Threat Modelling - Key Methodologies and Applications from OSS CIP (Civil Infrastructure Platform) Perspective

Dinesh Kumar
Project Manager, Toshiba Software India

SZ Lin (林上智)
TSC Representative, Moxa Inc.

About Us

• Dinesh Kumar <dinesh.kumar@toshiba-tsip.com>
  • Working for Toshiba Software India
  • Works for CIP Security work group

• SZ Lin (林上智) <sz.lin@moxa.com>
  • Working for Moxa Inc.
  • Contribute to Linux and other OSS projects

• 4096R/9561F3F9
  • 178F 8338 B314 01E3 04FC 44BA A959 B38A 9561 F3F9
Civil Infrastructure
The key challenges

- Apply IoT concepts to industrial systems.
- Ensure quality and longevity of products.
- Keep millions of connected systems secure.
CIP is the Solution

Industrial grade
- Reliability
- Functional Safety
- Real-time capabilities

Sustainability
- Product life-cycles of decades
- Backwards compatibility
- Standards

Security
- Security & vulnerability management
- Firmware updates
- Minimize risk of regressions
CIP is the Solution

Establishes an “Open Source Base Layer (OSBL)”

- CIP Core packages (tens)
- CIP kernel (10+ years maintenance, based on LTS kernels)
- company-specific middleware and applications (hundreds)
- additional packages (hundreds)
The Scope of CIP

- **On-device software stack**
  - **Linux Kernel**
    - Super Long Term Supported Kernel (SLTS)
  - **Middleware/Libraries**
    - Domain Specific communication (e.g. OPC UA)
    - Safe & Secure Update
    - Real-time support
    - CIP Core Packages
  - **User space**
    - App container infrastructure (mid-term)
    - Shared config. & logging
    - Monitoring
    - Security
  - **Kernel space**
    - App Framework (optionally, mid-term)
    - Multimedia
    - Real-time / safe virtualization

- **Tools**
  - Build environment (e.g. bitbake, dpkg)
  - Test automation
  - Tracing & reporting tools
  - Configuration management
  - Device management (update, download)
  - Application life-cycle management

- **Concepts**
  - Functional safety architecture/strategy, including compliance w/ standards (e.g., NERC CIP, IEC61508)
  - Long-term support Strategy: security patch management
  - Standardization collaborative effort with others
  - License clearing
  - Export Control Classification

- **Product development and maintenance**
  - Security patch management
  - Functional safety strategy
  - Standardization
  - License clearing
  - Export Control Classification
Security Workgroup

- Protect the asset in the civil infrastructure system by reducing the risk
- Adapt the international standard - ISA/IEC 62443 (Industrial Automation & Control System Cybersecurity Standards)
Cybersecurity Risk

Risk = Threat X Vulnerability X Consequence
What is Threat?

Threat

• Can be initiated by system itself as well as outsider
• Comparatively hard to detect than attacks
• Information may or may not be altered or damaged
• Circumstance that has ability to cause damage
• May or may not be malicious
• Can be intentional or unintentional

src: https://pixabay.com/zh/illustrations/away-junction-direction-1020200/
The process of anticipating 
“what could go wrong” 
and then forecasting 
“how it can go wrong.”
General Threat Modelling Objectives

- Attack surface reduction
- Secure default configurations
- Least privilege
- Defense in depth
- Compartmentalization
- Policy compliance
CIP - Objective of Threat Modelling

• Help CIP end users to re-use CIP platform reference threat modelling and build further security on top of it
• Periodically review and update threat model to incorporate newly reported threats
• Reduce the risk of Open Source Base Layer
Model capability, intent, and targeting for adversarial threats. Find out the actions that the threat agent might conduct.

**Threat actions**
Model the actions which might conducted by threat actor. The common method is STRIDE model developed by Microsoft.

**Threat activity**
Model the activity which conducted by a series of threat actions to achieve desired outcome. The common method is attack tree.

**Vulnerability viewpoint**
Model the vulnerability within the asset which may existed in the organization. Typically, massive of technical information is essential as indicators.
Key Threat Modelling Methodologies

• STRIDE threat modelling
• Attack trees
• Process for Attack Simulation and Threat Analysis (PASTA)
• Common Vulnerability Scoring System (CVSS)
• Security Cards
• Hybrid Threat Modelling Method (hTMM)
Risk mitigation by Threat Modelling

- **Four ways to reduce risk by using threat analysis report**
  - Redesign to eliminate
    - Takes more time more resources, sometime may not be feasible as component development is out of your control
  - Apply standard mitigations
    - Investigate or re-use how similar threats were mitigated
  - Invent new mitigations
    - It could be riskier if not done properly
  - Adapt compensating controls
    - Take appropriate extra measures in implementation
Data-flow Diagram (DFD) cont...

- **Processes**
  - are elements that, based on their input, perform actions and/or generate outputs.

- **Data stores**
  - are sinks or sources of data. Examples are databases or internal storage.

- **Data flows**
  - represent the flow of information between elements. A data flow can be a protocol specific communication link such as HTTPS or UDP.

- **External interactors**
  - are elements whose influence should be taken into account, but which are outside the scope of the analysis.

- **Trust boundaries**
  - divide the elements in the diagram into different trust zones, e.g. elements in open networks vs elements in internal networks.
Data-flow Diagram (DFD)

**External Entity**
- People
- Other systems
- Web portals

**Processes**
- DLL/.so
- Components
- Services
- exe
- Web services
- Assemblies

**Data flow**
- Function call
- Network traffic
- RPC

**Data Store**
- Database
- File
- Registry
- Config files
- Shared memory file
CIP Development DFD
## STRIDE: Threats affecting elements

<table>
<thead>
<tr>
<th>Elements</th>
<th>Spoofing</th>
<th>Tampering</th>
<th>Repudiation</th>
<th>Information Disclosure</th>
<th>Denial of Service</th>
<th>Elevation of Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Flows</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>×</td>
<td></td>
<td></td>
<td>×</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Data Stores</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>×</td>
<td></td>
<td></td>
<td>×</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Processes</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Interactors</td>
<td>×</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CIP as Networking Switch Use Case

- The image depicts ICS reference architecture for Zones and Conduits
- Zone-1 components consist of core components
- Let’s try to create DFD and threat model for network switch assuming switch is based on CIP platform

STRIPE: CIP DFD (As Networking Switch)
STRIDE: Networking Switch (CIP Threat Analysis View)

- **Title:** Potential Data Repudiation by Authentication for configuration
- **Category:** Repudiation
- **Description:** Authentication for configuration claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
- **Interaction:** User credentials
- **Priority:** High
• Threat Model Analysis Report reveals about the missing security measures in existing models
• For each missing point, counter measures information should be provided or security measures should be taken
• At each design change or new package addition this step should be repeated
# STRIDE: Standard Mitigations

<table>
<thead>
<tr>
<th>Threat</th>
<th>Security property</th>
<th>Mitigation methods</th>
<th>CIP feature to address standard Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoofing</td>
<td>Authentication</td>
<td>-Kerberos authentication&lt;br&gt;-PKI Systems, SSL, TLS&lt;br&gt;-Digital signatures</td>
<td>-shadow, pam,&lt;br&gt;-libpam_google Authenticator,&lt;br&gt;-openssl</td>
</tr>
<tr>
<td>Tempering</td>
<td>Integrity</td>
<td>-MAC(Mandatory Access Control)&lt;br&gt;-ACLs&lt;br&gt;-Digital Signatures&lt;br&gt;-Checksum</td>
<td>-acl&lt;br&gt;-openssl(digital signature verification)&lt;br&gt;-sha256, sha512</td>
</tr>
<tr>
<td>Repudiation</td>
<td>Non Repudiation</td>
<td>-Secure logging &amp; auditing&lt;br&gt;-Digital signatures</td>
<td>-auditd&lt;br&gt;-rsyslog</td>
</tr>
<tr>
<td>Information disclosure</td>
<td>Confidentiality</td>
<td>-Encryption&lt;br&gt;-ACLs</td>
<td>-openssl&lt;br&gt;-acl</td>
</tr>
<tr>
<td>Denial of service</td>
<td>Availability</td>
<td>-ACLs&lt;br&gt;-Security policies&lt;br&gt;-Quota</td>
<td>-pam&lt;br&gt;-opensslh&lt;br&gt;-acl</td>
</tr>
<tr>
<td>Elevation of privileges</td>
<td>Authorization</td>
<td>-ACLs&lt;br&gt;-Group of Role membership&lt;br&gt;-Input Validation</td>
<td>-acl&lt;br&gt;-security policies published via application rules</td>
</tr>
</tbody>
</table>
Generic Attack Tree **example**

- Root node of the tree is the global goal of the attacker
- Each node represents one attack
- An attack tree defines a collection of possible attacks
- An attack described in a node may require one or more of many attacks described in child nodes to be satisfied
Obtain CIP Repository Admin Privilege

**Obtain repository owner’s password**
- Bribe the owner
- Brute force attack

**Steal repository owner’s SSH private key**
- Steal the laptop or keycard

**Steal repository owner’s token**
- Capture screen

Capture screen
Attack Tree for CIP based systems

Tamper CIP Software

Replace the CIP official image

- Hack into file server

Forge Debian binary package

- Hack the binary package CDN server
- Change APT source list
- Steal Debian developer’s private key

Inject malicious code

- Hack the upstream repository

Exploit known vulnerability

- Fuzzing attack
- Pen-testing
Validating Threat Models

● Validate whole threat model
  ○ Does diagram match the final code or final system implementation?
  ○ Are all threats enumerated
  ○ Minimum: STRIDE per element that touches a trust boundary
  ○ Has test/QA reviewed the model
    ■ Tester often finds issues with threat models or uncover something not considered during threat modelling
  ○ Is each threat mitigated
  ○ Are mitigations done right
Next Step for CIP Threat Modelling

1. Define Security requirements
2. Perform Threat Modeling
3. Mitigate potential threats
4. At any design change/package addition evaluate existing Threat Models
5. Repeat the cycle

Status:
- Completed
- In-Progress
- Yet to start
Reference for CIP resources

- CIP Home page
  - https://www.cip-project.org/
- CIP Work Groups wiki page
  - https://wiki.linuxfoundation.org/civilinfrastructureplatform/start
- CIP membership page
  - https://www.cip-project.org/about/join
- CIP Core gitlab
  - https://gitlab.com/cip-project/cip-core
- CIP Kernel gitlab
  - https://gitlab.com/cip-project/cip-kernel/linux-cip
- CIP Documents
  - https://gitlab.com/cip-project/cip-documents
Threat Modelling Tools

- **Draw.io libraries for threat modelling**
  - [https://github.com/michenriksen/drawio-threatmodeling](https://github.com/michenriksen/drawio-threatmodeling)

- **OWASP-Threat-Dragon**
  - [https://threatdragon.org/login](https://threatdragon.org/login)

- **threatspec**
  - [https://threatspec.org/](https://threatspec.org/)

- **pytm**
  - [https://github.com/izar/pytm](https://github.com/izar/pytm)

- **Microsoft Threat Modelling Tool**
CIP Talks at ELCE, and CIP Mini Summit

• October 26
  • CIP Kernel: **Upstream first is our principle**
• October 27
  • CIP Security: **Threat Modelling**
  • **Real time Linux virtualization, Embedded systems building, bridging communities**
• October 28
  • CIP Security: **The international effort to establish Base Layer**
• October 30
  • CIP **Mini-summit**
Please Visit CIP Virtual Booth!

“CIP mini-summit” will be held on Oct. 30th (Frid)
thank you!
Join us
CIP for sustainable Smart Cities with Open Source Software
Question?
Thank you
References

- NIST Special Publication 800-30r1 Guide for Conducting Risk Assessments
  - [https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf)

- NIST Special Publication 800-39 Managing Information Security Risk

- Secure Code, Threat modeling sessions
  - [https://www.youtube.com/watch?v=gDtS68DPm6Q](https://www.youtube.com/watch?v=gDtS68DPm6Q)