Threat Report

Revision

Version 4
12/7/21 12:16 PM

SME

Process: Charles Wilson
Report: Matthew Bourdua

Abstract

This document describes the process used to create the summary threat report based on the output of the ranking and risking of threat candidates determined by the threat modeling of an element of the system.

Group / Owner

Security / Security Architect

Motivation

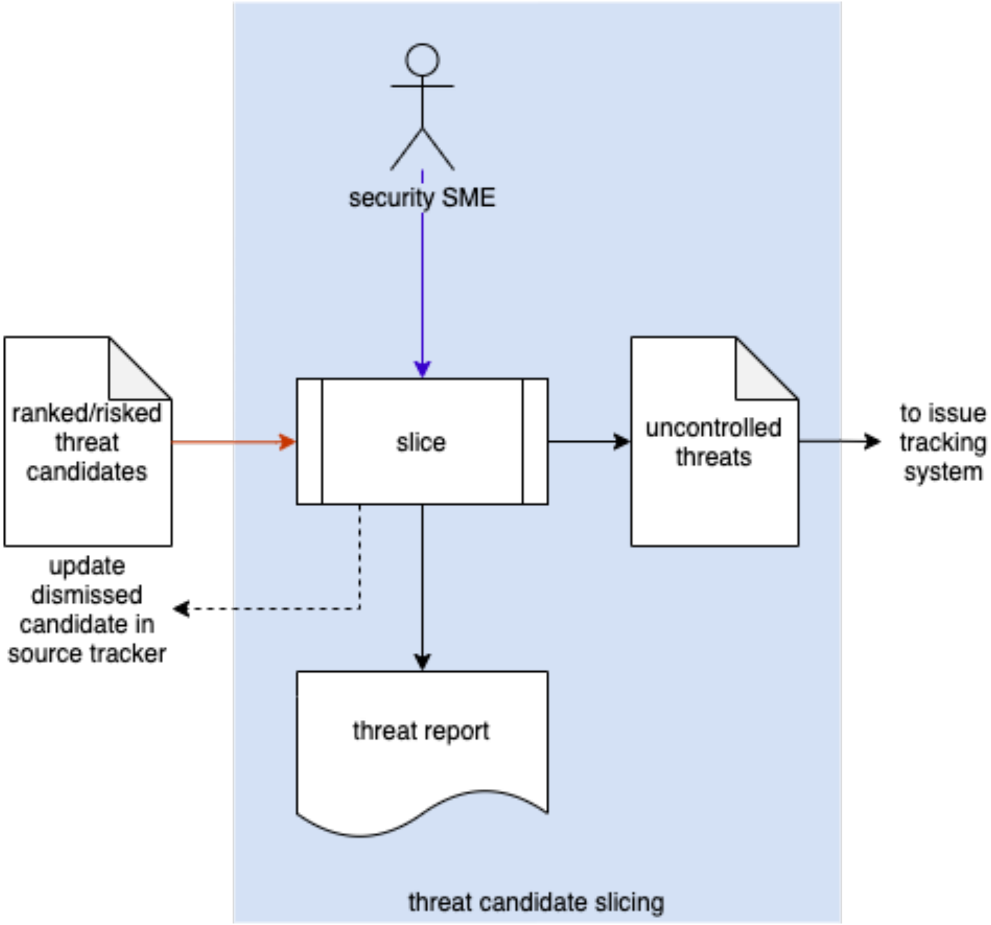
This document is motivated by the need to determine how to disposition of the system element's threat candidates. This is necessary given the nature of safety-critical, cyber-physical systems, subject to certifications such as **ISO 21434** and **ISO 26262**.

License

Overview

The information provided by the ranked / risked threat report is visualized using a two-dimensional scatter plot where the rank and risk values form the dimensions. A threshold, represented by a line through the space, is established and used to decide whether any given candidate is considered controlled or uncontrolled.

The following diagram illustrates the process to be used:



Process

The process activities shown here are documented in the **Threat Prioritization Plan** [1]. The ranked / risked threat candidates are sliced by the security SME into controlled and uncontrolled. The outputs are a **Threat Report** and a set of uncontrolled threats. Controlled threats are dismissed and documented in their source tracker (system tracking the threat candidates). Uncontrolled threats are entered into the issue tracking system.

Note: When dealing with multi-dimensional risk information, refer to the section below.

Threat Report

The threat report is an enhanced version of the threat candidates' initial report (**Threat Modeling Report** [3], **Attack Surface Analysis Report** [4], **Incident Report** [5]) with the additional detail from the **Ranked / Risked Threat Report** [2] limited to the threat candidates determined to be uncontrolled. The report should be organized in the same manner as the source report with the following added to summary and threat entry sections:

Summary additions:

- Description of ranking methodology
- Description of risking methodology
- Description of slicing criteria
- Slicing diagram image (scatter diagram with slicing line shown)

Threat entry additions:

- [Material from the **Ranked / Risked Threat Report**]
- Magnitude of the normal from the (risk, rank) to the slicing line

It is recommended that the report be generated from a portable data representation so that it can be programmatically manipulated.

Note: The magnitude of the normal may be used as a proxy for prioritization guidance.

Multi-dimensional Risk Information

When considering multi-dimensional risk information, additional analysis will be required. Such is the case with **ISO 26262** [6], **ISO 21434**, and to a lesser extent **ISO 12207** [7]. The first two specify that the following risk categories be considered:

- Safety
- Finance
- Operation
- Privacy

Consideration of these risk categories necessitates the ranked data be reviewed for each category separately for inclusion in the final threat report. As multiple SMEs will be required to assess the impact within each category, these reviews may be conducted in parallel.

The threat report will reflect the totality of areas reviewed.

Issue disposition will be dependent upon whether any of the categories yields an uncontrolled designation for the issue.

References

1. **Threat Prioritization Plan** (AVCDL secondary document)
2. **Ranked / Risked Threat Report** (AVCDL secondary document)
3. **Threat Modeling Report** (AVCDL secondary document)
4. **Attack Surface Analysis Report** (AVCDL secondary document)
5. **Incident Report** (AVCDL secondary document)
6. **ISO 26262-3:2018 Road vehicles – Functional safety – Part 3: Concept phase**
   https://www.iso.org/standard/68385.html
7. **ISO 12207 Systems and software engineering – Software life cycle processes**
   https://www.iso.org/standard/63712.html