Security Design review and best practices in CIP

Table of contents

Revision History

Revision No	Date	Change description	Author	Reviewed by
001	2022-12-13	Draft document of secure design review and best practices in CIP	Sai Ashrith	Dinesh Kumar
002	2022-12-16	Revised document	Sai Ashrith	Dinesh Kumar

Introduction

This document explains the measures taken in CIP to meet the security requirements (SR-1 to SR-5) and best practices in their design (SD-3 & SD-4). As CIP specifically does not have a design, details about secure design review and best practices taken in upstream are added in this document.

Scope

This document explains the design review practices based on a checklist with traceability from security requirements and threat mitigations to security design and guidelines to the product user. Evidences that the issues found during the design review are tracked down to closure are also mentioned in this document.

SD-3 : Security Design review

Below are the security requirement list traced back to their implementation in the design part providing the evidence that the requirements are met.

1. Evidence documents in CIP for inadequately addressed security requirements (SR-1 TO SR-5).
    - The document defining generic security context of CIP is available here.

- Threat model document for CIP generic security requirements in different areas like Context, Core Development, OS Image creation, networking switch and as a PLC is available here. The updation of threat model in CIP is done as mentioned in this section.
- CIP documentation on security requirements based on IEC 62442-4-2 is mentioned here.
- The scope and boundaries of the product shall be documented in near future after the deployment scenarios are figured out the SWG members. The CIP targets are targeted to achieve SL-3 as mentioned here.
- Security work group members from companies like Toshiba, Siemens, MoXa etc. participate in these requirement review meetings.
- Trust boundaries, exploitable product interfaces and assets are documented in this Secure design SD-1 document.
- Traceability matrix from security requirement to security design to confirm to confirm that the requirements are addressed in CIP during design phase shall be updated in the development lifecycle. Any issue found during this design review shall be tracked in here.
- Traceability matrix from the threats identified to security design in CIP is present here.

2. The possible threats to the CIP-Core system are listed here from various use cases and data flow scenarios. The security guidelines to operate CIP in a secure manner is documented here.

SD-4 : Secure Design best practices

CIP specifically does not have a design document because of it's different development model. So below content lists the best practices in secure design and review methods in upstream.

- Debian ensures that installation of its software or while using it, there shall be no security risk to the system. To achieve that Debian team does deep review in the source code of a particular package and ensure there are no flaws to introduce security bugs during release.
- In Debian, review and fixing any security bugs has different costs in different phases of development. So the developers try to do the security review in the design phase which will be much easier and cheaper than doing it in deployment or maintainence phase.
- Developers use some tools to make the security review easier such as rats, flawfinder etc.

While packaging software, some security principles like :

- In default, the software must run with minimum privilege it needs and the package will not install binaries like **setuid** or **setguid**.
- Daemons provided by the package shall run in lowest possible user privilege.