Deep Dive: Likely, Real and Unlikely Cyber-Physical Threats to ICS

Marina Krotofil

St. Petersburg
September 27-29, 2017
Just one of those opinionated opinions :-}
Industrial Control Systems

Corporate IT

Information Technology (IT)

Operational Technology (OT)

Physical process
IT security vs. OT security

ICS security

IT security
(cyber-security -> taking over the infrastructure)

OT security
(causing impact on the operations -> process and equipment)

Focus of the talk
Attack Development stage in ICS kill chain

Stage 2 shows the steps associated with a material attack that requires high confidence.

M. Assante, R. Lee. The Industrial Control System Cyber Kill Chain. SANS, 2015.
Stages of cyber-physical attack:

Access:
- Operator’s screens
- Regulatory filings
- Point database
- Safety briefs

Discovery:
- Historian
- Small changes to the process
- Realtime data from sensors
- Safety systems

Control:
- Minimal process model
- Accident data
- SEC filings
- Process experts
- Custom research

Damage:
- Custom operator spoofs
- Waiting for unusual events
- Log tampering
- Forensic footprint

Cleanup:
- ICCP
- Regulatory reporting
- Just-in-time manufacturing
- Wireless links

Final Payload:
- Damage
- Cleanup
Let’s dive into some specifics
In control world it is all about control loops

- **Actuators**
- **Physical process**
- **Sensors**
- **Setpoint**
- **Control system**

Graphs showing data trends over time.
Cyber-Physical Attack

1. Manipulate the process
   - Direct: Set point change; manipulation of actuators
   - Indirect: Deceiving controller/operator about process state

2. Capture process feedback
   - Direct: Direct observation of process values
   - Estimated or Derived: From existing measurements or calculations

3. Prevent response
   - Operators: Blind, Mislead
   - Control system (including safety): Modify operational/safety limits
Why feedback loop is so important?

- In most scenarios involving process manipulation, attacker needs a feedback mechanism to know how well she is doing
  - Is attack succeeding/ failing?
- Attack effect propagation
  - To monitor the extent of attack effect propagation
  - To monitor state in the neighboring systems
- To calculate **Time-to-Damage** to plan for concealing activities
  - When is the time to return control back to control system
Plant designs are attacker unfriendly

- So far I haven't ever worked with a scenario when feedback mechanism was easily or at all obtainable
- Typically values needed for attack are not measured
  - No readily available control methods exist
  - Multiple strategies to obtain feedback (but none is easy)

Mostly involves “non-glamorous” sensor data processing
Parameterization of cyber-physical attack

- Vacuum collapse – Implosion attack
- “Generic” type of attacks – works across multiple industries
- The final payload still needs to be parameterized on facility-to-facility basis
- This demo: 11 destroyed barrels
- $$$ in costs of equipment and man hours

How to measure SUCCESS of implosion attack?

There is no sensor measuring “roundness” of the pipe.
How to measure FAILURE of implosion attack?

Stuff typically not on the diagrams

J. Larsen. Hacking Critical Infrastructure like You are not a n00b. RSA, 2016.
Goal: catalyst deactivation

Alarm and physics propagation
Goal: catalyst deactivation

Number of needed implants

Diagram showing a process flow with labeled components such as Oxygen Feed, Ethylene Feed, Reactor, Vaporizer, Acetic Acid Recycle, Heat Exchanger, HAC Tank, and various other processes and sections labeled as #1, #2, #3, and #4.
Growing complexities and uncertainties

- An exploit can be always built, but
  - What will be the cost of final effort?
  - What is total cumulative uncertainty?

J. Larsen. Hacking Critical Infrastructure like You are not a n00b. RSA, 2016.
Reverse Engineering Physical Processes: MK


- Standard approaches from control engineering worked, but did not serve well our needs

- 9 months of work (tons of testing)

- Eventually we developed a customized approach based on few standard and home brewed algorithms

Black Hat’15: We should probably automate this process
Abe Davis -> automatic generation of physical models using modes (common frequencies)

JL tested the approach to building process models

Challenge #1: Process data is not as rich as image data

Challenge #2: Not suitable for processes with frequent changes of states (on/off)
  - E.g. water treatment

Let’s make some predictions
Near future unlikely mass-scale attacks

- **Complex cyber-physical attacks**
  - Of high engineering precision
  - Requiring high coordination
  - Requiring considerable time and effort

- **Attacks which take unknown/extended time to cause needed impact**
  - Killing catalyst vs. disconnecting circuit breakers

- **In general all attacks which require feedback loop**

- **Attacks with unclear collateral damage (?)**
Near future realistic threats (1)

- **Attacks with instantaneous/clear impact**
  - Design deviation attacks ("Out-of-Spec" attacks), e.g. in additive manufacturing
  - Equipment shut off, e.g. in power distribution industry
- Attacks which do not require extensive/custom OT comprehension (physical process, failure conditions, control strategies, alarms, etc.)
  - More of cyber-oriented attacks; attacks executed over HMI
  - “Easy Button” attacks

<table>
<thead>
<tr>
<th>Code</th>
<th>Name</th>
<th>Logic address</th>
<th>Access</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>TDC1</td>
<td>IDC injection time</td>
<td>16#28A2 = 10402</td>
<td>R/W</td>
<td>UINT (Unsigned16)</td>
</tr>
<tr>
<td>JOG</td>
<td>Jog assignment</td>
<td>16#2B66 = 11110</td>
<td>R/WS</td>
<td>WORD (Enumeration)</td>
</tr>
<tr>
<td>PS4</td>
<td>4 preset speeds</td>
<td>16#2C8A = 11402</td>
<td>R/WS</td>
<td>WORD (Enumeration)</td>
</tr>
<tr>
<td>PS8</td>
<td>8 preset speeds</td>
<td>16#2C8B = 11403</td>
<td>R/WS</td>
<td>WORD (Enumeration)</td>
</tr>
<tr>
<td>SP8</td>
<td>Preset speed 8</td>
<td>16#2C98 = 11416</td>
<td>R/W</td>
<td>UINT (Unsigned16)</td>
</tr>
<tr>
<td>JPF</td>
<td>Skip frequency</td>
<td>16#2C25 = 11301</td>
<td>R/W</td>
<td>UINT (Unsigned16)</td>
</tr>
<tr>
<td>PIF</td>
<td>PID : PI function feedback assignment</td>
<td>16#2E7D = 11901</td>
<td>R/WS</td>
<td>WORD (Enumeration)</td>
</tr>
</tbody>
</table>
OT attacks which parameters can be “calculated” or reliable estimated, e.g. cavitation in pumps

- Cavitation conditions can be calculated
- One never exactly knows the intensity of cavitation (but can try to maximize it)

Pump impeller inspection at Palisades nuclear power plant
It takes just a small leak and a drone to cause ignition

Will terrorist be able to do it?
Near future realistic threats (4)

- **Supply-chain attacks**
  - Allows to bypass multiple levels of security
  - Better scaling of attack efforts
Real threats and attacker capabilities (1)

- Massive espionage (stale news)
  - Increasing number of targeted process-related information espionage
- Non-ICS specific attacks
  - Ransomware, KillDisk, etc.
- Cyber-oriented attacks
  - Attacks executed over HMI; tools for targeted protocol and control equipment manipulation
  - Recently, tools were left behind by the adversary
Real threats and attacker capabilities (2)

- Automation of control infrastructure reconnaissance
  - Most known example being usage of OPC

Real threats and attacker capabilities (2)

- Automation of control infrastructure reconnaissance
  - Most well-known example being usage of OPC

- Havex (2012-2014)
- Ukr power grid attack (2016)
Easily accessible facilities serve as training platforms

- Provide access to equipment and protocols
- Provide real-world level of complexity
- Allows to study human behaviors and reactions

Real threats and attacker capabilities (3)
Conclusions

- **Cyber-physical attacks becoming new normal**
  - None of recent power grid hacks was publicly disapproved by any government
  - At the same time owners of industrial infrastructures still struggling to believe in security threats

- **Attack tools getting more advanced and wide-spread**
  - Open-source tools
  - Tools found in wild
  - Tools for purchase

- **Distinction between governmental and criminal threat actors is fading**
  - “Trading” and “business” relationships
THANK YOU

QUESTIONS?