#

CIP Threat Modeling

Table of contents

Revision History

Revision No	Date	Change description	Author	Reviewed by
001	2021-03-14	Draft Threat Modeling Document	Dinesh Kumar	TBR
002	2021-12-21	Updated in SWG meeting.	Yasin User	SWG

1. Objective

The primary objective of this document is to create Threat Model for CIP reference platform. This Threat Model document can be re-used by CIP member companies or end product owners and identify potential threats for the end product. End products may have different business goals and types of risks, accordingly Threats should be identified.

Since the main goal of CIP is to maintain Open Source Base Layer (OSBL) for long term by re-using existing open source resources, as a result core design of the platform will remain same, therefore CIP threat model will not depend upon any specific versions of Debian or CIP Kernel. However, the period and condition of reviewing CIP Threat Model will be defined in later part of this document.

Moreover, subsequent revisions of this document may consider additional details of existing scenarios or address newly reported security issues.

2. Assumptions

Assumption	Impact
CIP threat model is based on generic use cases of CIP reference platform	None

3. Scope

Scope of this document is to consider only generic use cases for CIP for Embedded and Networking Categories as well as CIP development scenarios.

4. Security Requirements

CIP Security requirements are defined in CIP Security Requirements document

Current Security requirements have been defined based on IEC-62443-4-2 security requirements as there were no specific security requirements shared by CIP members.

5. Threat Modeling Strategy

CIP Threat Modeling would be primarily based on following strategies

STRIDE

STRIDE will be used for analyzing key CIP development and CIP use cases scenarios.

Attack Trees

There are some scenarios which will be covered by using attack trees.

CVSS

Since CIP Core and CIP Kernel already uses CVE scanner and automatically apply fixes to open CVEs, CVSS is inherently used by CIP.

In addition to above mentioned methodologies, whenever some threat is identified by some use case or found in upstream, same can be incorporated to keep the Threat Model up-to-date.

6. Data Flow Diagrams(DFD)

This section will have multiple Data Flow Diagrams(DFDs) for various use case scenarios. Various scenarios for data flows in process view and development view have been considered

6.1 Development View

6.1.1 CIP Development Context Diagram Following diagram illustrates CIP context diagram which highlights external entities which will interact with CIP platform during development.

Assumptions All external entities are authenticated while interacting with CIP development environment.

Note

Threat IDs are generated as follows

Threat___ID

- Here section_no refers to section in this document
- ID refers to the ID generated in Threat Modeling Tool

CIP Development Context Diagram

Threat ID	Threats Identified	Category	Remarks	Mitigation
Threat_6.1.1_11	CIP Platform may be able to impersonate the context of Other OSS developers in order to gain additional privilege.	Elevation of privileges	A user gains increased capability or privilege by taking advantage of implementation bug	Not applicable

6.1.2 CIP Kernel Development Following data flow diagram illustrates CIP Kernel development and how various external entities make changes in the CIP code.

Assumptions

Only CIP Kernel maintainers have merge privileges, all other developers can only send merger request, it's up to CIP Kernel maintainer to accept or reject it.

CIP Kernel Development DFD

Threat ID	Threats Identified	Category	Remarks	Mitigation
Threat_6.1.2_5	Spoofing of Source Data Store Mainline Kernel repo	Spoofing	Mainline Kernel repo may be spoofed by an attacker and this may lead to incorrect data delivered to CIP Kernel Maintainer	
Threat_6.1.2_7	Authentication Service claims that it did not receive data from a source outside the trust boundary	Repudiation	Consider using logging or auditing to record the source, time, and summary of the received data.	
Threat_6.1.2_18	Weak Access Control for a Resource	Information disclosure	Review authorization settings.	
Threat_6.1.2_11	Authentication Service May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation of privileges	Each CIP member companies member should have right privileges	

Threat ID	Threats Identified	Category	Remarks	Mitigation
Threat_6.1.2_42	Spoofing of the CIP Member Companies External Destination Entity	Spoofing	Use highest available login security mechanism such as 2F authentication	
Threat_6.1.2_49	Weak Access Control for a Resource	Information disclosure	Review authorization settings of CIP Kernel git repo	
Threat_6.1.2_62	Spoofing of Destination Data Store CIP Kernel git repo	Spoofing	Consider using a standard authentication mechanism to identify the destination data store.	
Threat_6.1.2_63	The CIP Kernel git repo Data Store Could Be Corrupted	Tempering	Ensure the integrity of the data flow to the data store.	
Threat_6.1.2_67	Authenticated Data Flow Compromised	Tempering	An attacker can read or modify data transmitted over an authenticated data flow. send data encrypted	
Threat_6.1.2_68	Spoofing of Destination Data Store Mainline Kernel repo	Spoofing	Consider using a standard authentication mechanism to identify the destination data store.	
Threat_6.1.2_70	Weak Access Control for a Resource	Information disclosure	Review authorization settings.	

6.1.3 CIP Core Development Following diagram illustrates CIP Core development for isar and Deby. CIP Core has only meta-data and recipes as well as build tools. Actual package source code or binary packages are downloaded from Debian repos while creating CIP images.

CIP Core Development DFD

Threat ID	Threats Identified	Category	Remarks	Mitigation
Threat_6.1.3_79	Data Flow HTTPS Is Potentially Interrupted	Denial of Service	An external agent interrupts data flowing across a trust boundary in either direction.Use authentication and send encrypted data	
Threat_6.1.3_84	Spoofing of the CIP Core Maintainer External Destination Entity	Spoofing	Consider using a standard authentication mechanism to identify the external entity.	
Threat_6.1.3_87	Spoofing of Destination Data Store CIP Core repo	Spoofing	Consider using a standard authentication mechanism to identify the destination data store.	
Threat_6.1.3_88	The CIP Core repo Data Store Could Be Corrupted	Tempering	Ensure the integrity of the data flow to the data store.	
Threat_6.1.3_92	Spoofing of Destination Data Store CIP Core repo	Spoofing	Consider using a standard authentication mechanism to identify the destination data store.	
Threat_6.1.3_97	Spoofing of Source Data Store CIP Core repo	Spoofing	Consider using a standard authentication mechanism to identify the source data store.	
Threat_6.1.3_98	External Entity CIP Core Developer Potentially Denies Receiving Data	Repudiation	Consider using logging or auditing to record the source, time, and summary of the received data.	

Threat ID	Threats Identified	Category	Remarks	Mitigation
Threat_6.1.3_99	Weak Access Control for a Resource	Information disclosure	Review authorization settings.	

6.1.5 CIP OS Image Creation Following diagram illustrates data flow when CIP image is created. While creating CIP image CIP Kernel source is downloaded as well as Debian packages source or binaries. Once the image is created it is saved in external storage such as AWS.

CIP Image Creation DFD

Threat ID	Threats Identified	Category	Remarks
Threat_6.1.5_102	Spoofing of Source Data Store Debian upstream repo	Spoofing	Consider using a standard authentication mechanism to identify the source data store.
Threat_6.1.5_103	Spoofing of Destination Data Store CIP Development Storage	Spoofing	Consider using a standard authentication mechanism to identify the destination data store.
Threat_6.1.5_107	Spoofing of Source Data Store CIP Kernel repo	Spoofing	Consider using a standard authentication mechanism to identify the source data store.
Threat_6.1.5_112	Spoofing of Source Data Store CIP Development Storage	Spoofing	Consider using a standard authentication mechanism to identify the source data store.
Threat_6.1.5_113	Spoofing of Destination Data Store CIP Image storage	Spoofing	Consider using a standard authentication mechanism to identify the destination data store

Threat ID	Threats Identified	Category	Remarks
Threat_6.1.5_114	Data Store Denies CIP Image storage Potentially Writing Data	Repudiation	Consider using logging or auditing to record the source, time, and summary of the received data.
Threat_6.1.5_116	Data Store Inaccessible	Denial of Service	An external agent prevents access to a data store on the other side of the trust boundary.
Threat_6.1.5_122	Spoofing of Source Data Store CIP Kernel repo	Spoofing	Consider using a standard authentication mechanism to identify the source data store
Threat_6.1.5_123	Weak Access Control for a Resource	Information disclosure	Review authorization settings
Threat_6.1.5_126	Spoofing of Destination Data Store CIP Image storage	Information disclosure	Consider using a standard authentication mechanism to identify the destination data store.
Threat_6.1.5_130	The CIP Development Storage Data Store Could Be Corrupted	Tempering	Ensure the integrity of the data flow to the data store.
Threat_6.1.5_215	Potential Process Crash or Stop for gitlab CI	Denial of Service	CIP gitlab CI crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Threat_6.1.5_226	The CIP Image storage Data Store Could Be Corrupted	Tempering	Ensure the integrity of the data flow to the data store.
Threat_6.1.5_227	Data Store Denies CIP Image storage Potentially Writing Data	Repudiation	Consider using logging or auditing to record the source, time, and summary of the received data.

6.2 Process View

6.2.1 CIP as networking switch Following diagram depicts a CIP use case when Networking Switch is developed using CIP platform.

CIP As Networking Use Case DFD

Following threats table list all the threats identified using DFD.

Threat ID	Threats Identified	Category	Remarks
Threat_6.2.1_146	Potential Data Repudiation by Store & Forward	Repudiation	Consider using logging or auditing to record the source, time, and summary of the received data.
Threat_6.2.1_148	Potential Process Crash or Stop for Store & Forward	Denial of service	Store & Forward crashes, halts, stops or runs slowly; in all cases violating an availability metric Needs Investigation.
Threat_6.2.1_150	Elevation Using Impersonation	Elevation using impersonation	Store & Forward may be able to impersonate the context of DCS/PLC in order to gain additional privilege.
Threat_6.2.1_151	Store & Forward May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation of privileges	DCS/PLC may be able to remotely execute code for Store & Forward.
Threat_6.2.1_152	Elevation by Changing the Execution Flow in Store & Forward	Elevation of privileges	An attacker may pass data into Store & Forward in order to change the flow of program execution within Store & Forward to the attacker's choosing.
Threat_6.2.1_155	Spoofing of the DCS/PLC External Destination Entity	Spoofing	Consider using a standard authentication mechanism to identify the external entity.

Threat ID	Threats Identified	Category	Remarks
Threat_6.2.1_156	External Entity DCS/PLC Potentially Denies Receiving Data	Repudiation	Consider using logging or auditing to record the source, time, and summary of the received data.
Threat_6.2.1_163	Potential Process Crash or Stop for Store & Forward	Denial of service	Store & Forward crashes, halts, stops or runs slowly; in all cases violating an availability metric.Needs Investigation.
Threat_6.2.1_164	Data Flow Binary Is Potentially Interrupted	Denial of service	An external agent interrupts data flowing across a trust boundary in either direction.Needs Investigation.
Threat_6.2.1_166	Store & Forward May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation of privileges	ESD may be able to remotely execute code for Store & Forward.
Threat_6.2.1_173	Spoofing of the Safety ES External Destination Entity	Spoofing	Consider using a standard authentication mechanism to identify the external entity.
Threat_6.2.1_176	Authenticated Data Flow Compromised	Tempering	An attacker can read or modify data transmitted over an authenticated dataflow.
Threat_6.2.1_182	Weak Access Control for a Resource	Information disclosure	Review authorization settings.
Threat_6.2.1_191	Authorization Bypass	Information disclosure	Ensure that your program is the only one that can access the data, and that all other subjects have to use your interface.

Threat ID	Threats Identified	Category	Remarks
Threat_6.2.1_105	Weak Credential Storage	Information disclosure	Credentials held at the server are often disclosed or tampered with and credentials stored on the client are often stolen. For server side, consider storing a salted hash of the credentials instead of storing the credentials themselves. If this is not possible due to business requirements, be sure to encrypt the credentials before storage, using an SDL-approved mechanism. For client side, if storing credentials is required, encrypt them and protect the data store in which they're stored
Threat_6.2.1_106	Potential Excessive Resource Consumption for Authentication for configuration or Configuration data store	Denial of Service	Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.
Threat_6.2.1_234	Data Flow Authentication status Is Potentially Interrupted	Denial of Service	An external agent interrupts data flowing across a trust boundary in either direction.

Threat ID	Threats Identified	Category	Remarks
Threat_6.2.1_236	Potential Process Crash or Stop for Authentication for configuration	Denial of Service	Authentication for configuration crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Threat_6.2.1_238	Elevation Using Impersonation	Elevation of privileges	Authentication for configuration may be able to impersonate the context of Admin User in order to gain additional privilege.

6.2.2 CIP as PLC Following diagram depicts a CIP use case using PLC.

CIP based PLC

Threat ID	Threats Identified	Category	Remarks
Threat_6.2.2_197	Spoofing the PLC with communication interface Process	Spoofing	Consider using a standard authentication mechanism to identify the destination process.
Threat_6.2.2_198	Spoofing the Various sensors data, temperature, pressure External Entity	Spoofing	Consider using a standard authentication mechanism to identify the external entity.
Threat_6.2.2_200	Potential Data Repudiation by PLC with communication interface	Repudiation	Consider using logging or auditing to record the source, time, and summary of the received data.

Threat ID	Threats Identified	Category	Remarks
Threat_6.2.2_201	Data Flow Sniffing	Information disclosure	Data flowing across Sensors data may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.
Threat_6.2.2_202	Potential Process Crash or Stop for PLC with communication interface	Denial of Service	PLC with communication interface crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Threat_6.2.2_204	Elevation Using Impersonation	Elevation of privileges	PLC with communication interface may be able to impersonate the context of Various sensors data, temperature, pressure in order to gain additional privilege.
Threat_6.2.2_208	Spoofing of the Controlled processes External Destination Entity	Spoofing	Consider using a standard authentication mechanism to identify the external entity.
Threat_6.2.2_209	External Entity Controlled processes Potentially Denies Receiving Data	Repudiation	Consider using logging or auditing to record the source, time, and summary of the received data.

7. Potential Threats To the System and Mitigation

This section will have consolidated list of threats identified from various use cases and data flow scenarios. Example of mitigation could be any of the following

actions.

- Add Debian packages to CIP
- Provide Security Configurations
- Provide Security Guidelines

Threat ID	Use case / Scenario	Impact	Mitigation
Threat_6.2.1_146	CIP based networking switch has store & forward process, it claims that it did not receive data from a source outside the trust boundary	Repudiation	CIP should address this issue by including logging or auditing to record the source, time, and summary of the received data
Threat_6.2.1_148, Threat_6.2.1_163,Threat_6.2.1_164	CIP based networking switch has store & forward process, it crashes, stops or runs slowly	Denial of service	Needs Investigation.
Threat_6.2.1_150	CIP based networking switch has store & forward process, it may be able to impersonate the context of DCS/PLC to gain additional privileges	Elevation of using impresonation	Authentication and authorization of all external entities
Threat_6.2.1_151, Threat_6.2.1_152,Threat_6.2.1_166	Store & Forward process may be subject to Elevation of Privilege using Remote Code Execution	Elevation of privileges	Avoid using remote code execution
Threat_6.2.1_155,Threat_6.2.1_173	Spoofing of external entities which communicate or send/receive data to CIP	Spoofing	CIP should include standard authentication mechanism for all external entities

Threat ID	Use case / Scenario	Impact	Mitigation
Threat_6.2.1_156	External entities communicating with CIP potentially denies receiving data	Repudiation	Same mitigation as for Threat_6.2.1_146
Threat_6.2.1_176	Data flow between authenticated external entities tempered, e.g. An attacker can read or modify data transmitted over an authenticated dataflow	Tempering	CIP should include latest encryption capabilities and all data should be shared in encrypted form
Threat_6.2.1_182	Weak Access Control for a Resource	Authorization	CIP should provide guidelines to end product owners to have role based authorization policies for all users
Threat_6.2.1_191	When external entities can modify data without having privilege	Authorization bypass	CIP should provide guidelines all external entities use the interfaces exposed for data modifications
Threat_6.2.1_195	When CIP has weak Credential Storage or credentials are stored without encryption	Information disclosure	CIP should keep all credentials as encrypted and same should be recommended to end users
Threat_6.2.1_210	An attacker could execute code remotely if he got access to the system.	Remote code execution	CIP users should use whitelisting to ensure only known good processes can be executed.

Threat ID	Use case / Scenario	Impact	Mitigation
Threat_6.2.1_211	An attacker could manipulate the system time to enable another attack.	System defense weakend	CIP users should enable secure time updates in their systems.

8. Validation of Threats and Mitigation

TBD

9. CIP Core Packages for mitigation

Threat ID	Mitigation	Required package
Threat_6.2.1_146,Threat_6.2.1_156	CIP should address this issue by including logging or auditing to record the source, time, and summary of the received data	- auditd- rsyslog
Threat_6.2.1_148, Threat_6.2.1_163,Threat_6.2.1_164	Needs to discuss with members how to address this threat	- TBD
Threat_6.2.1_150,Threat_6.2.1_155,Threat_6.2.1_178	Avoid unauthorized authorization of all external entities	- shadow- pam- openssl- libpam_google_authenticator
Threat_6.2.1_151, Threat_6.2.1_152,Threat_6.2.1_166,Threat_6.2.1_182,Threat_6.2.1_191	Avoid using remote code execution from untrusted or third party product	- acl- Security policies
Threat_6.2.1_176	CIP should include latest integrity verification capabilities and all data should be shared in encrypted form	- acl- openssl (Digital Signature Verification)- Sha256, Sha512
Threat_6.2.1_191	CIP should provide guidelines all external entities use the interfaces exposed for data modifications	- Document in APP & HW guidelines

Threat ID	Mitigation	Required package
Threat_6.2.1_195	CIP should keep all credentials as encrypted and same should be recommended to end users	- openssl- acl- tpm2-tools- tpm2-abrmd- tpm2-tss
Threat_6.2.1_210	CIP users should use aide for whitelisting to ensure only known good processes can be executed.	- aide
Threat_6.2.1_211	CIP users should use chrony to securely update their system time.	- chrony

10. CIP Kernel Threat Modeling

CIP Security WG needs to discuss with CIP Kernel WG how to approach Threat Modeling for CIP Kernel, some of the options could be. 1. Identify the risks for CIP Kernel 2. Identify important data flows which might be compromised 3. Identify other sources which may pose risk to CIP and mitigate

11. Updating CIP Threat Model

CIP Threat Model should be updated and revised based on following conditions.

1. When CIP Core adapts new version of Debian
2. New Packages or functionality added which may be exploited by internal or external entities
3. When CIP adapts new version of CIP Kernel

12. Further Guidelines for End Product owners

End products owners are advised to follow steps listed here to re-use existing CIP reference Threat Model.

- Identify Security Requirements specific to the product
- Identify business goals for the product
- List down critical data flow for business scenarios
- Use one the Threat Modeling methods for additional use cases

13. Acronyms

Acronym	Detail
CIP	Civil Infrastructure Platform
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
PLC	Programmable Logic Controller
DCS	Distributed Control System
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure

14. CIP Core CVE scanner

CIP Core uses CVSS threat modeling methodologies and uses Debian based wrapper to automatically scan upstream repos and include the fixes.

The CVE scanner tool is available at

CIP Core CVE Scanner

15. CIP Kernel CVE scanner

CIP Kernel uses CVE scanner to get latest CVE fixes and applies to CIP Kernel. The repo is available at CIP Kernel CVE Scanner

16. References

Reference name	Link
Microsoft Threat Modeling Tool	https://www.microsoft.com/en-in/download/details.aspx?id=49168

17. Pending Work and known issues

1. Add setting for text wrapping, currently whole page is occupied by text
2. Split this document and keep CIP Kernel, CIP Core threat modeling in a separate document based on other members inputs
3. Discuss with other CIP WG members to identify real business CIP use case scenarios and create Threat Models for them
4. Further investigation to address embedded system specific exploits such as listed in https://www.apriorit.com/dev-blog/690-embedded-systems-attacks