Protection Against Cyber-Attacks: Introducing Resilience for SCADA Networks

Dr. Antonios Gouglidis
a.gouglidis@lancaster.ac.uk

Symposium on Innovative Smart Grid Cybersecurity Solutions
Vienna, Austria, 13th-14th March, 2017
Outline

• **Cyber-Attacks on Critical Infrastructures**

• **Resilience Strategy**

• **Resilience for SCADA networks**
  - Resilience Policies & Resilience Architecture

• **Results & Questions**
Cyber-attacks on Critical Infrastructures
Cyber-threats & actors to CI

- Cyber-threat
  - Unauthorised access
  - Loss of security
  - Loss of safety

- Threat actors
  - Script kiddies, hackers ...
  - Major firms / organisations ...
  - Cyber warfare
Likelihood vs. consequence*

Attack vectors
Resilience Strategy
Resilience and ways of achieving it...

• ‘... the ability of a network/system to defend against and maintain an acceptable level of service in the presence of challenges.’ *

• D²R²+DR
  – Real-time control (internal) loop
  – Background (external) loop

Common network architecture

- Internet
  - Data centre / Cloud
  - Applications, analytics, etc.
  - Users
  - Enterprise network
    - Remote access
  - Industrial network
    - Controller
      - Sensors fieldbus
        - Pump
        - Valve
        - Indicator
      - System fieldbus
        - PLC
        - HMI
        - Controller
  - Historian, SCADA server, etc.
Viewpoints for critical infrastructures

- Organisation
- Technology
- Individual
Resilience in Access Control Policies
Resilience in access control is the ability of a system not to restrict, but to enable access
Resilience policies – tool chain

Access control policy tool (ACPT)

Model in NuSMV +

Resilience specifications

NuSMV model checker

Detected resilience violations
Resilience Architecture for CI
Anomaly detection framework

Field Site(s)

Captured data

Pre-processing

Enterprise Network

Captured data

Pre-processing

Data - features

Anomaly Detector
As A Service

Notifications

13th – 14th March, 2017
Symposium on Innovative Smart Grid Cybersecurity Solutions
Resilience architecture

Defend

Physical infrastructure

Management plane

Detect

Monitoring plane

Detection plane

Preprocessing

Internal storage of monitoring metrics

AD_{Ind} AD_{Org} AD_{Tech}

Statistical model

Offline/Online Anomaly Detection Techniques

Predicted class

Analysis plane

Coarse-grain

Fine-grain

Policy engine

Logging results

events

Remediate & Recovery

apply update

re-configuration actions

WP3 – Deliverable 3.4

Symposium on Innovative Smart Grid Cybersecurity Solutions

13th – 14th March, 2017
Results and Discussion
Evaluation of SCADA attacks


• Gas pipeline log, captured in a laboratory environment, including:
  – Normal operation
  – Cyber-attacks
    • Reconnaissance
    • Denial-of-Service
    • Command injection
Comparison of techniques

- K-Means
- Naive bayesian
- Principal Component Analysis
- Gaussian Mixture Model
- Data density

Precision and Accuracy

13th – 14th March, 2017 Symposium on Innovative Smart Grid Cybersecurity Solutions
Questions?

Protection Against Cyber-Attacks: Introducing Resilience for SCADA Networks

Dr. Antonios Gouglidis
a.gouglidis@lancaster.ac.uk

Symposium on Innovative Smart Grid Cybersecurity Solutions
Vienna, Austria, 13th-14th March, 2017