MONDRAGON UNIBERTSITATEA

GOI ESKOLA POLITEKNIKOA
FACULTY OF ENGINEERING

Visualizing Network Flows and Related Anomalies in Industrial Networks using Chord Diagrams and Whitelisting

M. Iturbe, I. Garitano, U. Zurutuza, R. Uribeetxeberria

Electronics & Computing Department
Faculty of Engineering
Mondragon University

IVAPP 2016, Rome, Italy

Agenda

1. Introduction

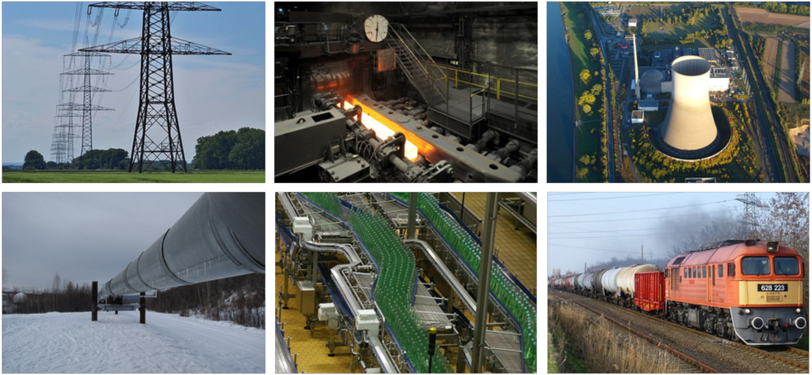
2. System Description

3. Results

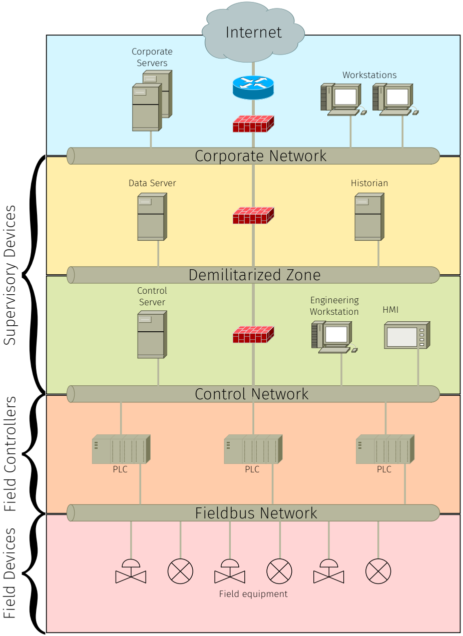
4. Conclusions

Introduction

Industrial Control Systems



CC-BY-SA 3.0 Kreuzschnabel, Schmimi1848, Wolkenkratzer, Brian Cantoni, Hermann Luyken, Beroesz


Internet
Corporate Servers
Workstations
Corporate Network
Data Server
Historian
Demilitarized Zone
Control Server
Engineering Workstation
HMI
Control Network
PLC
PLC
PLC
Fieldbus Network
Field equipment
Supervisory Devices
Field Controllers
Field Devices

ICS vs. IT

	Industrial Networks	IT Networks
Main Purpose	Control of Physical equipment	Data processing and transmission
Failure Severity	High	Low
Reliability Required	High	Moderate
Determinism	High	Low
Data Composition	Small packets of periodic and aperiodic traffic	Large, aperiodic packets
Average Node Complexity	Low (simple devices, sensors, actuators)	High (large servers/file systems/databases)

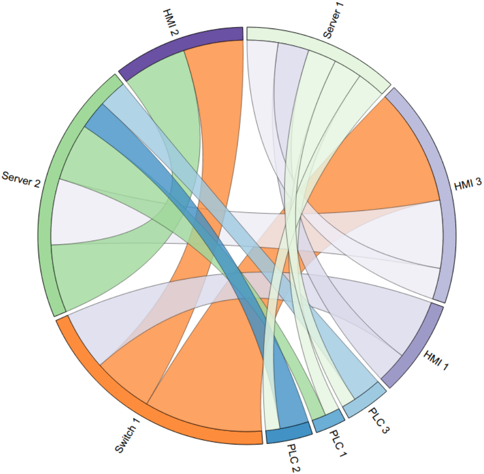
Whitelisting

Refers to the practice of registering the set of network flows that are allowed in a network, raising an alarm or disallowing connections that have not been explicitly allowed.

Whitelisting

- Recommended security measure by the industry.
- Barbosa et al. [1] demostrated its efficiency to detect flow anomalies.

Chord diagrams



Chord diagrams

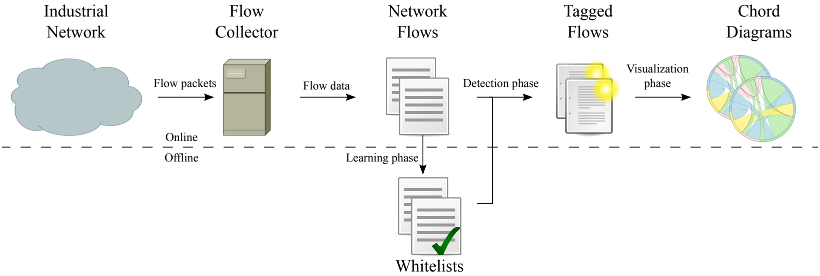
- Conceived initially for genomics
- Previous usage on security visualizations
    - ADS visual comparison [4]
    - Relationships between Phishing websites [3]
    - Relationships between IT subnets [2]

Objectives

- Gaps in related literature
  - No security visualizations for Industrial Networks
  - Previous works based on whitelisting only detect forbidden connections
- Objectives
  - Provide situational awareness through flow visualizations
  - Design a visual flow anomaly detection system
  - Detect flow anomalies through temporal whitelists
  - Visually highlight detected anomalies

System Description

Overview


Industrial Network
Flow Collector
Network Flows
Tagged Flows
Chord Diagrams
Flow packets
Flow data
Detection phase
Visualization phase
Online
Offline
Learning phase
Whitelists

Learning Phase

- Whitelists are formed with the detected network traffic.
- Source/Destination IP, Server port, IP protocol and packet number
- Whitelists of variable time length.

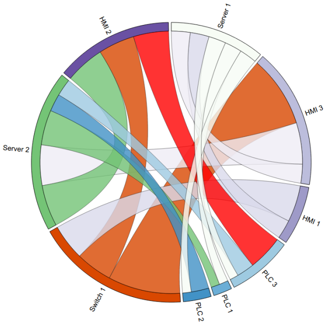
Detection Phase

- The system evaluates and tags incoming flows comparing them to the whitelists
- Types of tags
  - Legitimate flow
  - Anomalous flow
  - Incorrect port
  - Incorrect protocol
  - Absent flow
  - Anomalous flow size
- The system triggers an alarm if a non-legitimate flow is detected

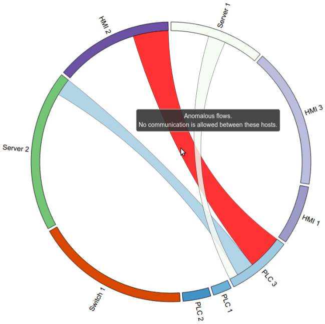
Visualization Phase

- The system builds the diagrams based on the tagged flows:
  - A host → A section in the circumference
  - Each host type has a distinctive color group
  - A bidirectional flow → A chord
  - Chords inherit the color of the more active host in the communication
- Highlights non-legitimate flows:
  - Missing flows, in black
  - The rest, in red

Visualization Phase



(a) Forbidden flow between PLC 1 and HMI 2.

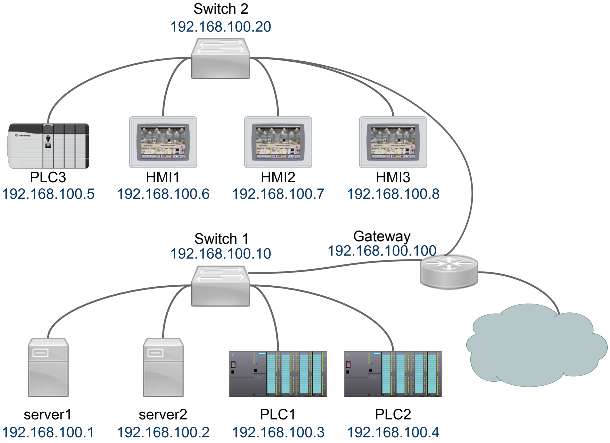


Anomalous flows.
No communication is allowed between these hosts.

(b) Detail of the forbidden flow.

Results

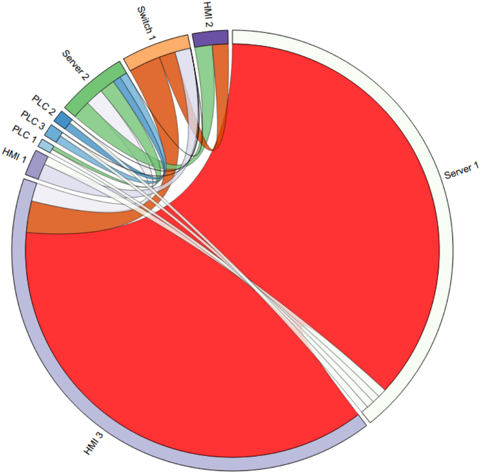
Test network



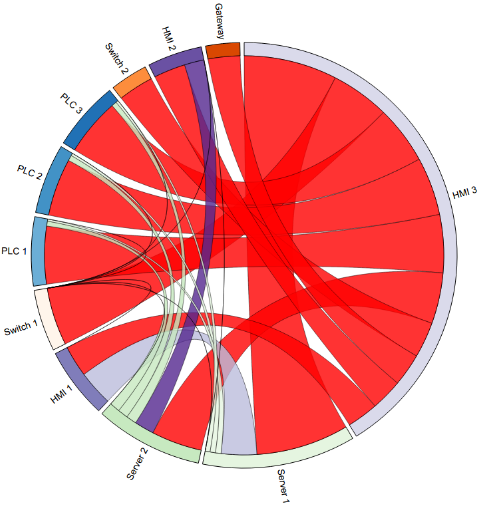
Tools

- NetFlow v5
- Logstash
- ElasticSearch
- D3

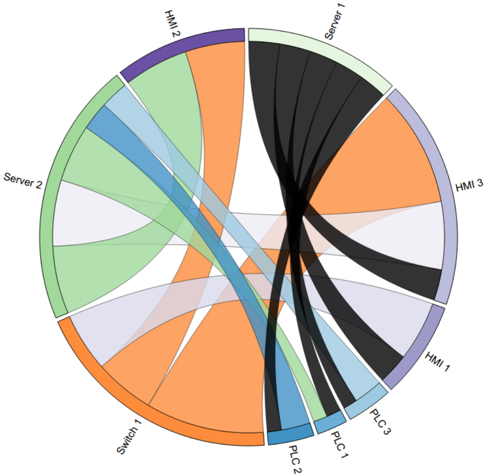
Denial of Service



Network scan



Downed host



Conclusions

Conclusions

- We propose a visual monitoring system based on whitelists and chord diagrams for ICSs.
- Collected flows in a time window are tagged and visualized.
    - Highlighting anomalous ones.

Future work

- Distinguish more anomalous flow types.
- Research into re-creation of whitelists or its edition consequences.

Thank you.

{miturbe,igaritano,uzurutuza,ruribeetxeberria}

@mondragon.edu

References I

- Rafael Ramos Regis Barbosa, Ramin Sadre, and Aiko Pras.
  Flow Whitelisting in SCADA Networks.
  International Journal of Critical Infrastructure Protection, 6(3):150–158, 2013.

- Siming Chen, Cong Guo, Xiaoru Yuan, Fabian Merkle, Hanna Schaefer, and Thomas Ertl.
  OCEANS: online collaborative explorative analysis on network security.
  In *Proceedings of the Eleventh Workshop on Visualization for Cyber Security*, pages 1–8. ACM, 2014.

References II

- Robert Layton, Paul Watters, and Richard Dazeley.
Unsupervised authorship analysis of phishing webpages.
In *Communications and Information Technologies (ISCIT), 2012 International Symposium on*, pages 1104–1109. IEEE, 2012.

- Johan Mazel, Romain Fontugne, and Kensuke Fukuda.
Visual comparison of network anomaly detectors with chord diagrams.
In *Proceedings of the 29th Annual ACM Symposium on Applied Computing*, pages 473–480. ACM, 2014.