Threat Modeling Report

Revision

Version 3
11/15/21 9:51 AM

SME

Process:	Charles Wilson
Report:	Matthew Bourdua

Abstract

This document describes the methodology to perform and report on the threat modeling of an element of the system.

Group / Owner

Security / Security Architect

Motivation

This document is motivated by the need to determine whether the element's design has security deficiencies. This is necessary given the nature of safety-critical, cyber-physical systems, subject to certifications such as **ISO 21434** and **ISO 26262**.

License

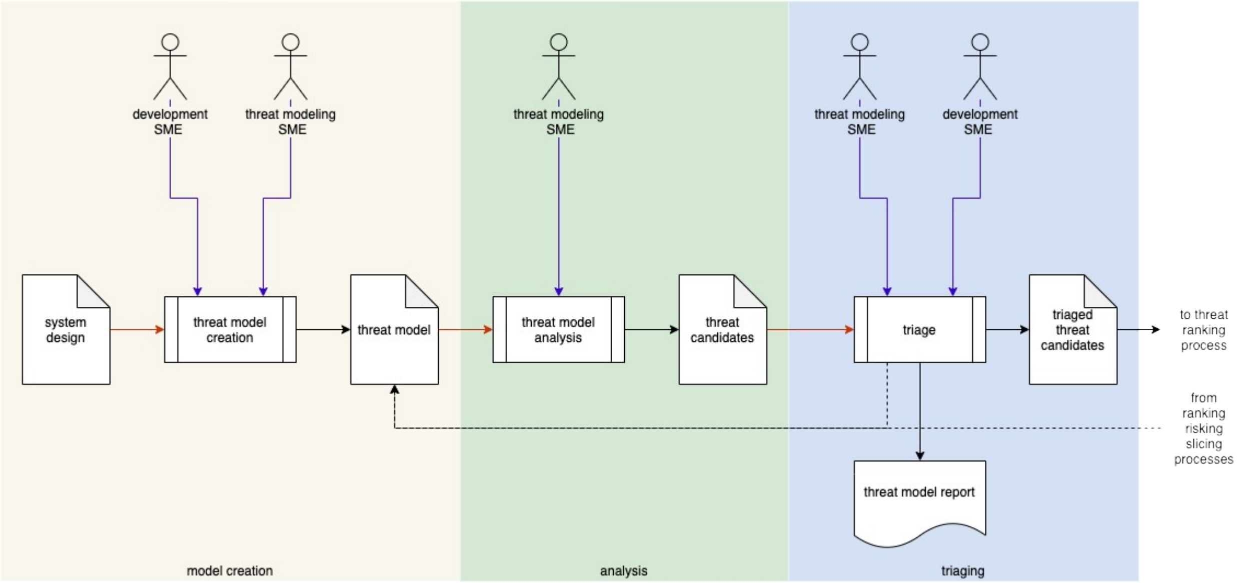
This work was created by **Motional** and is licensed under the **Creative Commons Attribution-Share Alike (CC4-SA)** License.

https://creativecommons.org/licenses/by/4.0/legalcode

Overview

The process of threat modeling involves creating an abstraction of the system and performing a systematic evaluation in order to expose possible design flaws. The abstraction is typically in the form of a data flow diagram (DFD [2]). The DFD contains a set of resources-managing processes connected by data flows. The elements of the threat model have attributes which assist in analysis. The threat model's data flows are analyzed using a well-defined methodology such as STRIDE [3].

The following diagram illustrates the process to be used:



Note: Threat modeling is a team exercise, encompassing program/project managers, developers, and testers.

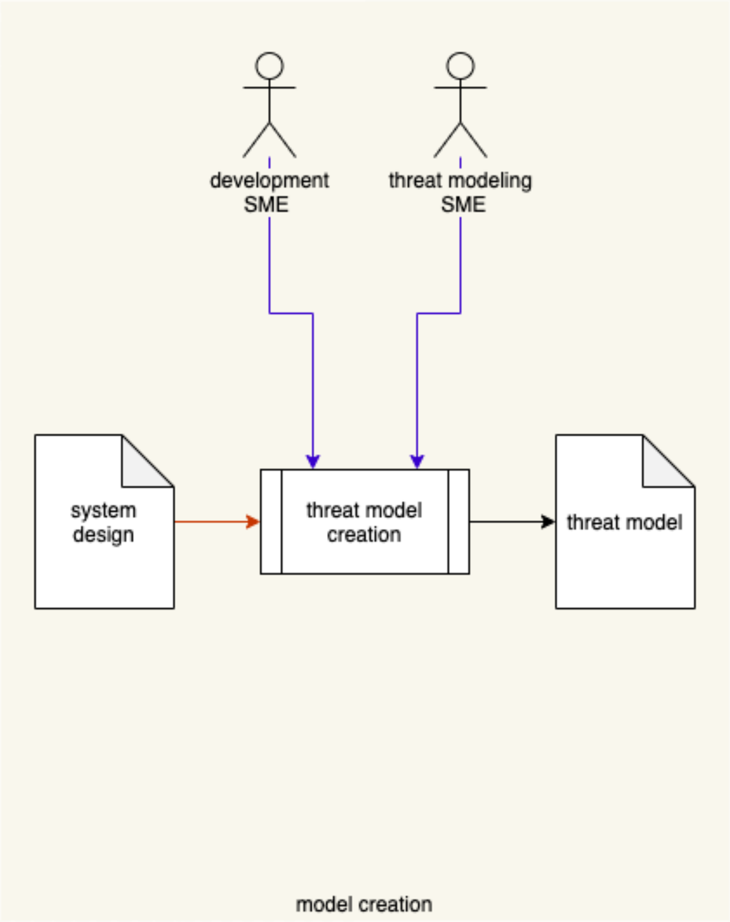
Note: Threat models should consider the multiple levels of abstraction present in a system.

Note: The threat modeling AVCDL work products are generated through application of the **Threat Prioritization Plan** [4].

Process

Threat Model Creation

Inputs	System design
Outputs	Threat model
Participants	Development SME Threat modeling SME

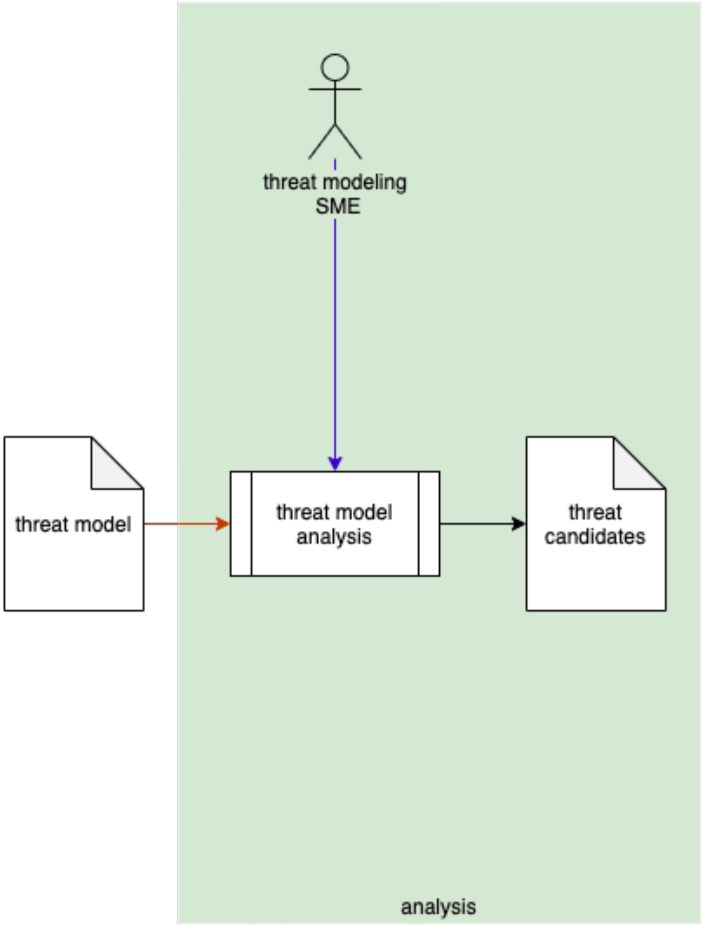


The threat modeling SME works with the development SME(s) to create a model of the system suitable for threat analysis. Any existing models are used as input to this process. For this activity, models are created using a formal modeling tool. The model is stored in the **Document Management System** [1]. This may be a set of models depending on the complexity of the system.

The system model uses trust boundaries to define the bounds of the system. External systems may be represented in the model to further clarify system bounds and the new system’s context within the overall design.

Threat Model Analysis

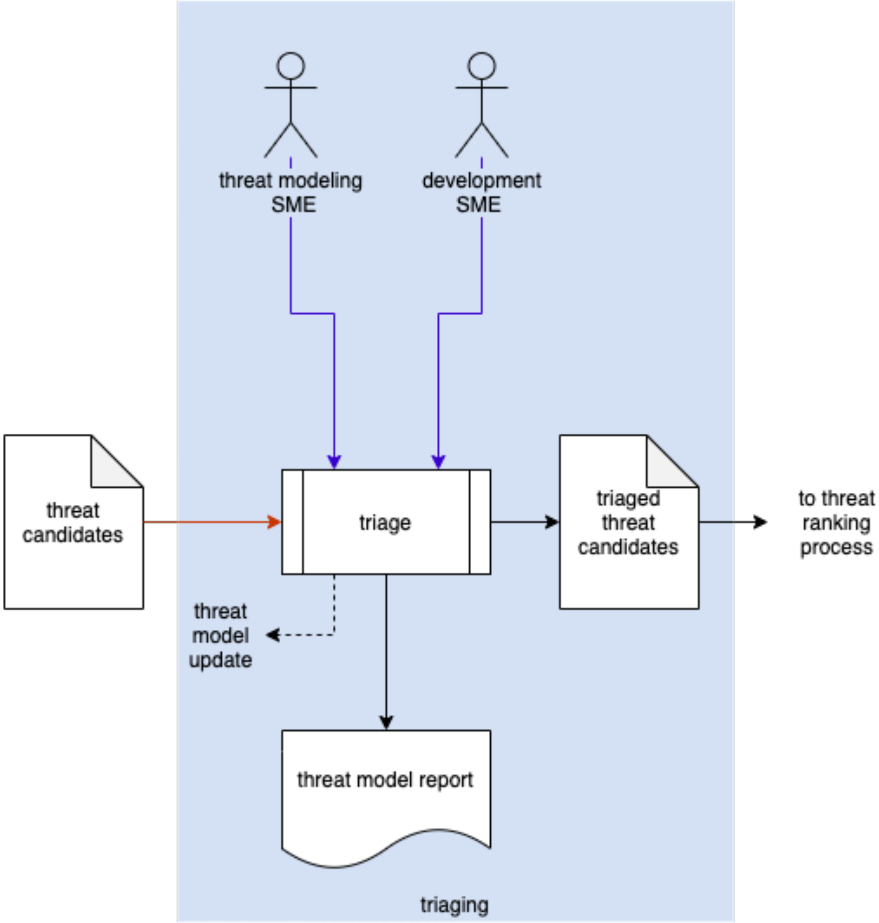
Inputs	Threat model
Outputs	Threat candidates
Participants	Threat modeling SME



The threat modeling SME processes the model to evoke a set of threat candidates.

Triage

Inputs	Threat candidates
Outputs	Triaged threat candidates Threat model report
Participants	Development SME Threat modeling SME



The threat modeling SME works with the development SME(s) to perform an initial triage of the threat candidates. This triage will yield one of three results:

1. A threat candidate exposes incomplete / incorrect information forming the model. The model will need to be updated and analysis redone.
2. A threat candidate is determined to be a non-issue due to circumstances not captured by the model. It will be marked as such and removed from consideration.
3. A threat candidate is determined to be plausible. It will be marked as such and where possible given a preliminary severity (where the severity designation may be used as a bug bar).

The outputs from this activity are a **Threat Modeling Report** and a file containing a set of triaged threat candidates.

Triaged Threat Candidates

The triaged threat candidates artifact is recommended to be a JSON representation capable of being used to produce the threat modeling report.

Threat Modeling Report

The threat modeling report should detail the threats to the system as exposed by the analysis of the threat model. The report should be organized into summary and threat details sections. The summary includes:

- Description of the system
- Image of the system (typically a DFD)

The threat details section contains one or more threat diagrams. Each of these is organized into summary and data flow sections. The summary includes:

- Diagram title (unique)
- Description of the diagram’s scope
- Image of the threat diagram

Individual data flows are used to organize the threat candidates. Each of these is organized into a summary and candidate threat list. The summary includes:

- Data flow ID (unique)
- Source of the data flow (originator)
- Destination of the data flow (recipient)
- Description of the data flow (payload)
- Image of the data flow in isolation

Individual threat candidates include:

- Threat ID (unique)
- Category (based on the analysis classification scheme [such as **STRIDE**])
- Summary of the threat
- Detailed description of the threat

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

References

1. **Document Management System**
   https://en.wikipedia.org/wiki/Document_management_system
2. **Data Flow Diagram (DFD)**
   https://en.wikipedia.org/wiki/Data-flow_diagram
3. **STRIDE**
   https://en.wikipedia.org/wiki/STRIDE_(security)
4. **Threat Prioritization Plan** (AVCDL secondary document)
5. **Ranked / Risked Threat Report** (AVCDL secondary document)
6. **Threat Modeling Report** (AVCDL tertiary document)