Updated Threat Model

Revision

Version 3
11/15/21 10:55 AM

SME

Charles Wilson

Abstract

This document describes the process used to update the threat model.

Group / Owner

Security / Security Architect

Motivation

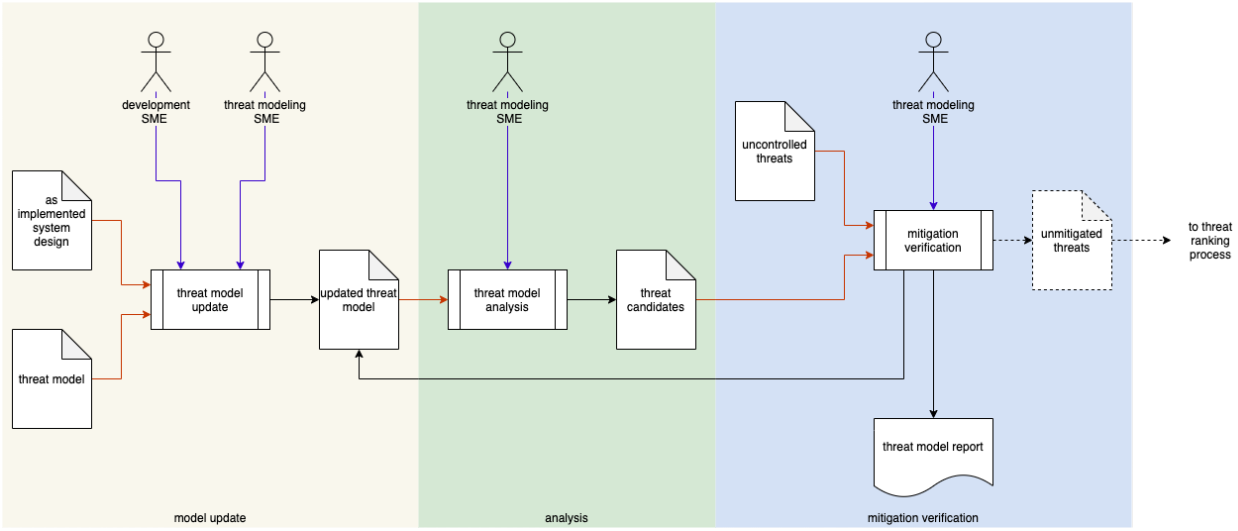
This document is motivated by the need to determine whether the security deficiencies identified during the design phase have been appropriately disposed. This is necessary given the nature of safety-critical, cyber-physical systems, subject to certifications such as **ISO 21434** and **ISO 26262**.

License

Overview

Many changes can occur between the creation/update of a threat model during the design phase and the verification phase. Reviewing the threat model allows for the verification that issues identified for mitigation have been appropriately dealt with and that no new issues have arisen.

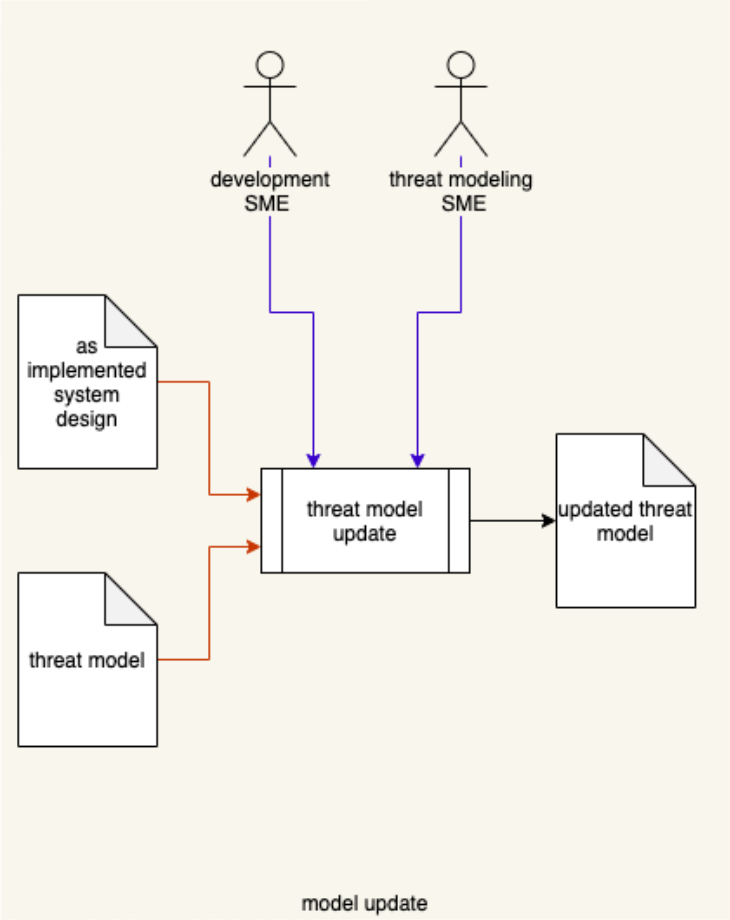
The following diagram illustrates the process to be used:



Process

Model Update

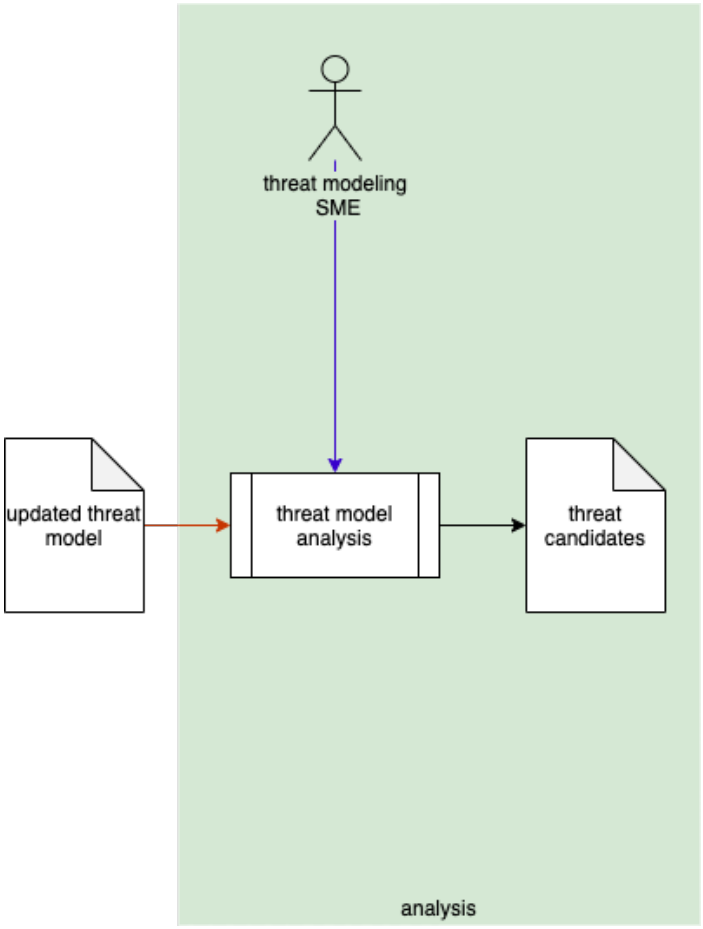
Inputs	As Implemented System design Threat Model
Outputs	Updated threat model
Participants	Development SME Threat modeling SME



The threat modeling SME works with the development SME(s) to create an **updated threat model** of the system. The **as-implemented system design** is used to update the threat model created in the design phase.

Analysis

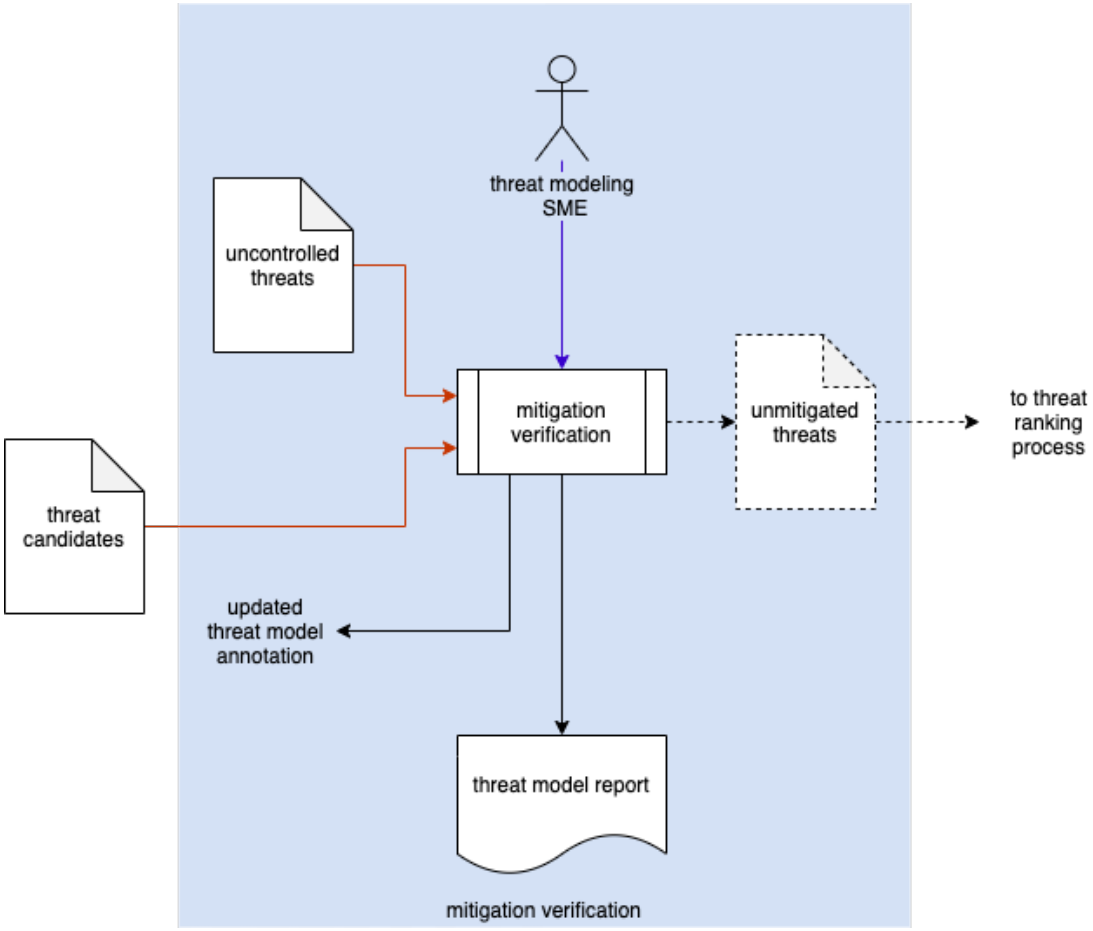
Inputs	Updated threat model
Outputs	Threat candidates
Participants	Threat modeling SME



The threat modeling SME takes the **updated threat model** and performs a threat analysis. This results in the creation of a list of **threat candidates**.

Mitigation Verification

Inputs	Threat candidates Uncontrolled threats
Outputs	Unmitigated threats
Participants	Threat modeling SME



The threat modeling SME takes the **threat candidates** and the previously established **uncontrolled threats** generated in the design phase and verifies that all uncontrolled threats have been mitigated. A **threat model report** is generated. The **updated threat model** is annotated with the findings of the verification. If any uncontrolled threats remain, a list of **unmitigated threats** is generated and passed along to the threat ranking process (specified in the **Threat Prioritization Plan**).

References

1. **Threat Prioritization Plan** (AVCDL secondary document)
2. **Threat Modeling Report** (AVCDL secondary document)