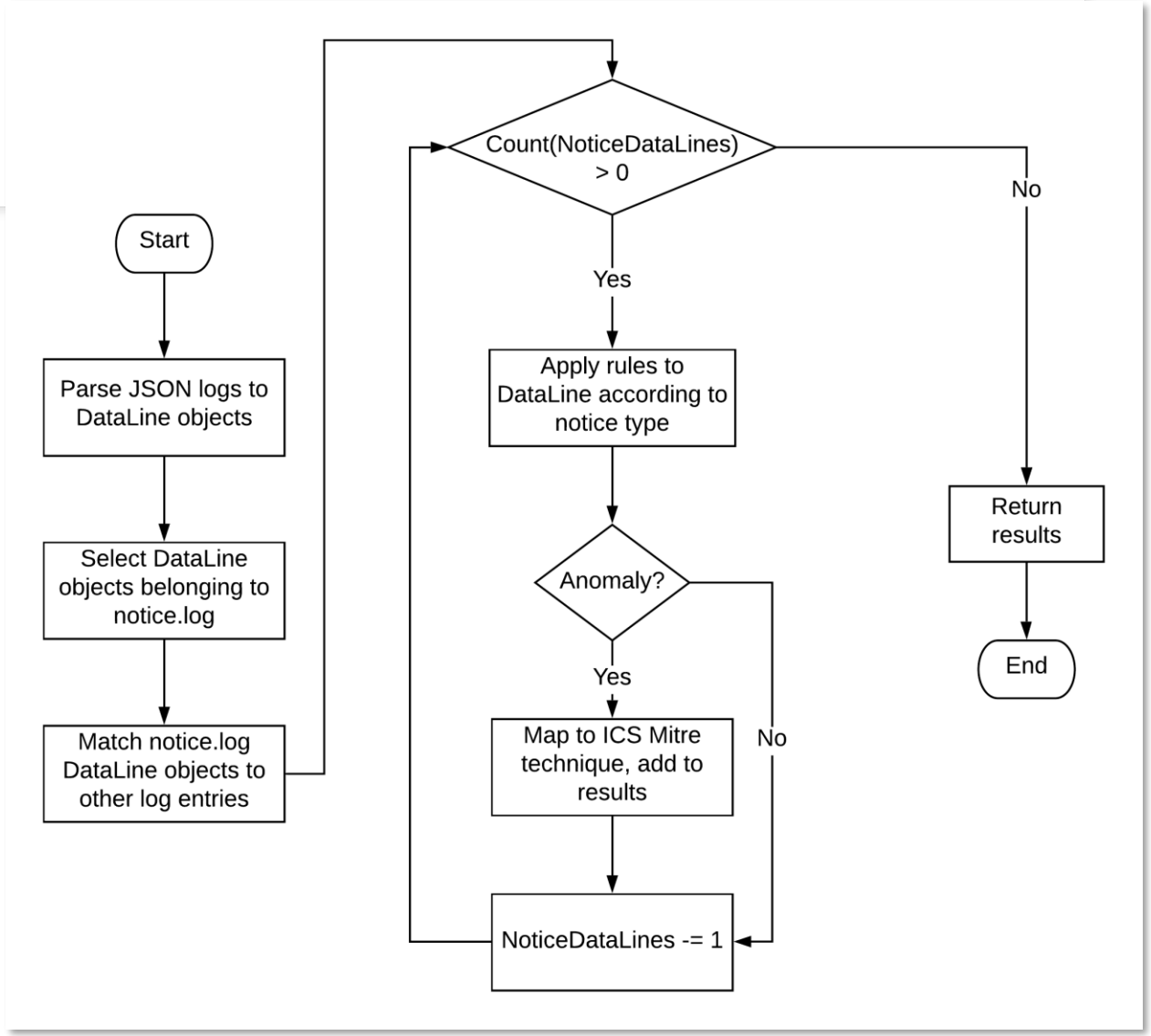

Example entry in notice.log file

Examples of custom Zeek scripts

- ICS protocols
- Portable executable
- Scanning
- MiTM
- Remote file copy

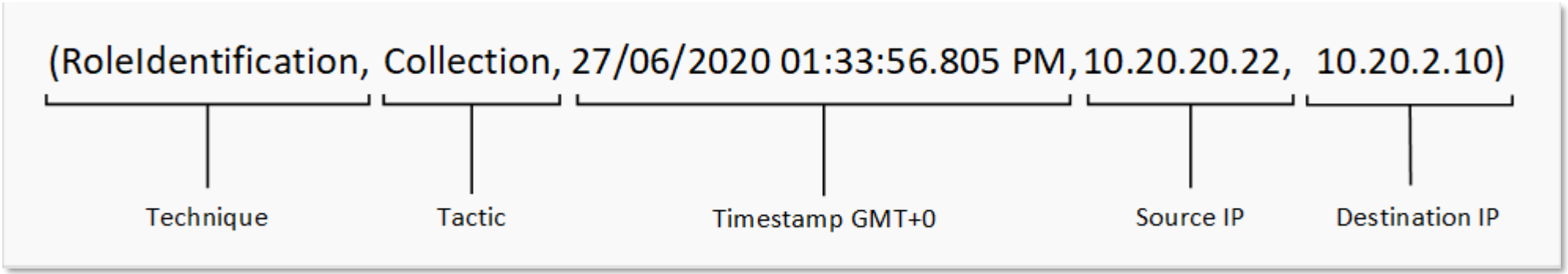
Anomaly Mapper

- ASP.NET Core
- JSON output from Data Logging Module
- Combines notice.log and other logs
  - Same UID and timestamp
- Set of rules to eliminate false-positives



Anomaly Mapper output

- Anomalies are mapped to techniques from ICS Mitre ATT&CK
  - Some anomalies can be mapped to several techniques
- Human factor (analyst) makes the information actionable



Results – spotting the techniques

- PoC tested on manufacturing dataset
- 10 out of 12 techniques spotted
- 2 techniques not detected:
  - WannaCry did not generate any network traffic
  - Stop/start CPU not parsed as S7comm Data
  - S7comm Plus command used, no parsers available

Technique	Detected
ARP spoofing	Yes
Establishing SSH session	Yes
Establishing RDP session	Yes
Altering outputs	Yes
Altering memory	Yes
Uploading executable file	Yes
Stop/start CPU PLC	No
TCP scan	Yes
WannaCry	No
Device Scanning	Yes
DNS tunneling	Yes

Results – confusion matrix

- 160 techniques, 115 true positive, 45 false positives
- Positive Predictive Value (precision)
  - Chance that an event picked up by our tool is an actual anomaly
  - PPV ~ 0.72
- True Positive Rate (sensitivity)
  - Chance that an anomaly is picked up by our tool and marked as an anomaly
  - TPR ~ 0.94

		Actual	
	Total population	Anomaly	Regular
Predicted	Anomaly	115	45
	Regular	7	N/A

Results – mapping techniques to ICS Killchain

- Network-based techniques mapped to ICS Killchain
- Simulated techniques:
  - Stage 1: Management & Enablement (C2)
  - Stage 1: Sustainment, entrenchment, development & execution (Act)
  - Stage 2: ICS Attack (Install/Modify, Attack)

Conclusions

How can network analysis be used to discover the potential presence of Advanced Persistent Threats (APT) in Industrial Control Systems (ICS)?

- PoC performs well in not missing anomalies (low ratio of false negatives)
  - Ratio of false positives should be improved
  - Additional tuning of the PoC is necessary

Conclusions cont.

How can network analysis be used to discover the potential presence of Advanced Persistent Threats (APT) in Industrial Control Systems (ICS)?

- Mapping anomalies to techniques based on information in ICS Mitre
  - Techniques of APTs provides insights into goals of adversaries
  - Allows defenders to focus on specific defenses
  - Limitation – only known techniques from publicly disclosed incident reports

- Stages of ICS Killchain put techniques into perspective
  - ICS Mitre tactics are not sequential
  - Layer of abstraction, sequence of adversary techniques

Future work

- Support for other ICS protocols
  - E.g. S7Comm Plus, EtherCAT, ProfiNET
- Further testing with other techniques from ICS Mitre
  - Rule enhancement
  - Host-based techniques
- Evaluation on other industrial environments

Questions?

Advanced Persistent Threat detection in Industrial Control Systems

Steffan Roobol sroobol@os3.nl

Dominika Rusek drusek@os3.nl

Github repository https://github.com/StefRoo/ICSMitreAnomalyParser