

# Secure Design Review Standard Operating Procedures (SOP)

[Application Threat Modeling SOP]

NOVEMBER 14, 2016



## Revision History

**Table 1. Revision History**

<b>Date</b>	<b>Version</b>	<b>Description</b>	<b>Author</b>
11/14/2016	1.0	First public release	Booz Allen Hamilton

## Table of Contents

1	Introduction .....	1
1.1	Document Audience .....	1
2	Secure Design Reviews .....	3
2.1	Roles and Responsibilities .....	3
2.2	Process Overview .....	4
2.3	Prerequisites .....	5
2.3.1	Requirements to request the development of an initial threat model .....	5
2.3.2	Requirements to request the validation of a finalized threat model .....	5
2.4	Scheduling .....	6
2.5	Deliverables .....	6
2.5.1	Initial threat model development deliverables .....	6
2.5.2	Finalized threat model validation deliverables .....	6
	Appendix A – Resources .....	7

# 1 Introduction

This document provides a high-level overview of how secure design review (application threat modeling) is conducted for custom-developed software applications agency-wide as part of the Department of Veterans Affairs (VA) Office Information Security (OIS) Software Assurance (SwA) Program. This document provides information to assist VA application developers with understanding secure design review processes, including performing secure design reviews of applications in a collaborative fashion with VA's SwA Program Office during development and also during the Assessment and Authorization (A&A) and continuous monitoring.

Broadly speaking, application-level vulnerabilities manifest themselves as one of two types: **design flaws** introduced by weaknesses during the requirements, design, or architecture phase; or **implementation bugs** introduced by weaknesses during the actual coding of the application. While VA Secure Code Review SOP focuses primarily upon implementation bugs, VA Secure Design Review SOP focuses on design flaws. This SOP leverages the Microsoft Threat Modeling Tool that supports the "Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege" (STRIDE) threat modeling process. STRIDE is an iterative process where an application's design is systematically decomposed and formulaically analyzed for vulnerabilities.

The introduction of application threat modeling at VA expands secure software development policies and practices not only for applications currently compatible with the requirements of VA Secure Code Review SOP, but also in particular for applications that are written in programming languages and / or environments that Hewlett Packard Enterprise (HPE) Fortify Static Code Analyzer (SCA) cannot successfully scan (e.g., many legacy applications). VA Secure Design Review SOP enables **all** VA applications to be analyzed, at a minimum, for design-related security flaws, providing a more comprehensive understanding of the security posture of custom-developed software applications agency-wide.

## 1.1 Document Audience

The processes described in this document are primarily intended for VA application developers and stakeholders that support VA SwA Program secure design review processes agency-wide, including:

- **VA Application Developers**

VA application developers may be either VA employees or contractors. The VA application developer performs secure design reviews of their applications in a collaborative fashion with VA SwA Program Office.

- **VA Software Assurance Program Office**

VA SwA Program Office manages the agency-wide VA SwA Program. The VA SwA Program Office establishes secure code review and secure design review

Standard Operating Procedures (SOP) and works with VA application developers in a collaborative fashion to perform application-level security analysis and to implement A&A and continuous monitoring authorization checks.

- **VA Certification Program Office (CPO)**

VA CPO implements the A&A and continuous monitoring processes process to support Federal Information Security Management Act (FISMA) compliance. The CPO gains its authority, in part, from VA Handbook 6500.3.

- **VA Network Security Operations Center (NSOC)**

VA NSOC provides continuous, around-the-clock monitoring of VA's network. VA NSOC personnel deter, detect, and defeat potential threats that may adversely affect VA networks and systems.

- **VA National Service Desk (NSD)**

VA NSD implements an agency-wide Tier 1 and Tier 2 help desk support function using its ticketing process. Ticketing categories and workflows have been created to support VA SwA Program Office to facilitate service requests.

## 2 Secure Design Reviews

Secure design reviews of VA custom-developed applications are conducted during development and also during authorization processes. Secure design reviews unlike secure code reviews may be performed before any code is written. Secure design review validations (i.e. reviews of application threat models by VA SwA Program Office to ensure compliance with VA Secure Design Review SOP) are conducted during A&A and continuous monitoring processes in a similar fashion as VA Secure Code Review SOP.

Close cooperation between the OIS and VA agencies and offices developing custom applications is critical to achieving secure design review objectives and increasing the level of confidence in the security of software developed specifically for use at VA.

Primary objectives of conducting secure design reviews at VA are to:

- Encourage the use of threat modeling tools during VA application development to promote the adoption of secure design principles and practices
- Ensure that secure design reviews are performed consistently and cost-efficiently
- Improve the security of VA applications agency-wide

### 2.1 Roles and Responsibilities

Roles and responsibilities for conducting secure design reviews at VA:

- **VA Application Developer Role and Responsibilities**
  - Determine and obtain their program and project needs for secure design reviews and assistance from VA SwA Program office
  - Work with VA SwA Program office to develop an initial threat model in a collaborative fashion
  - Analyze and refine threat models during development
  - Finalize threat models as needed during the authorization process
  - Make appropriate adjustments to the application design and corresponding source code implementation
  - Include mitigations in their application design and corresponding source code implementation for vulnerabilities identified in underlying third-part dependencies (e.g. open source or commercial libraries or frameworks)
- **VA Software Assurance Program Office Role and Responsibilities**
  - Work with VA developers to develop application threat models in a collaborative fashion
  - Perform validations of threat models developed according to VA Secure Design Review SOP
  - Provide end user support for threat modeling tools that are approved for use by VA SwA Program Office

- Provide secure design review validation support for secure design review validations as per this SOP
- **VA Certification Program Office (CPO) and VA Network Security Operations Center (NSOC) Role and Responsibilities**
  - Provide authorization requirements and guidelines during A&A and continuous monitoring processes
- **VA National Service Desk (NSD) Role and Responsibilities**
  - Provide support for VA SwA Program Office categories and workflows for secure design review service requests

## 2.2 Process Overview

The overall process consists of VA SwA Program Office working with VA developers to develop an initial threat model, VA developers refining and analyzing the model, then VA SwA Program Office validating the finalized model during authorization processes. Goals of threat model analysis are to identify potential architectural vulnerabilities as early as possible. Early detection enables easier and more cost-effective architectural changes to be made versus later in the software development lifecycle.

VA SwA Program Office validations review finalized models to ensure that best practices for performing secure design review have been followed. VA SwA Program Office determines whether additional analysis is needed, and assists VA application developers to ensure they understand how to meet the standards required. After validations are completed, the results are provided to the CPO and NSOC.

The overall secure design review process includes activities taken by VA application developers during development and also during authorization processes, as follows:

1. If it has not been done already, register the application with VA SwA Program Office
2. Upload required lists of technologies/libraries utilized, sequence diagrams, and other requested information to the VA SwA file server (see [Prerequisites](#))
3. Open a NSD ticket according to VA SwA Program Office procedures to request the development of an initial threat model diagram
4. Work iteratively with VA SwA Program Office to develop an initial threat model diagram based on the initial documentation provided (see [Deliverables](#))
5. Analyze the collaboratively-developed model to determine appropriate mitigations to identified potential vulnerabilities
6. Upload finalized threat model file, documentation supporting threat model mitigations, and other requested information (see [Prerequisites](#))
7. Open a NSD ticket according to VA SwA Program Office procedures to request the validation of the finalized threat model diagram

8. Resolve any issues identified during validation (see [Deliverables](#))

## 2.3 Prerequisites

The latest version of the Microsoft Threat Modeling Tool is required to be used in order to develop and analyze VA application threat models. Requirements for VA SwA Program Office secure design review service requests are below.

### 2.3.1 *Requirements to request the development of an initial threat model*

The following items are required in order to request the development of an initial threat model:

1. Lists of technologies/libraries utilized,
2. Sequence diagrams,
3. Deployment diagrams,
4. Lists of application interfaces and services utilized,
5. Installation and configuration procedures (if available), and
6. Readme file that explains where to find each of the above items within the provided documentation.

The above items should include the following information as appropriate:

- All external interfaces
- The nature of information being stored or processed by the application (e.g., categorization of information types)
- The protection mechanisms associated with each interface and model feature as appropriate
- Any unique application security requirements

### 2.3.2 *Requirements to request the validation of a finalized threat model*

The following items are required in order to request a secure design review validation:

1. Secure design review request form that has been filled out as per VA SwA Program Office procedures.
2. Threat model tool scan result file (Microsoft Threat Modeling Tool “.tm4” extension file).
3. All findings reported by the Microsoft Threat Modeling Tool have been analyzed in the TM4 file.
4. All mitigation descriptions must include documentation references, and referenced documentation must additionally be provided.
5. If a finding is a false positive, it has been analyzed as “Not Applicable,” with comments added to the TM4 stating the reason it is considered a false positive.

6. All model issues reported by the Microsoft Threat Modeling Tool have been fixed or addressed.

Note: Any model issues reported by the Microsoft Threat Modeling Tool can be seen in the Design View.

7. The most recent version of the Microsoft Threat Modeling Tool, and the threat model that was developed collaboratively with VA SwA Program Office were used when analyzing and finalizing the model.

## 2.4 Scheduling

After creating a secure design review request package, either to develop the initial model or to perform a validation, VA application developers will need to open a NSD ticket according to VA SwA Program Office request procedures. During the scheduling process, VA SwA Program Office will review the provided request package for their completeness (i.e. whether all request package items have been provided) and then coordinate further as needed with the VA developer to schedule the work.

## 2.5 Deliverables

VA Secure Design Review SOP defines two activities, each of which has different deliverables, depending on the activity as indicated below.

### 2.5.1 Initial threat model development deliverables

After an initial threat model has been developed, the following will be provided by VA SwA Program Office to the VA application developer:

1. Threat model tool scan result file (Microsoft Threat Modeling Tool “.tm4” extension file)
2. A Microsoft Lync online meeting invitation to review the initial model and to follow up to make any initial changes as needed

Note: It is the responsibility of VA application developers to maintain threat models and any corresponding analysis for application releases as appropriate and when new threats are discovered.

### 2.5.2 Finalized threat model validation deliverables

After a finalized threat model has been validated, the following will be provided by VA SwA Program Office to the VA application developer:

1. Secure design review validation report (PDF file), and
2. Secure design review validation entry on VA SwA Support Site (web page)

Note: It is the responsibility of VA application developers to upload the secure design review validation report and final application threat models and other deliverables to RiskVision as appropriate.

## Appendix A – Resources

- **[Microsoft Threat Modeling Tool](#)**

This site provides information about the Microsoft Threat Modeling Tool, including [download information](#). Technical guidance is also provided about how to use the tool, and about the method of threat modeling the tool implements.

- **[VA Software Assurance Support Site \(Public Wiki\)](#)**

This site is publicly accessible and provides information about the VA SwA Program, including procedures to request services, [FAQs](#), [Technical Notes](#), and VA SwA Program Office [Blog](#).

- **[VA Software Assurance Support Site \(Protected SharePoint Site List\)](#)**

This site is only accessible on the VA network and includes the current inventory of custom-developed applications that have been inventoried by VA SwA Program Office, and also results of validations.