RICS-el: Building a National Testbed for Research and Training on SCADA Security

Magnus Almgren, Peter Andersson, Gunnar Bjorkman, Mathias Ekstedt, Jonas Hallberg, Simin Nadjm-Tehrani, and Erik Westring
A five year national project

- Three collaborating universities
  - KTH
  - Chalmers
  - Linköping university
    (Project leader)
Working together with FOI,
Swedish defence research agency
at Linköping
Motivation
SCADA systems are complex

Photo by Rich Pedronelli (AP)
Combination of IT and OT elements

• Typical architectural pattern

• Many different protocols/vendors

• Real environments
  – Patchwork
  – Long life cycles
Cyber threats to availability and reliability

https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
Research gap

• Theory/prototypes -- Real world

Practitioners:
  – Is my system secure enough?
  – What are my risk reduction options?

Researchers:
  – Is my method better than others?
Other testbeds

• For power engineering research and education
• For training and competence development
  – EU projects (e.g. CRUTIAL), US national labs
RICS-el Testbed in Linköping
Current state...
Major elements

• Real SCADA vendor product
  – with HMI, historian, SCADA front-end
  – Power network simulator

• Operations network (WAN) with multiple RTUs, communicating with the IEC-60870-5-104 protocol

• Office network with work stations, servers realised on the CRATE cyber range at FOI
Data generation & Training exercises
Research with RICS-el data so far...

• CRITIS 2017:
  – Anomaly detection for synchronous streams

• CPSS 2018: Spontaneous data streams
  – Three types of analysis
    • Phase transition analysis
    • Predictability analysis
    • Frequent patterns analysis
Overview of datasets

- Extracted event sets for timing analysis of the IEC-104 data streams

<table>
<thead>
<tr>
<th>Traces</th>
<th>Duration</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>KTH-RTU1</td>
<td>6 days</td>
<td>468,199KB</td>
</tr>
<tr>
<td>KTH-RTU4</td>
<td>6 days</td>
<td>278,519KB</td>
</tr>
<tr>
<td>RICS</td>
<td>10 days</td>
<td>448,002KB</td>
</tr>
</tbody>
</table>

Emulated for CPSS 2016 paper
Training exercises

- October 2017:
  - iPilot exercise where Swedish nuclear power IT/OT teams defended attacked networks
  - Observers from 30 countries organised through IAEA
Conclusions

• There is an immediate payoff in terms of repeatable experiments
• Much longer data streams can now be created for research
• Ongoing work: creating OT bots and attacker bots
Reference group & collaborators

- Critical infrastructure operators
- Control system vendors
- Cyber security product vendors and consultants
- Agencies, standardisation bodies, awareness raising organisations
Questions?

www.rics.se