How Threat Modeling Can Influence ICS Security Posture

Luca Bongiorni
21st September 2019
• Principal Offensive Security Engineer at Bentley AppSec Team

• After this presentation, you will:

  – Understand what is Threat Modeling and how can help you Securing your Industrial Control Systems

  – Learn about its State of Art and which tools you can use nowadays
Vulnerability Vs Threat Vs Risk

Close the **Open Door** (Vulnerability) to keep out the **Bear** (Threat).
Otherwise we are **Screwed** (Risk).
Most of the **Attacks Methods** are related to **Application Security***

(i.e. OWASP Top 10 and SANS Top 25)

Which are:

- Well documented
- Already have recommended mitigations available

* Dell Security Annual Report 2015
Key SCADA Attack Methods

- Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
- Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
- Improper Control of Generation of Code ('Code Injection')
- Improper Authentication
- Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
- Cryptographic Issues
- Credentials Management
- Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
- Improper Access Control
- Improper Input Validation
- Information Exposure
- Resource Management Errors
Three Reasons for Threat Modeling

- **Produces Measurable Data** >> # of Threats & Associated Risk
- **It Smooth the path to Compliance** >> Happy Auditors
- **It Saves Money** >> Happy CFO/CEO/Shareholders
  - You Spot Security Flaws When It’s Much Cheaper to Fix Them

### Relative Cost of Fixing Defects

<table>
<thead>
<tr>
<th></th>
<th>Maintenance</th>
<th>Testing</th>
<th>Implementation</th>
<th>Design</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>100</td>
<td>15</td>
<td>6.5</td>
<td>1</td>
</tr>
</tbody>
</table>

*Integrating Software Assurance into the Software Development Life Cycle (SDLC), 2010*
Software Development Life Cycle

Requirements → Design → Development → Testing → Deployment

Risk Assessment → Threat Modeling → Static Analysis → Security Testing → Dynamic Testing

Secure Software Development Life Cycle
Threat Modeling Process

1. Create Assets’ Inventory
2. Architecture Review Model
3. Decompose Model in Single Assets
4. Identify Threats within those Assets
5. Document Threats
6. Rate Threats
STRIDE

- Invented in 1999 & Adopted by Microsoft in 2002
- The most mature
- It evaluates the system architecture by using Data Flow Diagrams (DFD)
- It is used to identify system’s entities and boundaries
- It applies a general set of known threats based on its acronym for its entity or boundary

<table>
<thead>
<tr>
<th>Threat</th>
<th>Property Violated</th>
<th>Threat Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
<td>Spoofing</td>
<td>Authentication Pretending being something/someone else</td>
</tr>
<tr>
<td>T</td>
<td>Tampering</td>
<td>Integrity Modifying something on net/disk/memory/etc</td>
</tr>
<tr>
<td>R</td>
<td>Repudiation</td>
<td>Non Repudiation Claiming that you didn’t do something or viceversa</td>
</tr>
<tr>
<td>I</td>
<td>Information Disclosure</td>
<td>Confidentiality Access information to someone not authorized</td>
</tr>
<tr>
<td>D</td>
<td>Denial of Service</td>
<td>Availability Exhausting resources needed to provide service</td>
</tr>
<tr>
<td>E</td>
<td>Elevation of Privilege</td>
<td>Authorization Allowing someone to do something not authorized</td>
</tr>
</tbody>
</table>
## STRIDEPP (ICS-STRIDE)

<table>
<thead>
<tr>
<th>Threat</th>
<th>Property Violated</th>
<th>Threat Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
<td>Spoofing</td>
<td>Authentication</td>
</tr>
<tr>
<td>S</td>
<td>Authentication</td>
<td>Pretending being something/someone else</td>
</tr>
<tr>
<td>T</td>
<td>Tampering</td>
<td>Integrity</td>
</tr>
<tr>
<td>T</td>
<td>Integrity</td>
<td>Modifying something on net/disk/memory/etc</td>
</tr>
<tr>
<td>R</td>
<td>Repudiation</td>
<td>Non Repudiation</td>
</tr>
<tr>
<td>R</td>
<td>Non Repudiation</td>
<td>Claiming that you didn’t do something or viceversa</td>
</tr>
<tr>
<td>I</td>
<td>Information Disclosure</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>I</td>
<td>Confidentiality</td>
<td>Access information to someone not authorized</td>
</tr>
<tr>
<td>D</td>
<td>Denial of Service</td>
<td>Availability</td>
</tr>
<tr>
<td>D</td>
<td>Availability</td>
<td>Exhausting resources needed to provide service</td>
</tr>
<tr>
<td>E</td>
<td>Elevation of Privilege</td>
<td>Authorization</td>
</tr>
<tr>
<td>E</td>
<td>Authorization</td>
<td>Allowing someone to do something not authorized</td>
</tr>
<tr>
<td>P</td>
<td>Physical DoS</td>
<td>Resilience</td>
</tr>
<tr>
<td>P</td>
<td>Resilience</td>
<td>Exhausting ICS operational controls in order to mine its reliability</td>
</tr>
<tr>
<td>P</td>
<td>Physical Harm</td>
<td>Safety</td>
</tr>
<tr>
<td>P</td>
<td>Safety</td>
<td>Undermining/Bypassing ICS safety controls in order to cause physical harm to assets and humans</td>
</tr>
</tbody>
</table>
DREADE (ICS-DREAD)

- DREAD methodology is used to rate, compare and prioritize the severity of risk presented by each threat that is classified using STRIDE.

<table>
<thead>
<tr>
<th>Threat</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>D Damage</td>
<td>How much damage will be caused?</td>
</tr>
<tr>
<td>R Reproducibility</td>
<td>How easy is it to reproduce the threat exploit?</td>
</tr>
<tr>
<td>E Exploitability</td>
<td>What is needed to exploit this threat?</td>
</tr>
<tr>
<td>A Affected users</td>
<td>How many users will be affected?</td>
</tr>
<tr>
<td>D Discoverability</td>
<td>How easy is it to discover this threat?</td>
</tr>
<tr>
<td>E Environmental Impact</td>
<td>How many living casualties there will be?</td>
</tr>
</tbody>
</table>
Purdue Enterprise Reference Architecture

A 1990s reference model for enterprise architecture
The Hamletic Question: Threat Modeling Yes or No?

Nowadays the ICS world is split in two:

• **Companies that do Threat Modeling already**
  – Recurring Problems:
    • Lack of Adequate Tools
    • Resources Vs # of Threats detected and mitigated

• **Companies that don’t do Threat Modeling**
  – Recurring Problems:
    • Lack of Resources (i.e. Time and Budget)
    • Lack of Expertise (i.e. Security Architect)
Work Instruction or Operating Procedure for Threat Modeling

- Product Security Leader
- 3 wk ago

Has anyone developed a work instruction or standard operating procedure for threat modeling of ICS/IIOT devices (or network)?

(I'm trying to do an analysis of what we can get the process architects, control engineers, or entry-level security professionals to document so that we can more efficiently use our principle ICS/IIOT security experts. This will also help us maintain a pipeline to get starting professionals trained and exposed to knowledge, skills, abilities, etc.. I will start by mapping out the workflow, so I was just curious if anyone has already done this for their org.)
Threat modelling

Hello Everyone,

I am curious to find out if people are creating threat models for their ICS? If so what tools are you using and are you happy with the tool?

We are currently using the Microsoft tool and it really does not lend itself to modeling an ICS environment. It is fine if you are developing C++ type software but not for the type of "integration" that normally makes up an ICS.

Thanks
Question for Engineers - Visio vs. CAD

Cybersecurity Engineer & Consultant  ·  9 mths ago

To engineers out there,

How would you want to see a Visio diagram? I have been working on a cyber security project using Visio to diagram an environment. Visio is generally fairly high level and conceptual. Some engineers on the project are wanting more detail, but I think what they want is a more physical representation of the environment. The physical layout will most likely be a handful of devices with minimal connections - everything is architected and separated by config e.g. VLANs, zones, etc.

Ultimately this will probably end up as a CAD drawing (that I won't create).

How would an engineer want to see what doesn't physically exist (logical, config) in a way that makes sense?

I'm thinking of replacing Visio style icons (brick wall for a firewall) with plain boxes to make it look more like a CAD drawing.
Which tools are you using for Threat Modeling?

- Microsoft Threat Modeling Tool: 34%
- Visio: 28%
- Excel: 24%
- PowerPoint: 9%
- Others: 5%
THE GOOD
THE BAD
AND THE UGLY
# Risk Assessment Template Excel

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>A (almost certain)</td>
<td>H</td>
<td>H</td>
<td>E</td>
<td>E</td>
<td>E</td>
</tr>
<tr>
<td>B (likely)</td>
<td>M</td>
<td>H</td>
<td>H</td>
<td>E</td>
<td>E</td>
</tr>
<tr>
<td>C (possible)</td>
<td>L</td>
<td>M</td>
<td>H</td>
<td>E</td>
<td>E</td>
</tr>
<tr>
<td>D (unlikely)</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>H</td>
<td>E</td>
</tr>
<tr>
<td>E (rare)</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

## Key

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td>Extreme Risk: Immediate action required to mitigate the risk.</td>
</tr>
<tr>
<td>H</td>
<td>High Risk: Action should be taken to compensate for the risk.</td>
</tr>
<tr>
<td>M</td>
<td>Moderate Risk: Action should be taken to monitor the risk.</td>
</tr>
<tr>
<td>L</td>
<td>Low Risk: Routine acceptance of the risk.</td>
</tr>
</tbody>
</table>

## Risk Status

- Open
- Closed
- In Progress
- Monitoring
- Resolved

[Graph of risk status]
Microsoft Threat Modeling Tool
It may become messy in ICS
• **What Can Do:**
  – **Good for Risk Assessment**
    • Allows evaluating a control system network as part of a comprehensive cybersecurity assessment
  – Specify cybersecurity recommendations
  – Report using standards-based information analysis
  – Provide a baseline cybersecurity posture

• **What CANNOT Do:**
  – **Bad for Threat Modeling**
    • Validate accuracy of user inputs or Identify Threats from a STRIDE POV
  – Ensure implementation of cybersecurity enhancements or mitigation techniques
  – Identify all known cybersecurity vulnerabilities
  – Re-Use Existing 3D models of the ICS Plant in scope
ICS Threat Modeling Nowadays

- **Not yet Fully Implemented**
- **A lot of uncertainties on:**
  - How to do it Systematically
  - How to Scale it
  - Which Tool to use
    - Excel spreadsheets and Risk Matrixes
    - Microsoft Threat Modeling tool
- **Extremely Time Consuming** (due the reasons above)
- **Need for a Better Approach**
  - Ad-Hoc Tools
  - Continuous Threat Modeling & Dedicated Methodology for ICS
    - CATHAMA
STRIDEPP + DREADE + PERA/CPwE = CATHAMA

Continuous Advanced Threat Hunting And Modeling Activity
CATHAMA

- Based on Assets Levels (0 to 5) Division from Purdue Model (PERA)
- Continuous Effort in Hunting, Analyzing, Evaluating and Prioritizing Threats
- Risk Rating It is supported by Intel Feeds, Existing Vulnerabilities of each Asset (e.g. CVEs) and Automated Scanners reports
- Able to Simulate Existing Threats and What happens to the plant in case of a patch/hotfix is going to be applied.
  - E.g. Device A.1.2.3 has new 1-day RCE. It is used in different parts of the plant. One more critical than other places. We need to simulate what happens when patch is applied. SLA uptime is impacted? Is it safe to patch now?
Your Success Stories or Opinions Are Valuable!

https://www.surveymonkey.com/r/55FDWT6
Wanna Hear More About Threat Modeling in ICS?

@lucabongiorni
Resources

• Usual standards related to Risk Assessment mostly: NIST 800-82, NERC-CIP, IEC 6244.

• The problem I see in ICS, related to Threat modeling, is the lack of proper tools and a specific resources exclusively related to Threat Modeling (and not Risk Assessment).

• Said that I really love the two following books:
  – Hacking Industrial Control Systems, Clint Bodungen, 2017