Final Security Review Report

Revision

Version 5
4/22/24 4:01 PM

SME

Charles Wilson

Abstract

This document describes the process to perform and report on a final security review (**FSR**).

Group / Owner

Security / Secure Software Assessor

Motivation

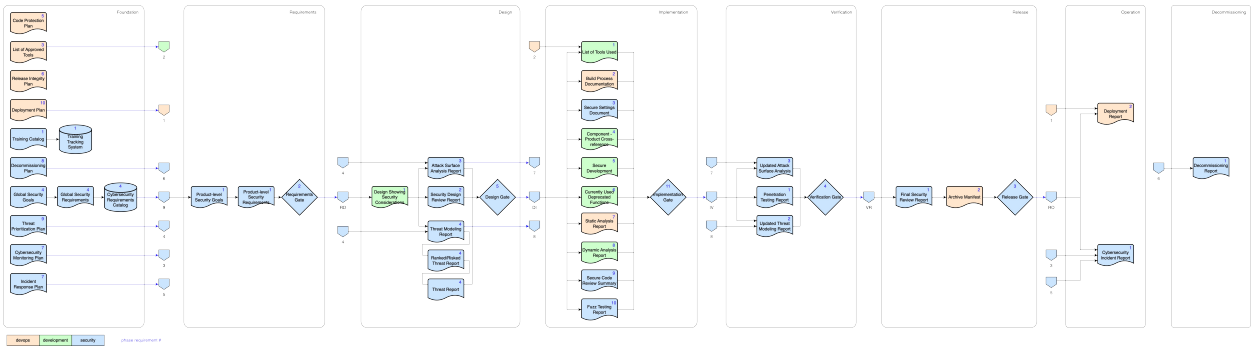
This document is motivated by the need to perform a check of all product security activities prior to the release gate. This is necessary given the nature of safety-critical, cyber-physical systems, subject to certifications such as **ISO/SAE 21434** and **ISO 26262**.

License

Overview

The FSR is a deliberate examination of all the security activities performed during product development. The FSR is performed by the secure software assessor with assistance from the groups responsible for the various phase requirement products under consideration. The FSR is neither a “penetrate and patch” exercise, nor a chance to perform security activities that were previously ignored or forgotten. It is a **go / no go** activity. In addition to the **report** activities, verification of the **plan** activities is undertaken.

The following diagram shows the dependency sequence leading to release:



Note: Regressions discovered during the FSR indicate a failure in earlier phase gate activities.

Note: All activity reports and plans should be stored and tracked in the organization’s document management system.

Phase Requirement Product Review

There are two classes of AVCDL phase requirement product considered by the FSR:

- Activity documentation
- Post-release plans

Activity Documentation

The bulk of the FSR is focused on verifying that due diligence has been made in the creation of the product. Each of the documentation activities contributes toward evidencing that. There should be no issues found with the documentation. As noted in the overview, any substantive security issues brought to light at this stage point to a failure at prior phase gates. Several of these reports may be created from files generated from the phase requirement activities. In cases where those files are intended for sharing with external sources it should be verified that the appropriate standards for data interchange are being used.

The activity documentation includes:

- **Design Showing Security Considerations**
- **Security Design Review Report**
- **Attack Surface Analysis Report**
- **Threat Modeling Report**
- **Ranked / Risked Threat Report**
- **Threat Report**
- **List of Tools Used**
- **Build Process Documentation**
- **Secure Settings Document**
- **Fulfillment of Associated Security-related Requirements**
- **Currently Used Deprecated Functions**
- **Static Analysis Report**
- **Dynamic Analysis Report**
- **Secure Code Review Summary**
- **Fuzz Testing Report**
- **Penetration Testing Report**
- **Updated Threat Model**
- **Updated Attack Surface Analysis**

Post-Release Plans

In addition to verifying the pre-release AVCDL phase requirement documentation products, it is important to verify that plans are in place to manage the post-release lifetime of the product. There should be sufficient attention to detail to cover common scenarios. Unlike activity documentation, the plans should be crafted to work well within the structure of the organization. Only when information needs to be shared externally should there be an express focus on interchange standards.

The post-release plans include:

- **Deployment Plan**
- **Cybersecurity Monitoring Plan**
- **Incident Response Plan**
- **Decommissioning Plan**

Report Content

The content of the FSR report is a simple list of all activity documents and post-release plans showing their go / no-go status. In the case where multiple elements of the system have been considered separately, a matrix would be a suitably compact representation.

References

1. **AVCDL** (primary document)
2. **Design Showing Security Considerations** (AVCDL secondary document)
3. **Security Design Review Report** (AVCDL secondary document)
4. **Attack Surface Analysis Report** (AVCDL secondary document)
5. **Threat Modeling Report** (AVCDL secondary document)
6. **Ranked / Risked Threat Report** (AVCDL secondary document)
7. **Threat Report** (AVCDL secondary document)
8. **List of Tools Used** (AVCDL secondary document)
9. **Build Process Documentation** (AVCDL secondary document)
10. **Secure Settings Document** (AVCDL secondary document)
11. **Fulfillment of Associated Security-related Requirements** (AVCDL secondary document)
12. **Currently Used Deprecated Functions** (AVCDL secondary document)
13. **Static Analysis Report** (AVCDL secondary document)
14. **Dynamic Analysis Report** (AVCDL secondary document)
15. **Secure Code Review Summary** (AVCDL secondary document)
16. **Fuzz Testing Report** (AVCDL secondary document)
17. **Penetration Testing Report** (AVCDL secondary document)
18. **Updated Threat Model** (AVCDL secondary document)
19. **Updated Attack Surface Analysis** (AVCDL secondary document)
20. **Deployment Plan** (AVCDL secondary document)
21. **Cybersecurity Monitoring Plan** (AVCDL secondary document)
22. **Incident Response Plan** (AVCDL secondary document)
23. **Decommissioning Plan** (AVCDL secondary document)