Cyber-physical Systems Security – An Experimental Approach

Dieter Gollmann, Marina Krotofil
Security in Distributed Applications, Hamburg University of Technology

helped by Pavel Gurikov, Alexander Isakov, Jason Larsen, Alexander Winnicki
Security is a fashion industry
Whoever thinks his problem can be solved using cryptography, doesn’t understand his problem and doesn’t understand cryptography

Roger Needham, Butler Lampson
Security is a strange area; solving a problem in general is often easier than solving its specific instances

Fred Schneider
Cyber-physical systems (CPS) are physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core.

Such systems use computations and communication deeply embedded in and interacting with physical processes to add new capabilities to physical systems. These cyber-physical systems range from miniscule (pace makers) to large-scale (the national power-grid).

[National Science Foundation]
Cyber-physical systems are IT systems “embedded” in an application in the physical world.

- Consist of sensors, actuators, control units, operator consoles, and communication networks.
- Some of these systems are critical because they are part of an infrastructure critical for society.
- Critical infrastructure protection has been a high profile topic for a decade at least.
- Is this a matter of research or a matter of education?
A new science of cyber-physical system design will allow us to create new machines with complex dynamics and high reliability; it will allow us to be able to apply the principles of cyber-physical systems to new industries and applications in a reliable and economically efficient way.

Progress requires nothing less than the reintegration of physical and information sciences – the construction of a new science and technology foundation for CPS that is simultaneously physical and computational.

[National Science Foundation]
Focus on cyber-threats to the IT core
  - e.g. attacks targeting network traffic
  - e.g. attacks infecting nodes with malware
  - e.g. attacks by unauthorized users

View the “cyber” part of a cyber-physical system as an infrastructure

Consider defences that protect this infrastructure

Traditional IT security “is” infrastructure security
  - Securing the networks
  - Securing the operating system
Supervisory Control and Data Acquisition

Computer controlled systems that monitor and control industrial processes in the physical world

- Favourite example: electrical grid

Large body of literature on SCADA security, looks at

- intercepting and manipulating traffic
- infection by malware
- access by unauthorized users
- malicious actions by authorized users (insiders)
- manipulations with catastrophic consequences (terrorist threat, blackmail)
Defences

- Threats considered are in essence generic IT security threats
- Impact in the physical world only used to stress the importance of security
- Defences are generic IT security defences
  - Firewalls, intrusion detection systems, authentication, access control, code signing, cryptographic mechanisms, proper security and risk management, etc.
- Educating industries introducing IT in their processes about potential IT specific dangers is commendable
Example

- Single public utility operating electrical grid, water supplies, public transport (familiar setup in Germany)
- Single network for electrical grid and public transport
- Terminals for the grid in the public domain!
- Solution: proper network separation
- Matter of education
Cryptography

- Useful for traffic protection
- Familiar design challenges
  - Crypto for restricted devices, for restricted protocols
  - Key management
- Can crypto get in the way of safety?
  - Safety-critical alarms are better not encrypted
  - “When integrity check fails, message MUST be discarded”
    Will there be time for a resend in safety-critical situations?
- Matter of education, for “traditional” communication security experts
What is Missing?

- Close integration between the cyber part and the physical part characteristic for CPS
  - Meant to differentiate CPS from embedded systems …

- Defences end at the interfaces between the physical world and the IT infrastructure

- No defence against attacks manipulating inputs before they are passed to the IT infrastructure

- A secure infrastructure will pass wrong data securely to their destination; this is not good for security
Attacks in the Physical Domain

- Attacker may manipulate inputs in the physical domain before they are fed to the IT infrastructure
  - Manipulation of sensors
  - Manipulation of the environment around sensors
  - Misleading user input

- Attack goals:
  - Get the system in a state desired by the attacker
  - Make the system perform actions desired by the attacker

- Attacks use existing controls to influence system behaviour by manipulating inputs (physical domain) or by corrupting nodes in the system (cyber domain)
Manipulations of a controller have less to do with the confidentiality, integrity, and availability of information and more to do with the performance and output of a physical production process

Ralph Langner on Stuxnet
Securing CPS – 2\textsuperscript{nd} Attempt

- Treat IT core as a control system, not as an infrastructure
- What is new for the defender?
- What is new for the attacker?
“We would never raise an alarm based on a single sensor reading; we rather combine readings from different types of sensors to assess the situation”
Veracity

- What is new for the defender: don’t trust your inputs, even if they are cryptographically protected
- Veracity: property that a statement about an aspect relevant in a given application truthfully reflects reality
- Not guaranteed by familiar IT infrastructure security services
  - Authentication verifies the origin but not the veracity of assertions
Veracity

- Refers to aspects outside the IT infrastructure: the adversary is not an entity launching an attack in the infrastructure but an entity making false assertions.

- Data are already false when fed to the infrastructure.
Veracity

- May be achieved by tamper resistant sensors in tamper resistant environments
  - Expensive, relies strongly on physical security
- May be achieved by correlating observed and expected (based on physical laws) relationships between variables
- Will depend on specific characteristics of the system
Example – location services

- Establish location of a node by measuring its distance / position with respect to other nodes
  - GPS: satellite signals (beacons) for establishing position
  - Keyless car entry
  - WLAN: find real coordinates by using received signal strength (RSS) for measuring distance to access points
  - Internet: round-trip time (RTT) for measuring ‘distance’ to construct synthetic coordinates

- Can be compromised by providing manipulated inputs
  - Report wrong round-trip times
  - Jamming of beacons
  - Fake beacons
What is new for the attacker: having physical impact

“An attacker who gets access to the network can do whatever he wants to do”

Attacker may be able to create and traffic he wants

Attacker is able to create any physical effect he wants??
What do we need to make progress in CPSS?

- Real(istic) cases for testing our assumptions
- Tennessee-Eastman process is a standard example in process research, but it is only one example
- We (security researchers) have looked at a vinyl acetate process monitored by a chemical engineer
Stages of cyber-physical attacks

- Access
- Discovery
- Cleanup
- Damage
- Control
Stages of cyber-physical attacks

- Access
- Cleanup
- Discovery
- Damage
- Control
Access
Traditional IT hacking

- 1 ActiveX 0day
- 1 Clueless user
- Mix and repeat until done

- AntiVirus and Patch Management
- Database Links
- Backup Systems
Discovery
Process discovery

What and how the process is producing

How it is controlled

How it is built and wired
Stripper is....

Stripping column
Understanding points and logic

Ladder logic

Programmable Logic Controller

Piping and instrumentation diagram

Pump on the plant
Maximal economic damage?

Reaction

Refinement

Final product
Process does not operate in a vacuum
If we adjust one of the valves what happens to everything else?
How much can the process be changed before raising alarms or being shut down?
Control
Process control challenges

- Process dynamic is highly non-linear (???)

- Behavior of the process known to the extent of its model
  - So on to controllers. They cannot control the process beyond their control model
Control loop ringing

Caused by a negative real controller poles
Outcome of the control stage

<table>
<thead>
<tr>
<th>Sensitivity</th>
<th>Magnitude of manipulation</th>
<th>Recovery time</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>XMV {1;5;7}</td>
<td>XMV {4;7}</td>
</tr>
<tr>
<td>Medium</td>
<td>XMV {2;4;6}</td>
<td>XMV {5}</td>
</tr>
<tr>
<td>Low</td>
<td>XMV{3}</td>
<td>XMV {1;2;3;6}</td>
</tr>
</tbody>
</table>

Reliably useful controls
Damage
Technician

“It will eventually drain with the lowest holes loosing pressure last”

Engineer

“It will be fully drained in 20.4 seconds and the pressure curve looks like this”
Process observation

Chemical composition

- Reactor exit flowrate
- Reactor exit temperature
Technician answer

Reactor with cooling tubes

Graph showing Reactor Temperature over 24 hours.

- Y-axis: Reactor Temperature
  - Ranges from 158.5 to 160.5
- X-axis: Hours
  - From 0 to 24

The graph indicates periodic fluctuations in reactor temperature.
\[
(c \sum_{k=1}^{7} C_{i,k} C_p C_{i,k} + \rho_b C_p) \frac{\partial T_i}{\partial t} = - \frac{\partial \left( \nu_i \sum_{k=1}^{7} (C_{i,k} C_p C_{i,k}) T_i \right)}{\partial z} - \phi_i \rho_b (r_{1,i} E_1 + r_{2,i} E_2) - Q_i^{RCT}
\]
Engineering answer

Vinyl Acetate production

Graphs showing reactor temperature and VAM concentration over time.
Product loss

Product per day: $96,000$

Reactor: Loss 137.21 Kmol (11469.70 $)

![Chemical Reaction Diagram]

- Normal reaction
- Under attack

<table>
<thead>
<tr>
<th>Chemicals</th>
<th>Average Outflow [Kmol/min]</th>
</tr>
</thead>
<tbody>
<tr>
<td>O2</td>
<td>0</td>
</tr>
<tr>
<td>Co2</td>
<td>0</td>
</tr>
<tr>
<td>C2H4</td>
<td>10</td>
</tr>
<tr>
<td>C2H6</td>
<td>6</td>
</tr>
<tr>
<td>VAc</td>
<td>6</td>
</tr>
<tr>
<td>H2O</td>
<td>2</td>
</tr>
<tr>
<td>HAc</td>
<td>2</td>
</tr>
</tbody>
</table>
Outcome of the damage stage

Product per day: 96.000$

<table>
<thead>
<tr>
<th>Product loss, 24 hours</th>
<th>Steady-state attacks</th>
<th>Periodic attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>High, ≥ 10.000$</td>
<td>XMV {2}</td>
<td>XMV {4;6}</td>
</tr>
<tr>
<td>Medium, 5.000$ - 10.000$</td>
<td>XMV {6;7}</td>
<td>XMV {5;7}</td>
</tr>
<tr>
<td>Low, 2.000$ - 5.000$</td>
<td>-</td>
<td>XMV {2}</td>
</tr>
<tr>
<td>Negligible, ≤ 2.000$</td>
<td>XMV {1;3}</td>
<td>XMV {1;2}</td>
</tr>
</tbody>
</table>
Clean-up
Socio-technical system

• Maintenance staff
• Plant engineers
• Process engineers
• ……

Cyber-physical system
Creating forensics footprint

- Process operators may get concerned after noticing persistent decrease in production and may try to fix the problem.
- If attacks are timed to a particular maintenance work, plant employee will be investigated rather than the process.

1. Pick several ways that the temperature can be increased
2. Wait for the next natural recalibration
3. Perform the first attack
4. Wait for the recalibration to be repeated
5. Switch to the next method
6. Go to 4
Creating forensics footprint

Four different attacks
Defeating chemical forensics

**Reactor Average Efficiency Loss: 4.36 %**

- Normal reaction
- Under attack

**Reactor Average Selectivity Loss: 2.73 %**

- Normal reaction
- Under attack

**Total Product:** 429.04 Kmol (35865.28 $)

- VAc
- H2O
- HAc

**Reactor Average Conversion Rates:**

- O2 30.67%
- C2H4 9.81%
- HAc 29.08%
Defenses
Defense opportunities

- Better understanding the hurdles the attacker has to overcome
  - Understanding what she needs to do and why
  - Eliminating low hanging fruits
  - Making exploitation harder

- Wait for the attacker
  - Certain access/user credentials need to be obtained
  - Certain information needs to be gathered

- Building attack-resilient processes
  - By design (slow vs. fast valves)
  - Hardening (adjusting control cycle and/or parameters)
Conclusions

- For a CPS security analysis, one has to understand both sides of a cyber-physical system
  - IT infrastructure
  - Nature of the physical behaviors
  - Safety-measures that block certain physical events

- **Challenge for the security specialist**
  - Understanding the physical effects of actions in cyber-space
  - Specific to (the class of) systems being analyzed

- **Challenge for the process engineer**
  - Learning to think out of the box (salty cookie paradigm)
  - Getting used to answering (apparently) weird security questions