INTRODUCING CYBER SECURITY AT THE DESIGN STAGE OF PUBLIC INFRASTRUCTURES: A PROCEDURE AND CASE STUDY

Sridhar Adepu and Aditya Mathur
iTrust Centre for Research in Cyber Security
Singapore University of Technology and Design

CSDM Asia, February 24-26, 2016
OUTLINE

- Introduction
- Security by design
- Architecture of SWaT
- Impact analysis
- Conclusion
CONTRIBUTIONS

- A scalable and automatable security-by-design procedure to understand the response of a Cyber Physical System to attacks on its communications infrastructure.

- Dynamic State Condition Graph (D-SCG) as a formal modeling device for sensor-actuator constraints in a CPS.
WHAT IS CPS?
Cyber-attacks against CPS

“Cyber attack" refers to an attempt at disturbing the state of an Industrial Control Systems (ICS) through its communication network.
Popular breaches

- Maroochy shire sewage system 2000.
- Stuxnet Attack in 2010.
- Ukraine power plant black out 2016.
- Ukraine railway system black out 2016.
SECURITY BY DESIGN

1. Design Process
2. Model [Update] sensor-actuator constraints
3. Attacker models
4. Impact analysis
5. Update control algorithms
   - Update hardware
   - Design update
6. State Condition Graph
7. Updated design

Requirements

Attacks

Attacker objectives met
SWaT Testbed: Simplified View

PLC | Sensors/actuators | PLC | PLC
---|---|---|---
Level 0 | | Level 1 | |
PLC | SCADA Workstation/HMI | PLC | PLC
Level 2 | | | |
ARCHITECTURE OF SWaT: COMMUNICATION
Dynamic State Condition Graphs

(a) Tank A → Pump P → Valve → Tank B

(b) LL: Low
HH: High
sa, sb: level sensors for tanks A and B
\( h_a(t) \), \( h_b(t) \): Level of tanks A and B
ATTACKER MODEL

- Attacker model is a pair (T;O), where T is an attack type to realise objective O.

- Example, “Damage generator A in a power grid,” or “Damage pump P302 in a water treatment network.”

- A cyber attack is a sequence of actions, a procedure, initiated by the attacker where each action is initiated via a cyber component, such as a wireless link or a SCADA computer.
ULTRA FILTRATION PROCESS
## Impact Analysis: Damage the Ultrafiltration

<table>
<thead>
<tr>
<th>Attack</th>
<th>Actions</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Spoof messages going to PLC 3 by compromising the wireless link from the sensors</td>
<td>Attacker can send false data to PLC 3.</td>
</tr>
</tbody>
</table>
| 2      | Set the high pressure sensor PSH-301 to 2.0 Bar                           | System state: PSH301 > 2.5 Bar  
In PLC: PSH301 < 2.5 Bar  
Hence, in the absence of the attack, P301 should be turned OFF, but as the PLC has the incorrect state information, it does not turn P301 OFF. |
| 3      | Set the differential pressure switch DPHS-301 to 0.3 Bar                  | System state: DPHS301 > 0.5 Bar  
In PLC: DPHS301 < 0.5 Bar  
Hence, in the absence of the attack, P301 should be turned OFF, but as the PLC has the incorrect state information, it does not turn P301 OFF. |
| 4      | Set the differential pressure indicator DPIT-301 to 0.3 Bar               | System state: DPIT301 > 0.4 Bar  
In PLC: DPIT301 < 0.4 Bar |

**Impact on SWaT:** UF does not enter immediate backwash cycle; UF deterioration accelerated; UF is likely to be damaged if the attack persists for sufficient time. The time to damage the UF will depend on the incoming water quality and the properties of the membranes in the UF unit.
### Summary of Impact Analysis on SWAT

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>DSCG Used</th>
<th>Outcome</th>
<th>Damage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bias</td>
<td>p2_off</td>
<td>Dosing does not get activated to change the water properties</td>
<td>Water produced does not maintain desired chemical properties</td>
</tr>
<tr>
<td>Covert</td>
<td>p4_on</td>
<td>Water dechlorination does not take place for 10 minutes</td>
<td>Increased chances of damage to the RO unit</td>
</tr>
<tr>
<td>Replay</td>
<td>p5_on</td>
<td>Impure water gets into the RO unit permeate tank</td>
<td>No hardware damage</td>
</tr>
<tr>
<td>Surge</td>
<td>p3_off</td>
<td>Ultrafiltration unit damage accelerated due to delay in backwash</td>
<td>Increased chances of UF damage</td>
</tr>
</tbody>
</table>
DESIGN UPDATE

- Based on the impact analysis, a detailed design of the defense mechanisms ought to be considered.

- Installation of additional water quality sensors will require the PLC code to be updated, and update the corresponding DSCG for further impact analysis.

- Independent network of sensors is one of the possible detection method.
CONCLUSIONS AND FUTURE WORK

- The case study presented in this paper offers a glimpse into how the notion of “Security by Design” can be realised in practice.

- The analysis procedure needs some automation for it to be applicable in the design of realistic systems.

- However, doing so requires a clear understanding of component semantics such as when does a component fail.

- DSCGs could become an even more powerful tool once they are enhanced with physical operational constraints of each device included in the model.
THANK YOU