DEVELOPING SITUATIONAL AWARENESS FOR INDUSTRIAL CONTROL SYSTEM NETWORKS

Jarkko Holappa
Lead Security Consultant, GI CSP, CISSP
INTRODUCTION
Nixu: One-stop shop for high-end cyber security consulting

- Security consulting since 1988
- Capacity and reliability: 140 persons, 17 M€ turnover
- Secure premises: Finnish Defence Forces audited facilities
- No strings attached: Product vendor independent
- Certifications: CISSP, CISA, CISM, CSSLP, CPTS, GCIH, GICSP, GCFA, GCIA, GSNA, GSSPC, CCNA, ISO27001 Auditor, MCSE, QSA, PA-QSA, etc
- Payment Card Industry (PCI DSS) Qualified Security Assessor and ASV company
- c. 140 clients in over 400 assignments during year 2013
- Assignments in around 20 countries

Delivery models: Advisory assignment – Implementation project – Assessment – Continuous Service
**Figure 3: Key barriers in adopting the Industrial Internet**

**Q: What are the greatest barriers inhibiting business from adopting the industrial Internet?**

<table>
<thead>
<tr>
<th>Barrier</th>
<th>Overall</th>
<th>North America (n=43)</th>
<th>Europe (n=30)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of interoperability or standards</td>
<td>65%</td>
<td>60%</td>
<td>67%</td>
</tr>
<tr>
<td>Security concerns</td>
<td>72%</td>
<td>64%</td>
<td>72%</td>
</tr>
<tr>
<td>Uncertain ROI (e.g., insufficient business cases)</td>
<td>53%</td>
<td>60%</td>
<td>53%</td>
</tr>
<tr>
<td>Legacy equipment (e.g., no connectivity or embedded sensors)</td>
<td>38%</td>
<td>50%</td>
<td>47%</td>
</tr>
<tr>
<td>Technology immaturity (e.g., large-scale analytics)</td>
<td>24%</td>
<td>21%</td>
<td>27%</td>
</tr>
<tr>
<td>Privacy concerns</td>
<td>19%</td>
<td>14%</td>
<td>20%</td>
</tr>
<tr>
<td>Lack of skilled workers (e.g., data scientists)</td>
<td>15%</td>
<td>12%</td>
<td>20%</td>
</tr>
<tr>
<td>Societal concerns (e.g., economic dislocation)</td>
<td>3%</td>
<td>5%</td>
<td>3%</td>
</tr>
</tbody>
</table>

Source: World Economic Forum Industrial Internet Survey, 2014
Why Cyber Security Situational Awareness for Control Systems?

- Getting visibility to enterprise IT is essential from business, operational security and risk management perspective.

- Why would you want to leave your industrial control system out from this? (aka 21 Misconceptions)?
  - “Nobody Wants to Attack Us”
  - “We Only Have Obscure Protocols/systems”
  - “Cybersecurity Incidents Will Not Impact Operations”
  - “One-Way Communication Offers 100% Protection”
  - “Serial-Link/4–20 mA Wire Communications are Immune”
  - “Vendors Have a Full Command of Their Products Security”
  - “It’s Certified, It’s Secured”
  - …

- Why not to leave out?
  - Cannot manage [cyber] business risks, if you don’t know what is happening in your production environment
  - Improves process predictability and robustness

---

Updating ICS systems

Networking

- Process control systems
- IT/Office systems

Patch-level
Updating ICS systems
Cyber security situational awareness

= To detect attacks that have gotten through defences

= To detect deviances in the process
- Internet
  - Remote access

- Enterprise
  - Office workstations
  - Corporate antivirus/patch management/domain controller
  - Manufacturing planning
  - Business resource planning

- DMZ
  - Application servers
  - Historians
  - Engineering Station
  - Patch management for DMZ and Control zone

- Process Control
  - Operator consoles
  - Domain control
  - Field I/O
CASE: SETTING THE STAGE

- Three main automation systems
- Control network, DMZ, enterprise network
- The scope was in the control network and DMZ
- Relatively low amount of network traffic
- Single vendor environment
- Baselining:
  - One month: collecting network traffic mirroring it from the switches
  - Making preliminary asset inventory
**CHALLENGES**

- **Communications**
  - Proprietary communication protocols, (out of the box solutions do not work)
  - Creative ways of using known protocols, implementations of standardized protocols varies from vendor to vendor
  - Text-based communication

- **Customization:**
  - Sensor must be taught to understand proprietary protocol
  - Deviations must be taught.

- **Undocumented log sources, specifications hard to get**

- **Monitoring of remote access: who did and what (Shared accounts widely used)**

- **Planned outages**
  - USB sticks, other previously unknown devices

- **Not possible to do any preventive or active measures**
  - Traffic was mirrored from switches
  - Using data diodes to transfer information to dmz
HOW

- Small steps at the time: Not everything at once, start from manageable entity
- Establish a baseline
  - Who talks to Whom
  - Changes in the profile: new devices, new network connections (or attempts)
  - Utilize fact that the environment is relatively static, anomaly detection techniques work when the baseline is known
- Utilise correlation to improve reliability of identified event
  - HMI $\leftrightarrow$ Network traffic
  - Sent commands (Network) $\leftrightarrow$ Received commands (PLC)
- Focus on easy actions to monitor high priority systems
Examples of events that can be monitored from control systems

- Deviations
  - New events in logs or network,
  - New devices or network connections
  - Known attacks, anomalies

- User actions/change management
  - Settings and access rights changes
  - Configuration changes
  - Logins and logouts

- Service availability
  - Error messages and response times in logs
  - Probes (ping, content fetch)
  - Events/time unit (lower or upper limits)
  - Workflow monitoring

- Environmental
  - Opening and closing of cabinets
  - Heat and moisture variations
DMZ environments logs: Inbound traffic
2. Firewall/Data Diode logs: Network border
3. Intrusion Detection System: Attacks that has passed firewall
4. Netflow from switches: All traffic from process control networks
5. Event logs from servers: All events of interest
6. Intelligence of vulnerabilities, assets and users
7. Actionable alerts to operators
BENEFITS

- Capability to manage risk from security breaches helps optimizing the cyber defence
- Up-to-date asset inventory → possibility to do passive (no scanning) vulnerability management
- Real-time visibility to environment’s security
- Centralized view and monitoring of security related events
- Greater value of existing security technology, more effective use of log and event information.
- Reduced risk of non-compliance due e.g. improved reporting
- Better visibility improves reaction times of incidents and reduces downtime caused by them
- Recording audit trail leads improved forensics capabilities
- Monitoring the environment for cyber security may reveal other problems
LESSONS LEARNED

- Co-operation with the ICS vendor is a must

- Make ICS characteristics work for you:
  - Baseline, relatively static environment
  - Typically low amount of network traffic (but also low bandwidth networks..). Possible to record all network traffic over a long period of time for later use (e.g. incident handling, forensics)

- Analyzing security events and resolving security incidents require special knowledge, experiences and proper tools and a process
  - Security monitoring and incident response is not a side job