Attack Surface Analysis Report

Revision

Version 3
11/15/21 9:45 AM

SME

Charles Wilson

Abstract

This document describes the process used to perform and report on an attack surface analysis.

Group / Owner

Security / Security Architect

Motivation

This document is motivated by the need to have the minimal necessary attack surface. This is necessary given the nature of safety-critical, cyber-physical systems, subject to certifications such as **ISO 21434** and **ISO 26262**.

License

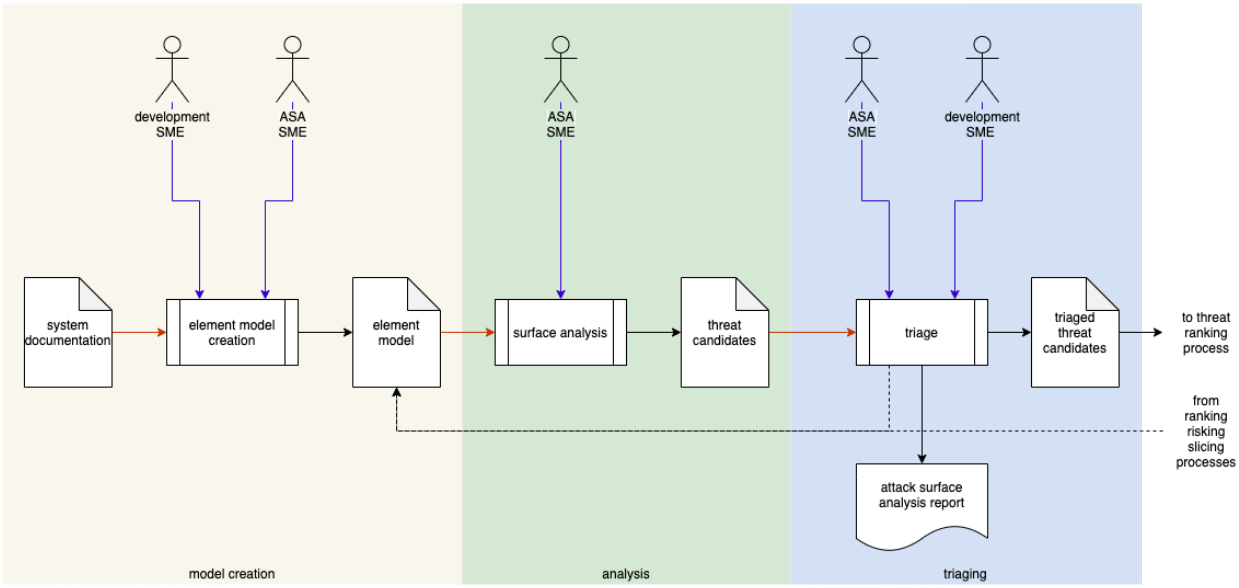
Overview

Attack Surface Analysis (**ASA**) is the process of evaluating an element of a system using only knowledge of the interfaces it presents. The analysis drives recommendations for reduction of the element's attack surface reducing the potential number of attack paths. Attack surface reduction encompasses shutting off or restricting access to system services, applying the principle of least privilege, and employing layered defenses wherever possible. ASA considers the API surface of a trusted entity. The most important entity is the operating environment but may be a stand-alone element which the system depends on.

Note: Microsoft has created a cross-platform application [1] which analyzes the footprint of an application to determine the attack surface presented.

Note: Attack surface analysis is a methodology which trails in maturity when compared with threat modeling. Automated measures in this area will be limited.

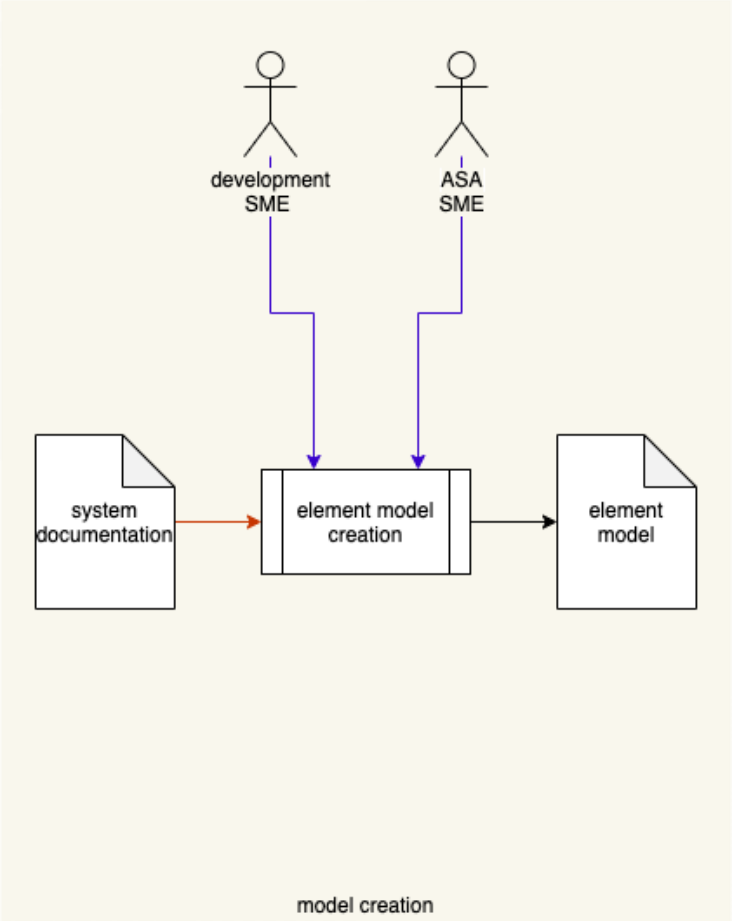
The following diagram illustrates the process to be used:



Process

Model Creation

Inputs	Element documentation
Outputs	Element model
Participants	Development SME ASA SME

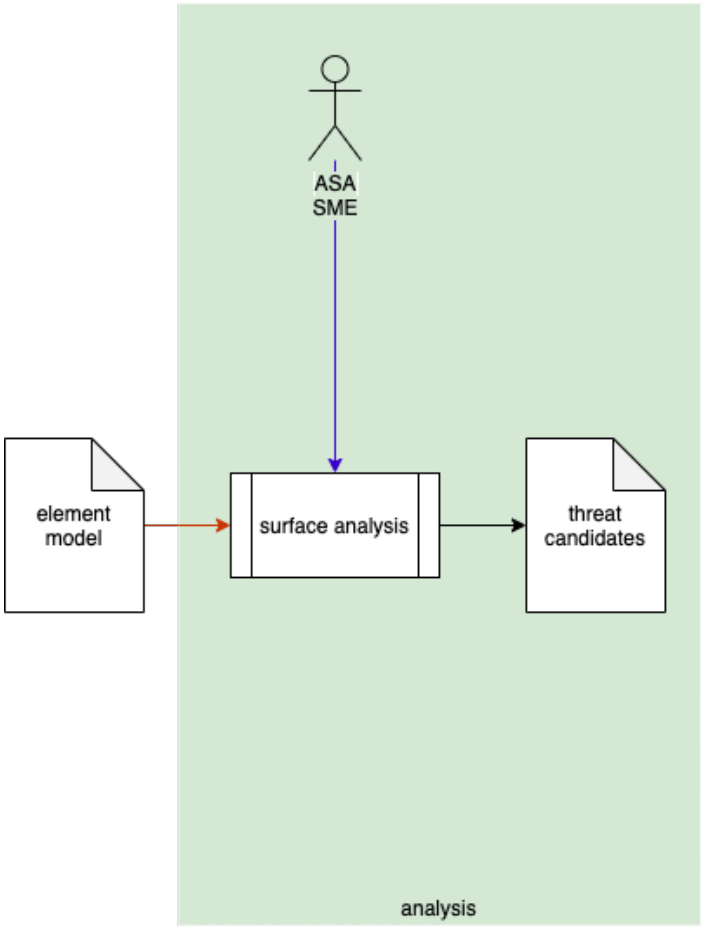


The ASA SME works with the development SME(s) to create a model of the system suitable for analysis. Any existing documentation regarding the element is used as input to this process. For this activity, models should be created using a formal modeling tool when possible. This may be a set of models depending on the complexity of the system.

Unlike the threat modeling activity, the ASA activity presumes that the trust boundary is the entire surface of the element under consideration.

Analysis

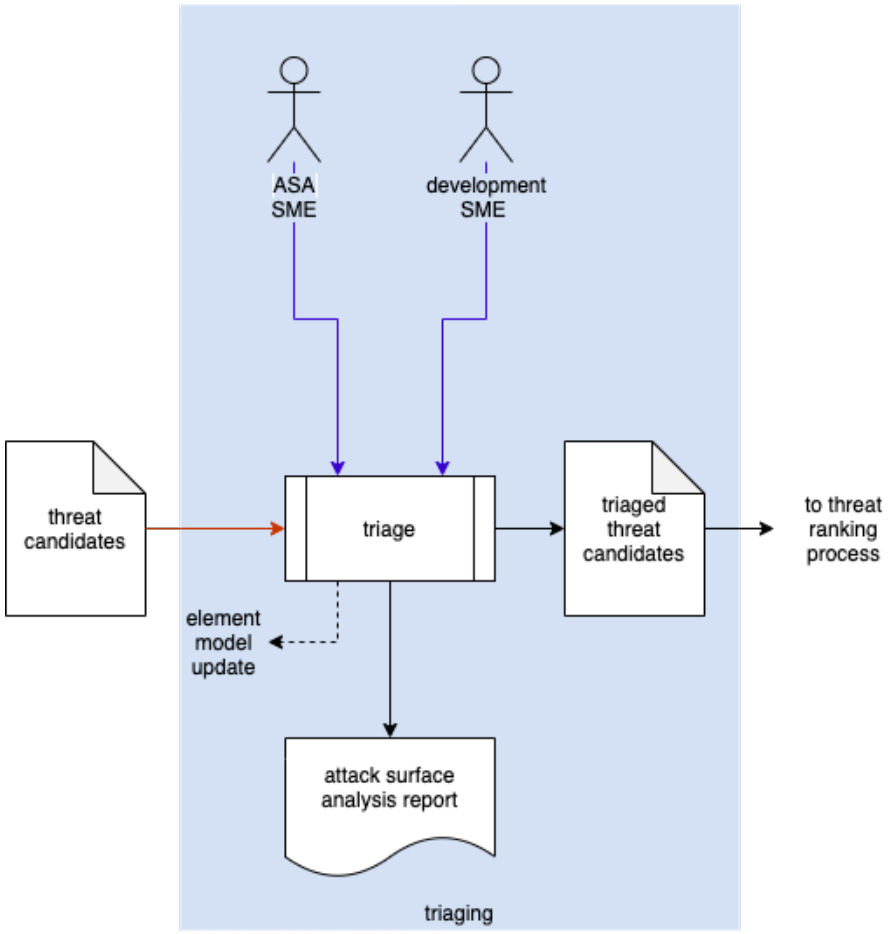
Inputs	Element model
Outputs	Threat candidates
Participants	ASA SME



The ASA SME processes the element model to evoke a set of threat candidates. Candidates are those aspects of the element's presented surface which are not required for implementation of the system. These may include services, ports, APIs, protocols, etc.

Triage

Inputs	Threat candidates
Outputs	Triaged threat candidates Attack surface analysis report
Participants	Development SME ASA SME



The ASA 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 the **Attack Surface Analysis Report** and a set of **triaged threat candidates**. The candidates are passed along per the **Threat Prioritization Plan**.

Report Content

Attack Surface Analysis Report

The attack surface analysis report should detail the areas of excessive exposure. These should be organized by type and provide sufficient information to enable a developer to reduce the exposure level. These will form a 3-tuple (**type**, **reason**, **mitigation**)

Types of excessive exposure include:

- Ports (physical and logical)
- Protocols
- System services
- Data structures
- User accounts
- Diagnostics
- Remote execution
- Data connection lifetime
- Features
- Memory (general resource) pressure susceptibility

Reasons for reduction include:

- Unused
- Debug-only (non-production)
- Out-of-specification (unchecked protocol parameters, extra commands, …)

The recommended mitigation should be actionable and verifiable.

Triaged Threat Candidates

The triaged threat candidates have the same structure as those derived from threat modeling. Refer to the **Threat Modeling Report** secondary document for additional information.

References

1. **Microsoft Attack Surface Analyzer**
   https://github.com/microsoft/attacksurfaceanalyzer
2. **Threat Modeling Report** (AVCDL secondary document)
3. **Threat Prioritization Plan** (AVCDL secondary document)