A Multi-Level Approach to Resilience of Critical Infrastructures and Services

Antonios Gouglidis

2nd HyRiM End User Workshop
Barcelona, 15.11.2016
Contents

• Motivation

• Resilience

• Proposed architecture

• Evaluation results

• Concluding remarks
Motivation

• Protection of Critical Infrastructures

• Threats on the rise – Serious cyber attack believed likely

• Investigate threats

• Provide foundations
  – Novel protection mechanisms
... a typical attack ...
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

Viewpoints for utility networks
Resilience architecture

Defend

Physical infrastructure

C_{Ind}

C_{Org}

C_{Tech}

Monitoring plane

Preprocessing

Internal storage of monitoring metrics

AD_{Ind}

AD_{Org}

AD_{Tech}

Detection plane

Statistical model

Offline/Online Anomaly Detection Techniques

Predicted class

Analysis plane

Loggin results

Coarse-grain

Fine-grain

Policy engine

Remediate & Recovery

apply update

re-configuration actions
What metrics to measure?

- **Periodic**: Measure security control maturity and performance
  - E.g., Percentage of applications and systems subject to security testing
  - Challenge: High-level with long-term validation requirements

- **Real-Time**: Provide indicators of real-time threats
  - E.g., number of un-authorised access attempts, network throughput
  - Challenge: Conversion of measurements to representative metrics
#### Examples of Threats and Metrics

<table>
<thead>
<tr>
<th>Threat</th>
<th>Metrics</th>
<th>OTI Level</th>
<th>Collector</th>
</tr>
</thead>
<tbody>
<tr>
<td>BYOD</td>
<td>No. of connected personal devices&lt;br&gt;No. of invalid running applications</td>
<td>Organisation&lt;br&gt;Individual</td>
<td>$C_{Org}$&lt;br&gt;$C_{Ind}$</td>
</tr>
<tr>
<td>Remote Access</td>
<td>No. of active remote connections</td>
<td>Organisation</td>
<td>$C_{Org}$</td>
</tr>
<tr>
<td>Spear Phishing</td>
<td>No. of spam e-mail</td>
<td>Individual</td>
<td>$C_{Ind}$</td>
</tr>
<tr>
<td>Network Scanning</td>
<td>No. of packets&lt;br&gt;No. of bytes&lt;br&gt;No. of active flows</td>
<td>Technical&lt;br&gt;Technical</td>
<td>$C_{Tech}$&lt;br&gt;$C_{Tech}$&lt;br&gt;$C_{Tech}$</td>
</tr>
<tr>
<td>Malware</td>
<td>Process utilisation&lt;br&gt;Memory utilisation</td>
<td>Technical</td>
<td>$C_{Tech}$&lt;br&gt;$C_{Tech}$&lt;br&gt;$C_{Tech}$</td>
</tr>
</tbody>
</table>
Evaluation Testbed

- Two hosts with Kernel Virtual Supervisor
- Apache HTTP daemon
- Volatility introspection library
- 10-minutes runs
- Anomaly Detection Techniques
  - K-Means
  - Principal Component Analysis
Evaluation

ASG for SpearPhish using K-means

ASG for Malware (Zeus) using PCA

ASG for RemoteAccess using K-means

ASG for Netscan using PCA

Day 1

Day 2

Day 3
Evaluation of SCADA attacks


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

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

**Precision vs. Accuracy**

15.11.2016 2nd HyRiM End User Workshop, Barcelona
Conclusion and Future Steps

- Currently offering monitoring and detection services
  - Data Density algorithm
    - Unsupervised and memory less

- Identify threats using the OTI viewpoints

- Integrate our testbed/platforms

- Investigate the analysis and management planes
Questions?