Ranked / Risked Threat Report

Revision

Version 6
5/31/22 11:19 AM

SME

Process: Charles Wilson
Report: Matthew Bourdua

Abstract

This document describes the process to perform and report on the rank / risk activity performed on the output of the threat modeling of an element of the system.

Group / Owner

Security / Security Architect

Motivation

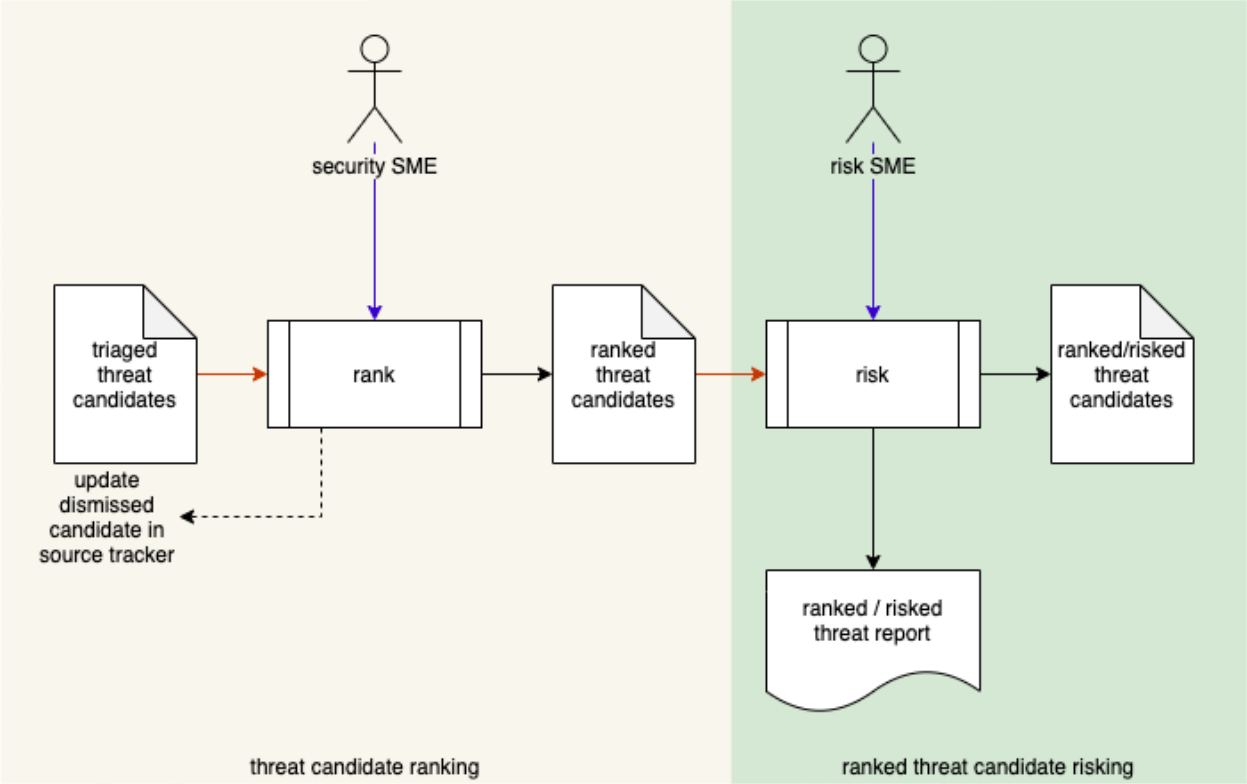
This document is motivated by the need to determine the relative severity (rank) and impact (risk) of the system element's threat candidates. This is necessary in order to properly assess the disposition of these candidates and required given the nature of safety-critical, cyber-physical systems, subject to certifications such as **ISO 21434** and **ISO 26262**.

License

Overview

The ranked / risked threat report summarizes the analysis performed on the output of the threat modeling activity which provides input into the threat candidate slicing activity. As indicated by the title, there are two discrete operations which take place. The first is the ranking of threat candidates to determine their relative severity. The second is the risking of threats to determine their potential harm.

The following diagram illustrates the process to be used:



Process

The process activities shown here are documented in the **Threat Prioritization Plan** [1]. The triaged threat candidates are ranked by the security SME and then risked by the risk SME. The outputs are a **Ranked / Risked Threat Report** and a file containing a set of ranked / risked threat candidates. The latter is the input to the process creating the **Threat Report** [3].

Ranked / Risked Threat Report

The ranked / risked threat report should detail the ranked and risked threats enumerated in the triaged threat candidates list. The report should be organized into summary and ranked / risked threat details sections. The summary includes:

- Description of the system
- Threat candidates' source [**threat modeling**, **attack surface analysis**, **incident response**]
- URI to threat candidate source tracker
- Description of ranking methodology
- Description of risking methodology

Individual ranked / risked threat candidates include:

- Threat ID (unique)
- Summary of the threat
- Detailed description of the worst case if threat is exploited
- Rank (severity)
  - Raw value (raw rank scoring system value)
  - Canonical value (such as a **CVSS** [6] vector)
  - Quantized value (ISO 21434 RQ-15-10: [**none**, **very low**, **low**, **medium**, **high**])
  - Justification of value determination
- Risk (impact)
  - Raw value (raw risk scoring system value)
  - Canonical value
  - Quantized value (ISO 21434 RQ-15-16: [**0**, **1**, **2**, **3**, **4**, **5**])
  - Justification of value determination

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

Rank / Risk Quantization

Rank quantization can be mapped from information provided by ranking mechanisms such as **CVSS** [6] to **ISO 21434** as follows:

CVSS score	0	0+	1	2	3	4	5	6	7	8	9	10
CVSS rating	none	low				medium			high		critical	
ISO 21434	none	very low				low			medium		high	

Risk quantization can be similarly mapped from information provided in **ISO 26262-3** [7], **ISO 14971** [8] and **FIPS 199** [9]:

ISO 26262		**ISO 14971**		**ISO 21434**	**FIPS 199**
S0	No injuries	none	No injuries	0	none
S1	Light injuries	negligible	Inconvenience or temporary discomfort	1	low
	Moderate injuries	minor	Temporary injury or impairment, not requiring professional medical intervention	2	medium
S2	Severe and life-threatening injuries (survival probable)	serious	Injury or impairment requiring professional medical intervention	3	
S3	Life-threatening injuries (survival uncertain)	critical	Permanent impairment or life-threatening injury	4	high
	Fatal injuries	catastrophic	Death	5	

References

1. **Threat Prioritization Plan** (AVCDL secondary document)
2. **Threat Modeling Report** (AVCDL secondary document)
3. **Threat Report** (AVCDL secondary document)
4. **Attack Surface Analysis Report** (AVCDL secondary document)
5. **Incident Response Report** (AVCDL secondary document)
6. **CVSS (Common Vulnerability Scoring System)**
   https://www.first.org/cvss/
7. **ISO 26262-3:2018 Road vehicles – Functional safety – Part 3: Concept phase**
   https://www.iso.org/standard/68385.html
8. **ISO 14971:2019 Medical devices – Application of risk management to medical devices**
   https://www.iso.org/standard/72704.html
9. **NIST FIPS 199 Standards for Security Categorization of Federal Information and Information Systems**
   https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf