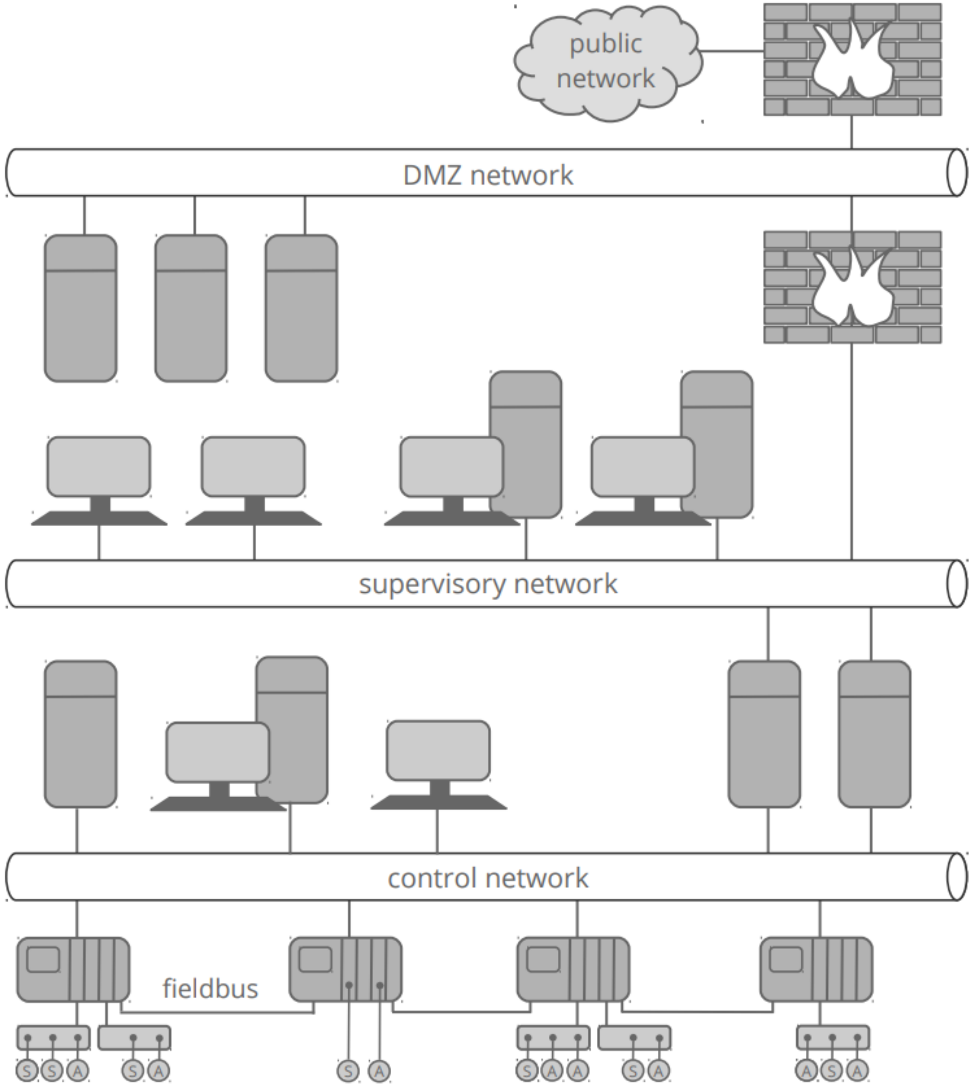
Whitelisting for Characterizing and Monitoring Process Control Communication

17th International Conference on Network and System Security (NSS 2023)

University of Kent, Canterbury, UK | August 14-16, 2023

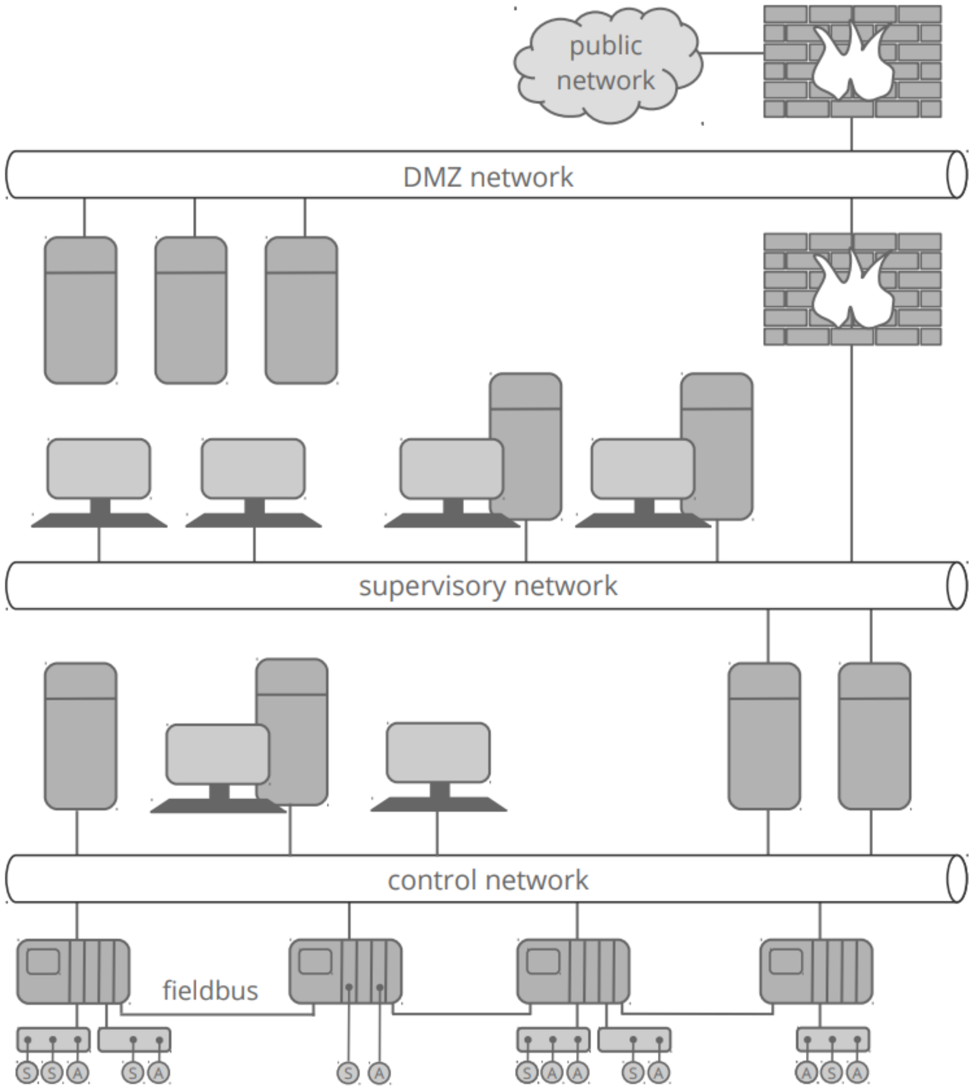
Andreas Paul, Franka Schuster, Hartmut König

OT Networks: Characteristics and challanges



- **Complex and heterogeneous networks**
  - *Devices:* Standard IT vs. embedded systems
  - *Network protocols:* Proprietary vs. TCP/IP
  - Interconnection of different network segments and connection to public networks
- **Highly sensitive environment**
  - *Safety and Availability requirements:* Passive methods only
  - *Secrecy:* Infrastructure and attack information not publicly available
- **Unknown attacks**
  - Explicit description of attacks not useful for attack detection
  - Popular approach: NIDS + anomaly detection

OT Networks: Characteristics and challanges

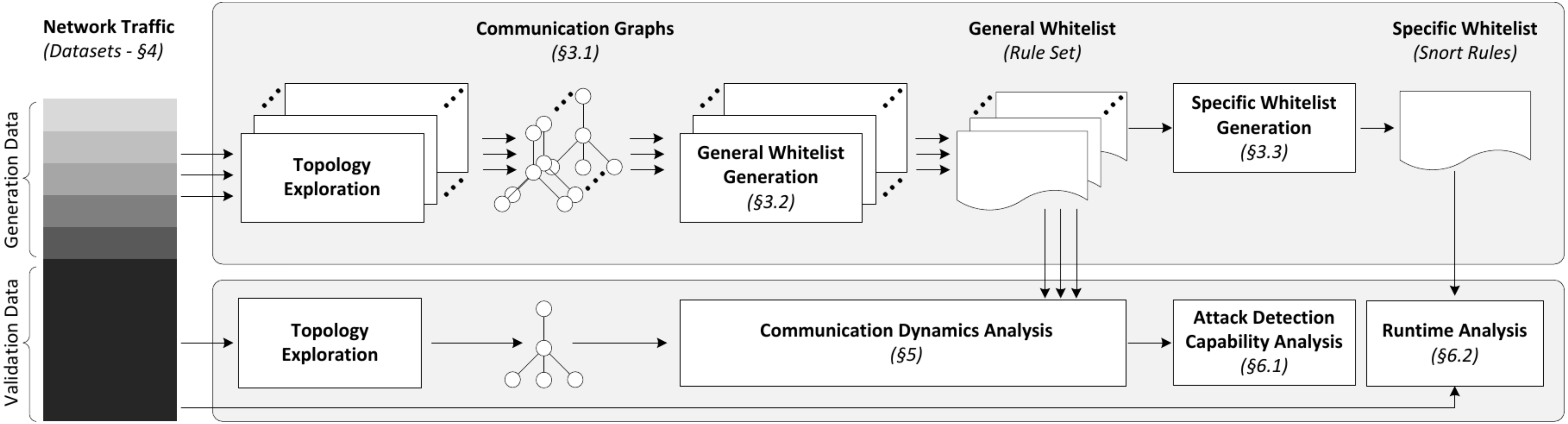


- **Complex and heterogeneous networks**
  - *Devices:* Standard IT vs. embedded systems
  - *Network protocols:* Proprietary vs. TCP/IP
  - Interconnection of different network segments and connection to public networks
- **Highly sensitive environment**
  - *Safety and Availability requirements:* Passive methods only
  - *Secrecy:* Infrastructure and attack information not publicly available
- **Unknown attacks**
  - Explicit description of attacks not useful for attack detection
  - Popular approach: NIDS + anomaly detection

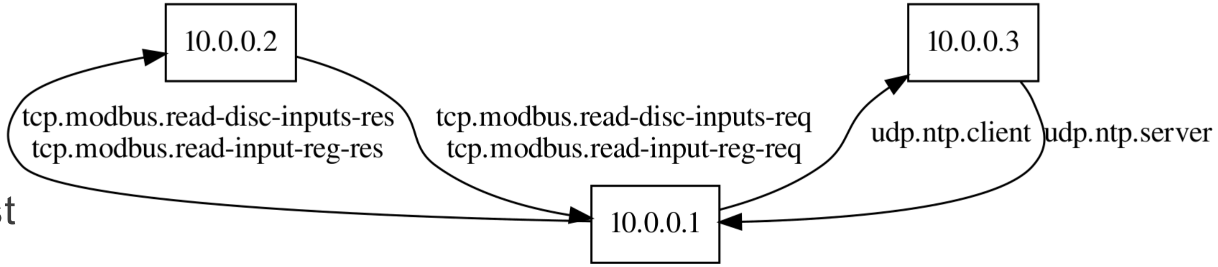
Prerequisite: Well-describable normal behaviour / static network communication → Measurement and analysis of communication dynamics

Simple approach: Communication whitelisting → Automated whitelist generation and efficiency analysis

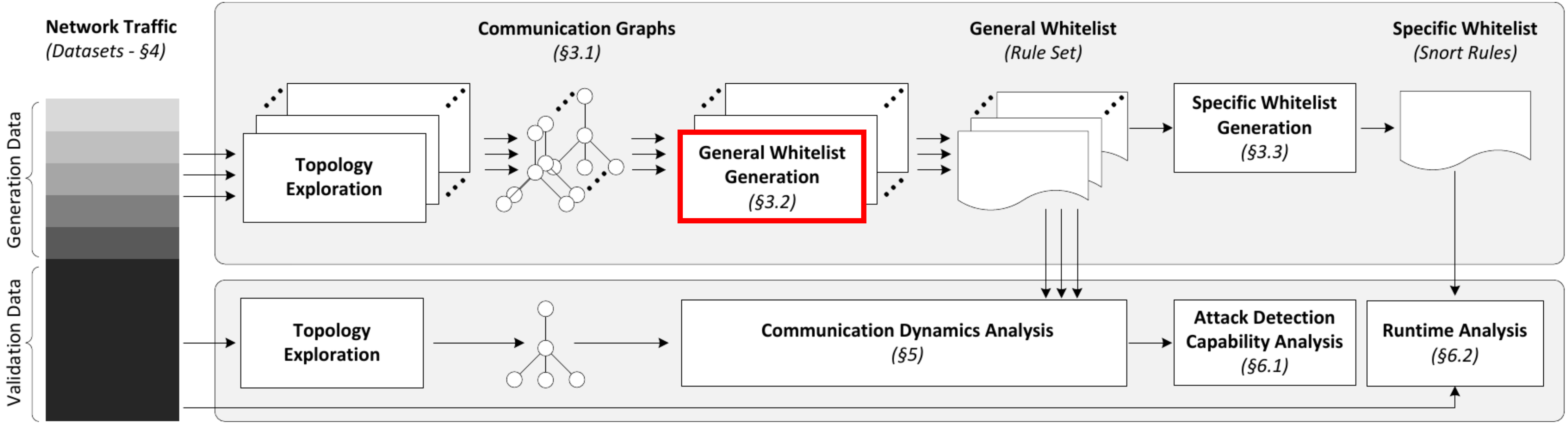
Methodology: Overview



- **Topology exploration** (network traffic preprocessing): automated generation of **communication graphs**
- Type of communication is described by edges
  → Set of all edges can already be considered as a whitelist
- Whitelist: **set of** rules intended to address different aspects of communication separately



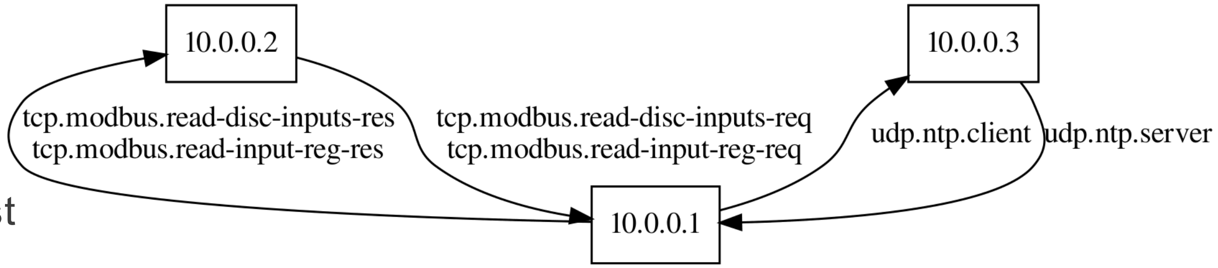
Methodology: Overview



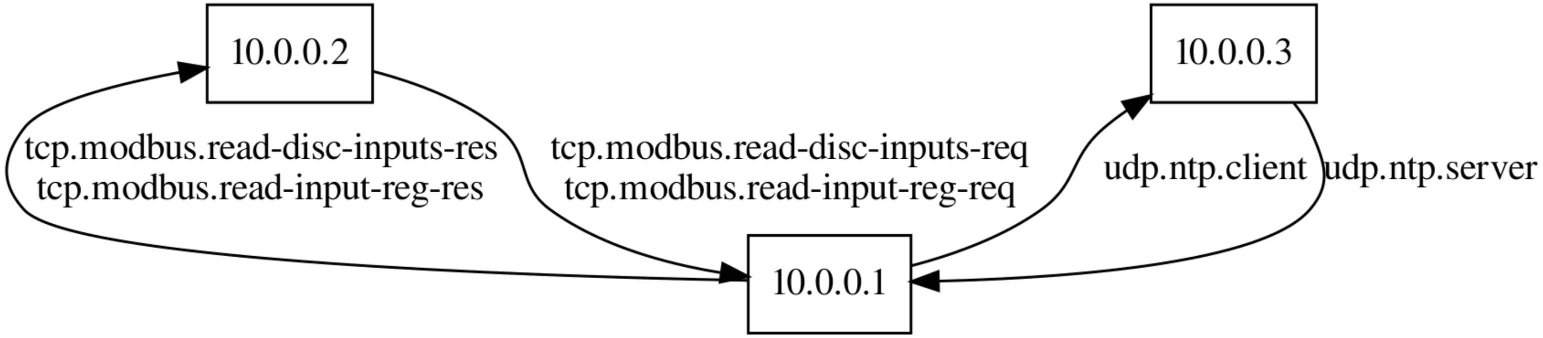
- **Topology exploration** (network traffic preprocessing): automated generation of **communication graphs**

- Type of communication is described by edges
  → Set of all edges can already be considered as a whitelist

- Whitelist: **set of** rules intended to address different aspects of communication separately

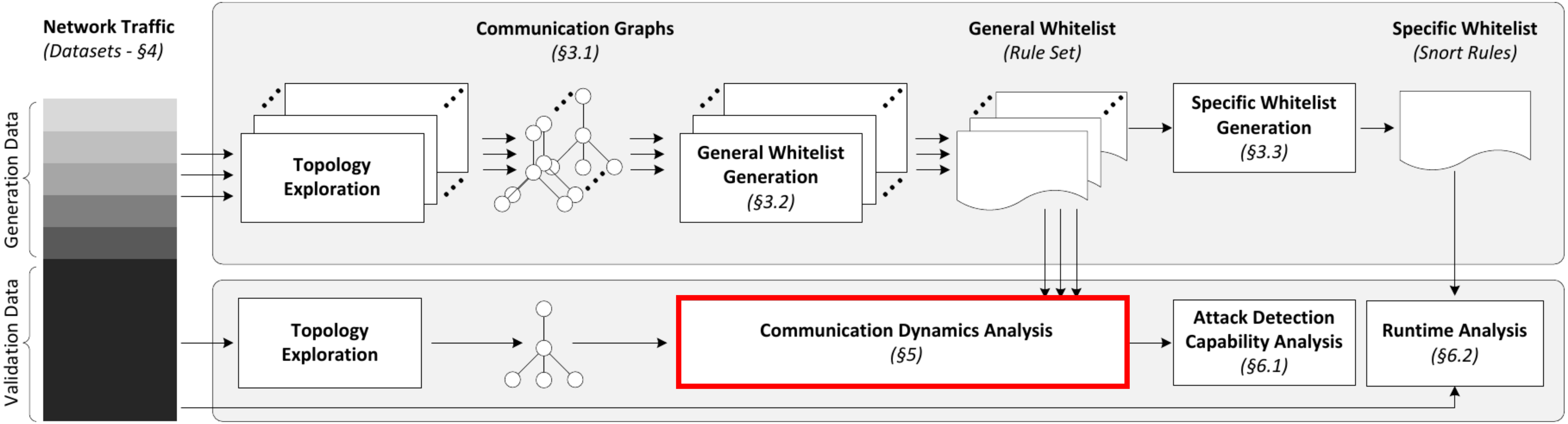


General whitelist generation



Class	Rule set	Rule elements	Example
Device-oriented	r_U	$r = (A_{src}, A_{dst})$	({10.0.0.1, 10.0.0.2, 10.0.0.3}, {10.0.0.1, 10.0.0.2, 10.0.0.3})
	$R_{K_{src}}$	$r = (a_{src}, A_{dst})$	-
	$R_{K_{dst}}$	$r = (a_{src}, A_{dst})$	({10.0.0.1}, {10.0.0.2, 10.0.0.3})
Communication-oriented	R_T	$r = (a_{src}, a_{dst}, T)$	(10.0.0.1, 10.0.0.3, {udp})
	R_P	$r = (a_{src}, a_{dst}, P)$	(10.0.0.1, 10.0.0.2, {modbus})
	R_U	$r = (a_{src}, a_{dst}, U)$	(10.0.0.1, 10.0.0.2, {read-disc-input-res, read-input-reg-res})

Methodology: Communication dynamics analysis

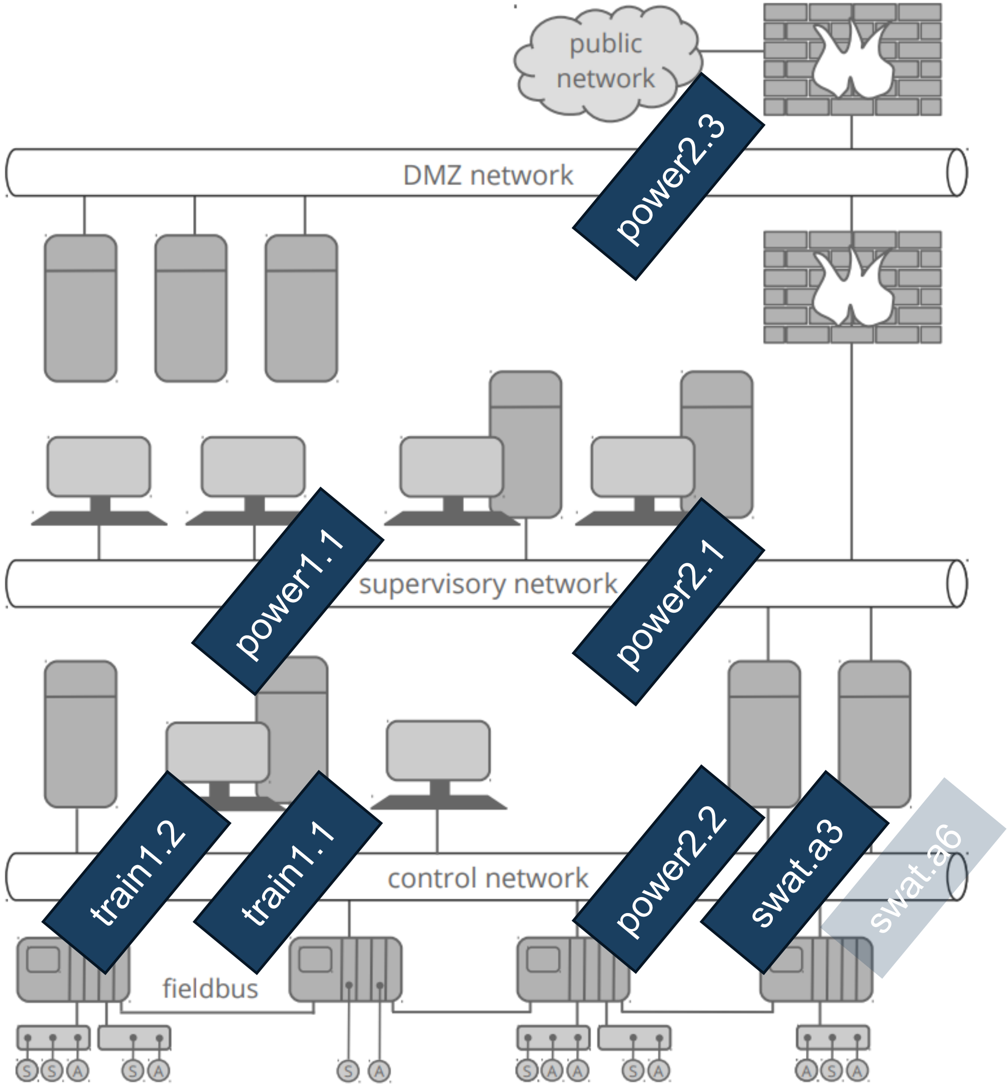


- **Multi-step whitelist generation**
  - generation data is split into n sub-captures
  - per generation step: increasing number of sub-captures used for whitelist generation
  - After each generation step i:
    - Mismatching packet rate (MPR) m_i is determined
    - MPR decrease is determinded: $d_i = m_i - m_{i+1}$ $(1 \leq i < n)$

- **Measures for MPR evolution analysis**

Measure	Meaning	Static communication is indicated by…
$\bar{d}$	Mean MPR decrease	Low value
v	Variation coefficient	High value
g	Gini coefficient (normalized)	High value

Evaluation – Aspect 1: Communication dynamics analysis



Datasets

Dataset	Duration (hh:mm:ss)	#Packets (millions)	Packet rate (k/second)	#Devices
power1.1	02:39:34	90.53	9.46	114
power2.1	02:15:36	66.08	8.12	71
power2.2	01:25:40	6.10	1.19	66
power2.3	17:36:10	83.89	1.32	682
train1.1	01:35:44	17.00	2.96	76
train1.2	02:41:10	9.96	1.03	155
swat.a3	24:12:58	1,248.96	14.00	61
swat.a6	03:40:00	321.03	24.00	98
cicids.17	08:05:36	11.68	0.40	9,727

Communication dynamics analysis: Results (1/2)

Dataset	Network Level	$\frac{\#Triggered\ rules}{\#Total\ rules}$ Device-oriented			Comm.-oriented			#mism. packets	
		r_U	$R_{K_{src}}$	$R_{K_{dst}}$	R_T	R_P	R_U		m_{10}
power1.1	superv.	$\frac{1}{1}$	$\frac{0}{10}$	$\frac{9}{54}$	$\frac{0}{151}$	$\frac{3}{151}$	$\frac{2}{151}$	336 47,604	0.000721 0.102202
power2.1	superv.	$\frac{1}{1}$	$\frac{0}{9}$	$\frac{13}{83}$	$\frac{2}{226}$	$\frac{8}{226}$	$\frac{1}{226}$	366,176 367,188	1.166194 1.169417
power2.2	control	$\frac{0}{1}$	$\frac{0}{5}$	$\frac{1}{68}$	$\frac{0}{222}$	$\frac{0}{222}$	$\frac{2}{222}$	27 31	0.000917 0.001052
power2.3	DMZ	$\frac{1}{1}$	$\frac{19}{109}$	$\frac{96}{514}$	$\frac{18}{3{,}028}$	$\frac{31}{3{,}028}$	$\frac{31}{3{,}028}$	9,146,857 9,187,419	19.463888 19.550202
train1.1	control	$\frac{0}{1}$	$\frac{0}{34}$	$\frac{0}{67}$	$\frac{0}{207}$	$\frac{0}{207}$	$\frac{0}{207}$	0	0.0
train1.2	control	$\frac{1}{1}$	$\frac{1}{50}$	$\frac{12}{123}$	$\frac{1}{270}$	$\frac{1}{270}$	$\frac{0}{270}$	6,252	0.126118
swat.a3	control	$\frac{1}{1}$	$\frac{0}{21}$	$\frac{8}{53}$	$\frac{1}{272}$	$\frac{0}{272}$	$\frac{6}{272}$	57 64	0.000009 0.000011
cicids.17	-	$\frac{1}{1}$	$\frac{1}{40}$	$\frac{2{,}796}{7{,}065}$	$\frac{88}{27{,}145}$	$\frac{1{,}326}{27{,}145}$	$\frac{16}{27{,}145}$	1,592,881 1,593,120	54.123183 54.131304

Communication dynamics analysis: Results (2/2)

Dataset	Network Level	$\frac{\#Triggered\ rules}{\#Total\ rules}$						#mism. packets	MPR Evolution			
		Device-oriented			Comm.-oriented							
		r_U	$R_{K_{src}}$	$R_{K_{dst}}$	R_T	R_P	R_U		m_{10}	$\bar{d}$	v	g
power1.1	superv.	$\frac{1}{1}$	$\frac{0}{10}$	$\frac{9}{54}$	$\frac{0}{151}$	$\frac{3}{151}$	$\frac{2}{151}$	336 47,604	0.000721 0.102202	0.000532 0.000534	1.697286 1.686094	0.827277 0.819754
power2.1	superv.	$\frac{1}{1}$	$\frac{0}{9}$	$\frac{13}{83}$	$\frac{2}{226}$	$\frac{8}{226}$	$\frac{1}{226}$	366,176 367,188	1.166194 1.169417	0.000731	1.388637	0.772760
power2.2	control	$\frac{0}{1}$	$\frac{0}{5}$	$\frac{1}{68}$	$\frac{0}{222}$	$\frac{0}{222}$	$\frac{2}{222}$	27 31	0.000917 0.001052	0.005911	2.747624	0.991066
power2.3	DMZ	$\frac{1}{1}$	$\frac{19}{109}$	$\frac{96}{514}$	$\frac{18}{3,028}$	$\frac{31}{3,028}$	$\frac{31}{3,028}$	9,146,857 9,187,419	19.463888 19.550202	0.569613 0.570594	2.312673 2.309209	0.946033 0.945694
train1.1	control	$\frac{0}{1}$	$\frac{0}{34}$	$\frac{0}{67}$	$\frac{0}{207}$	$\frac{0}{207}$	$\frac{0}{207}$	0	0.0	0.000631	2.649324	0.985537
train1.2	control	$\frac{1}{1}$	$\frac{1}{50}$	$\frac{12}{123}$	$\frac{1}{270}$	$\frac{1}{270}$	$\frac{0}{270}$	6,252	0.126118	0.397197	2.821426	0.998874
swat.a3	control	$\frac{1}{1}$	$\frac{0}{21}$	$\frac{8}{53}$	$\frac{1}{272}$	$\frac{0}{272}$	$\frac{6}{272}$	57 64	0.000009 0.000011	0.000177 0.008177	2.797246 2.827717	0.996615 0.999923
cicids.17	-	$\frac{1}{1}$	$\frac{1}{40}$	$\frac{2,796}{7,065}$	$\frac{88}{27,145}$	$\frac{1,326}{27,145}$	$\frac{16}{27,145}$	1,592,881 1,593,120	54.123183 54.131304	2.941505 2.940656	0.847902 0.848042	0.477112

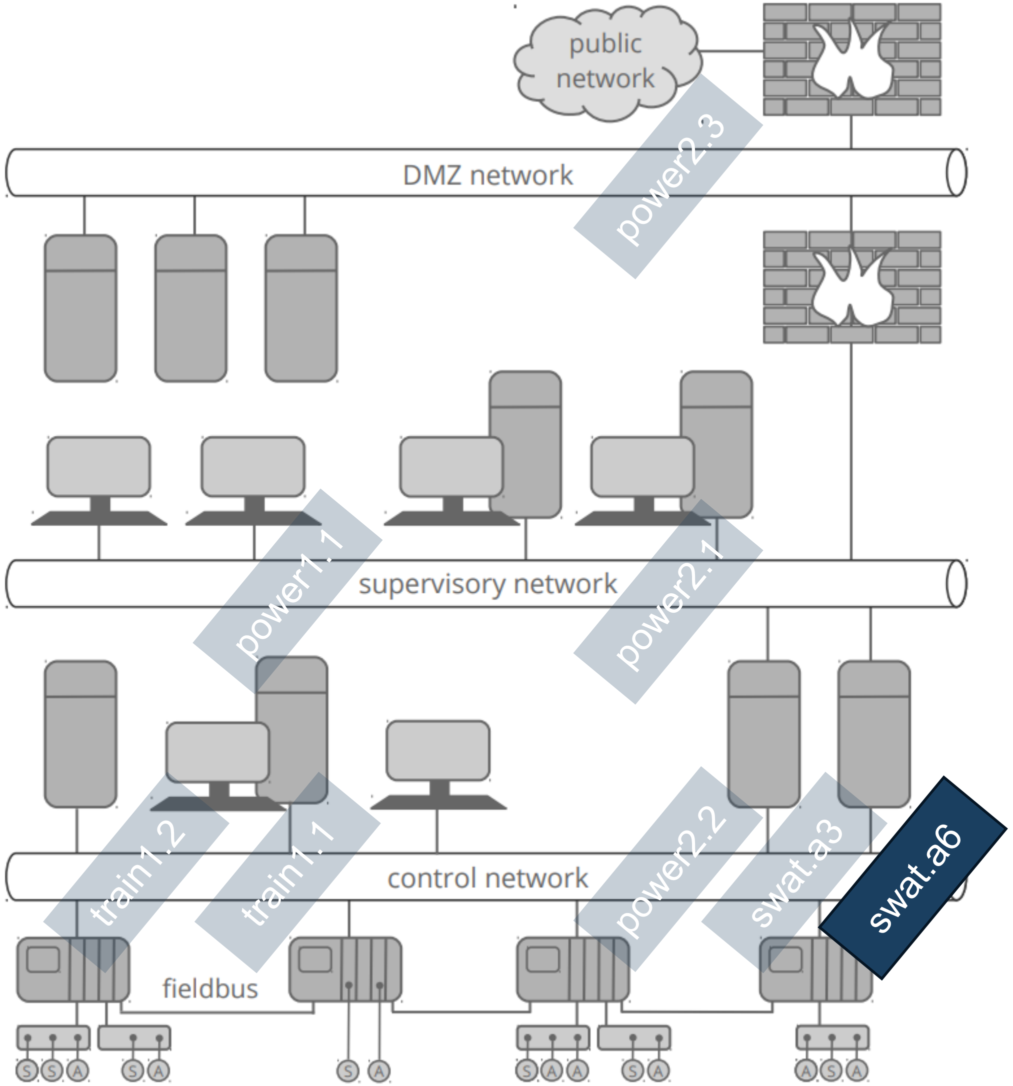
Communication dynamics analysis: Findings

- **Different OT network layers exhibit different (measurable) communication dynamics**
  - Clustering based on dispersion measures (v, g) allows traffic to be assigned to a network layer
  - The lower the network layer, the smaller the differences in communication dynamics among different networks of the same layer

- **Strong correlation between communication dynamics and whitelist completion effort**
  - Extreme cases: n rules or 1 rule is responsible for logging n packets
  - Negative correlation about -0.81 between the proportion of triggering rules from the total amount of rules and v, g
    → The more static the communication, the lower the proportion of triggering rules

- **Detection of whitelist violations is dominated by device-oriented rules**
  - The majority of whitelist mismatching packets are logged by communication-oriented rules in case of one dataset (power1.1)
  - For the other datasets, between 61% and 98% of the logged packets are detected by device-oriented rules
    → Dominated by rule set $R_{K_{src}}$

Evaluation – Aspect 2: Attack detection capability

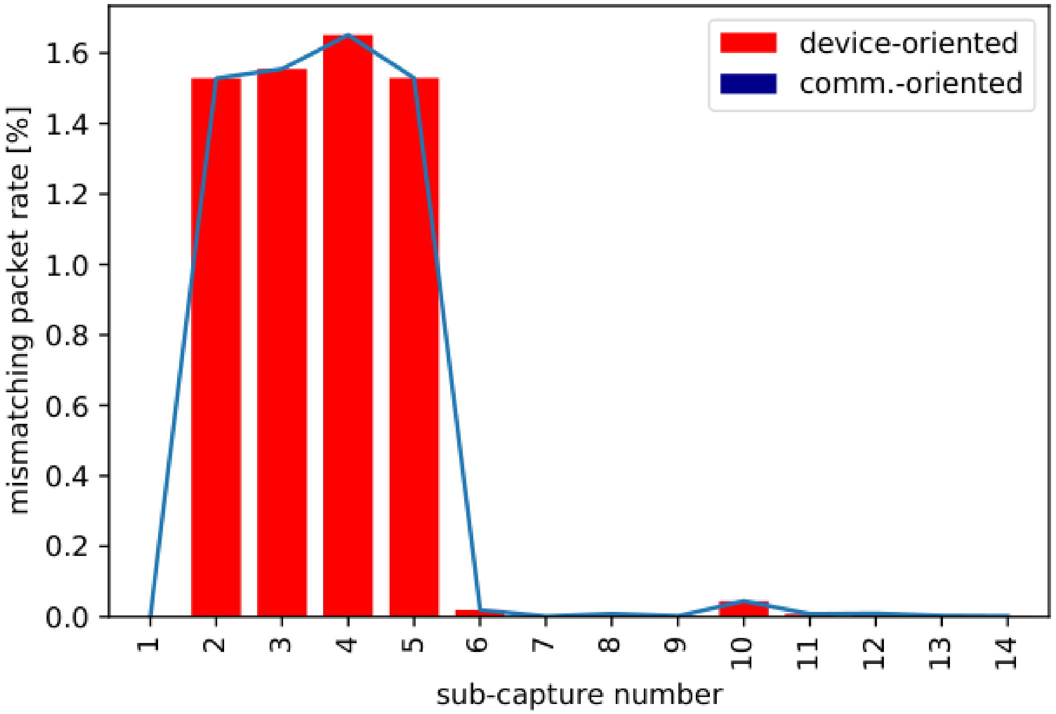


Datasets

Dataset	Duration (hh:mm:ss)	#Packets (millions)	Packet rate (k/second)	#Devices
power1.1	02:39:34	90.53	9.46	114
power2.1	02:15:36	66.08	8.12	71
power2.2	01:25:40	6.10	1.19	66
power2.3	17:36:10	83.89	1.32	682
train1.1	01:35:44	17.00	2.96	76
train1.2	02:41:10	9.96	1.03	155
swat.a3	24:12:58	1,248.96	14.00	61
swat.a6	03:40:00	321.03	24.00	98
cicids.17	08:05:36	11.68	0.40	9,727

Attack detection capability: Analysis of the swat.a6 dataset (1/3)

Total MPR

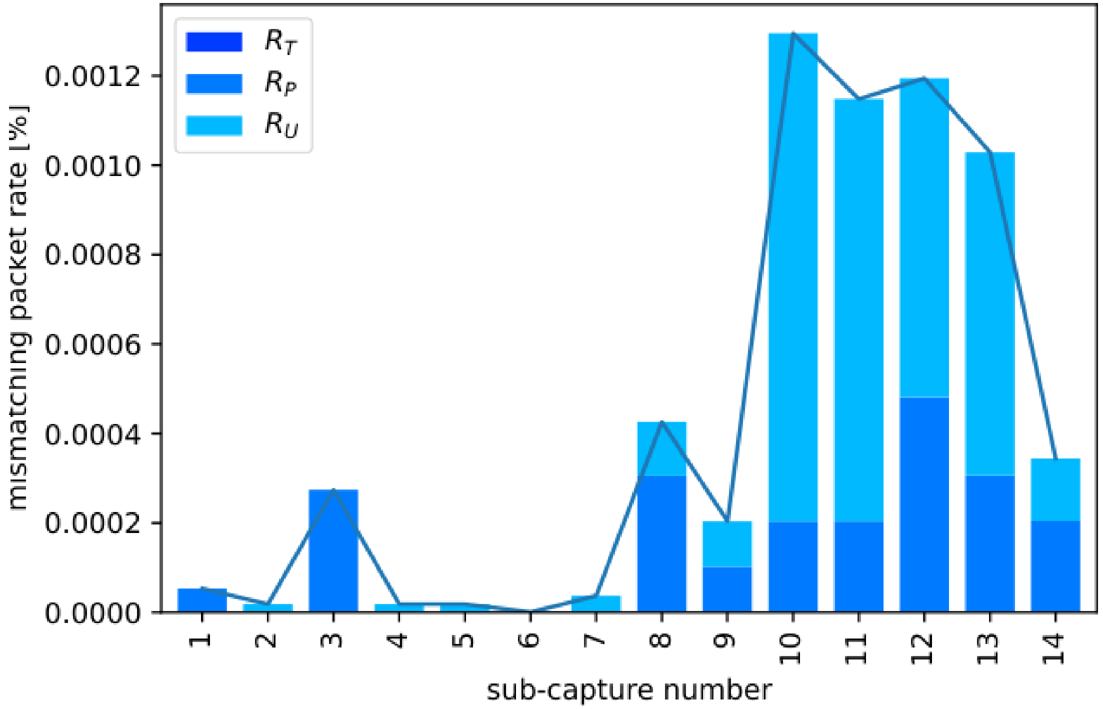


- Dataset is devided into 15 sub-captures (0-14)
- Whitelist was generated from *sub-capture 0*
- Chart: Individual analysis of the remaining sub-captures by determining the total MPR

- **Attack activities**
  - *Sub-capture 1:* Infiltrate SCADA Workstation via USB thumb drive with first malware
  - *Sub-captures 2-5:* Data exfiltration
  - *Sub-capture 10:* Infiltrate SCADA Workstation with second malware, via downloading from C2 Server
  - *Sub-captures 11-13:* Sensor/Actuator disruption

Attack detection capability: Analysis of the swat.a6 dataset (2/3)

Communication-based MPR



- Dataset is devided into 15 sub-captures (0-14)
- Whitelist was generated from *sub-capture 0*
- Chart: Individual analysis of the remaining sub-captures by determining the communication-based MPR

- **Attack activities**
  - *Sub-capture 1:* Infiltrate SCADA Workstation via USB thumb drive with first malware
  - *Sub-captures 2-5:* Data exfiltration
  - *Sub-capture 10:* Infiltrate SCADA Workstation with second malware, via downloading from C2 Server
  - *Sub-captures 11-13:* Sensor/Actuator disruption

Attack detection capability: Analysis of the swat.a6 dataset (3/3)

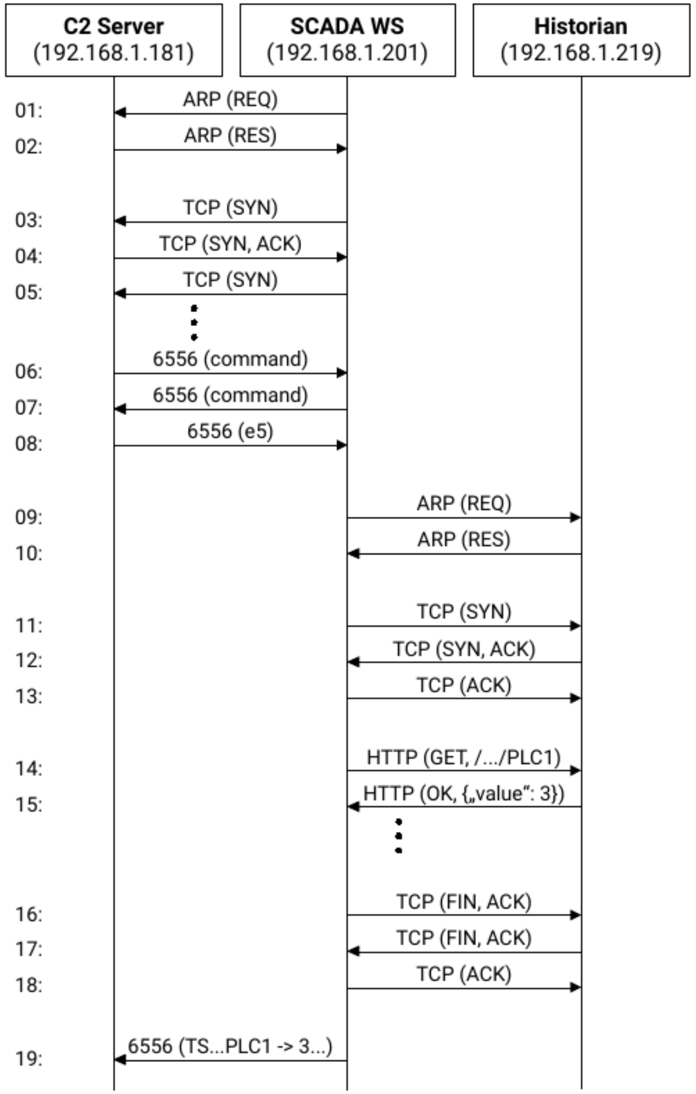
Principle of the data exfiltration attack

1. *Messages 1-5:* TCP connection establishment on Port 6556 from SCADA Workstation to C2 Server

2. *Messages 6-8:* Command transmission from C2 Server to SCADA Workstation

3. *Messages 9-18:* Process data requests from SCADA Workstation to Historian via HTTP

4. *Message 19:* Data transmission from SCADA Workstation to C2 Server



Final remarks

- **Communication dynamics of OT networks**
  - OT networks have a (measurable) static communication behaviour compared to IT networks
  - Completeness of a whitelist cannot be guaranteed, even after an extended learning period
  - Assessment: Manageable effort to create and maintain a complete whitelist, especially at lower OT network layers
- **Whitelist benefits**
  - Interpretability: By knowing the triggering rule, attacks can be specifically traced
  - Extensibility: Automatically generated whitelists can be easily extended (manually or automatically)
  - Efficiency: Simple means to limiting an attacker's options for action
- **Application of the approach and future work**
  - Creation of a specific whitelist to support existing products (e.g. open-source solutions such as Snort)
  - Provide a baseline for advanced analysis techniques

Thank you for your attention!

Questions? Remarks?

Contact information:

E-Mail: andreas.paul@codewerk.de