



threat

MICROSOFT THREAT MODELING

25-7-2023

TABLE OF CONTENT

Overview	3
Microsoft threat modeling.....	3
Why do we use it?	3
How do we use it?	3
Conclusion	9

OVERVIEW

Microsoft Threat Modeling Tool 2016 is an easy-to-use tool that can:

- Create data flow diagrams (DFDs) for products or services.
- Analyze data flow diagrams to automatically generate a set of potential threats.
- Suggest potential mitigations to design vulnerabilities.
- Produce reports on the identified and mitigated threats.
- Create custom templates for threat modeling.

MICROSOFT THREAT MODELING

Microsoft Threat Modeling is a structured approach and toolset for identifying and addressing security threats in software applications and systems, promoting proactive cybersecurity.

Why do we use it?

These tools help security professionals and developers visualize, analyze, and mitigate risks early in the development process, resulting in more secure and robust software. Additionally, Microsoft Threat Modeling Tools integrate well with other Microsoft security solutions, making them a convenient and effective choice for threat modeling in Microsoft environments.

How do we use it?


1. Download and install the Microsoft Threat Modeling Tool on your computer.

Microsoft Threat Modeling Tool 2016

Important! Selecting a language below will dynamically change the complete page content to that language.

Language: English Download

Choose the download you want

 File Name	Size
<input checked="" type="checkbox"/> Threat Modeling Tool 2016 Getting Started Guide.docx	1.3 MB
<input checked="" type="checkbox"/> Threat Modeling Tool 2016 User Guide.docx	1.6 MB
<input checked="" type="checkbox"/> ThreatModelingTool2016.msi	4.0 MB

Download Summary:
KBMBGB

1. Threat Modeling Tool 2016 Getting Started Guide.docx
2. Threat Modeling Tool 2016 User Guide.docx
3. ThreatModelingTool2016.msi

Total Size: 6.9 MB

Next

2. Create a new model: Launch the tool and start a new threat model project.

MICROSOFT THREAT MODELING TOOL 2016

Threat Model:

Create A Model

Model your system by drawing diagram (s). Make sure you capture important details.

Template For New Models

SDL TM Knowledge Base (Core)(4.1.0.9) Browse...

Open A Model

Open an existing model and analyze threats against your system; do not worry, the tool will help you identify them.

Recently Opened Models

[Sample Threat Model.tm7](#)

Getting Started Guide

A step-by-step guide to help you get up and running now.

Threat Modeling Workflow

1. Select your template.
2. Create your data flow diagram model.
3. Analyze the model for potential threats.
4. Determine mitigations.

Template:

Create New Template

Define stencils, threat types and custom threat properties for your threat model from scratch.

Open Template

Open an existing Template and make modifications to better suit your specific threat analysis.

Template Workflow

Use templates to define threats that applications should look for.

1. Define stencils
2. Define categories
3. Define threat properties
4. Define threat
5. Share your template

3. Define the System: Define the boundaries of your system, including components, data flows, and interactions. In this scenario, we create a simple design of a web application developed to interact with third-party service in between internet boundaries defined (External or Internal network)

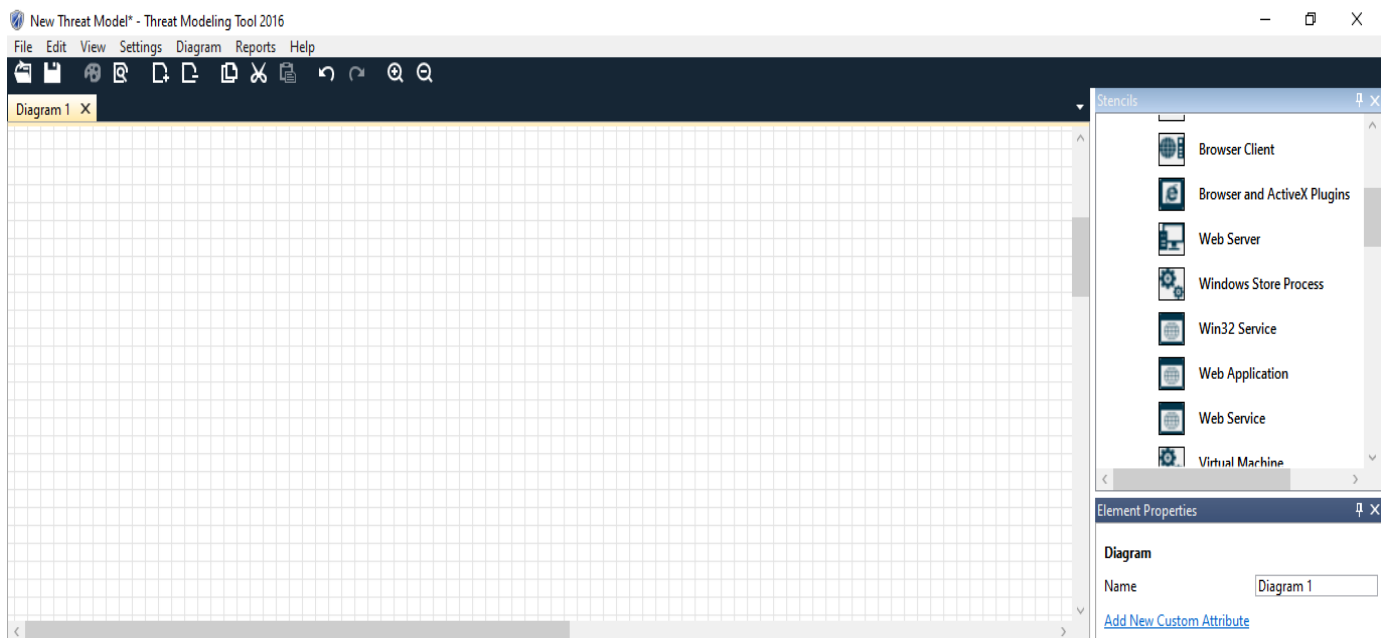


Figure 1 Design view

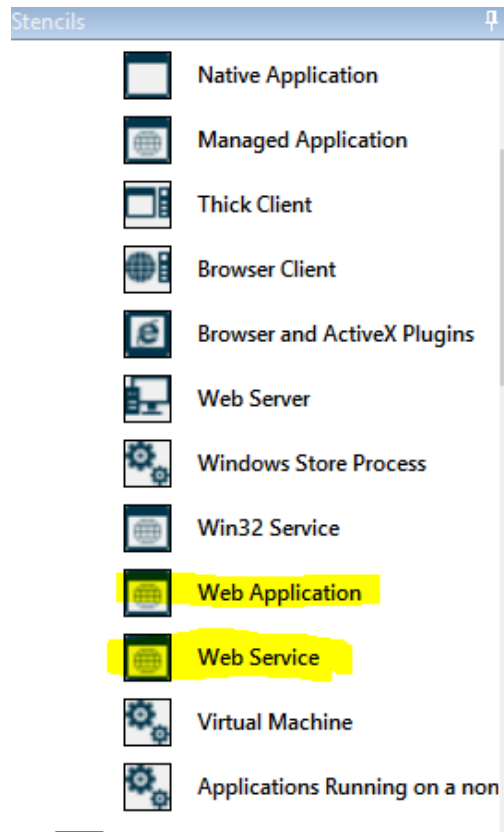


Figure 2 Select web Applications and Web services.

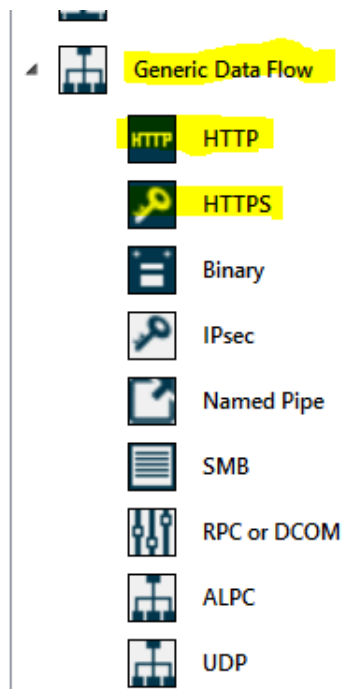


Figure 3: Go to Generic Data Flow and Select HTTP or HTTPS

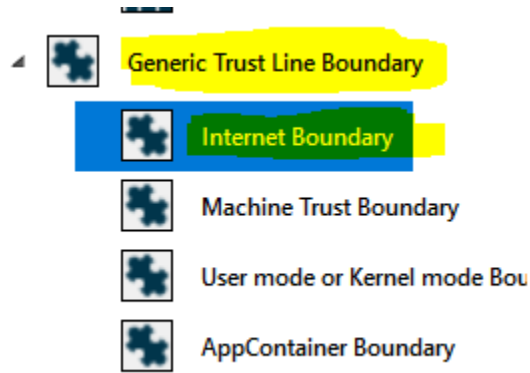


Figure 4 Goto generic Trust Line Boundary and select the Internet Boundary.

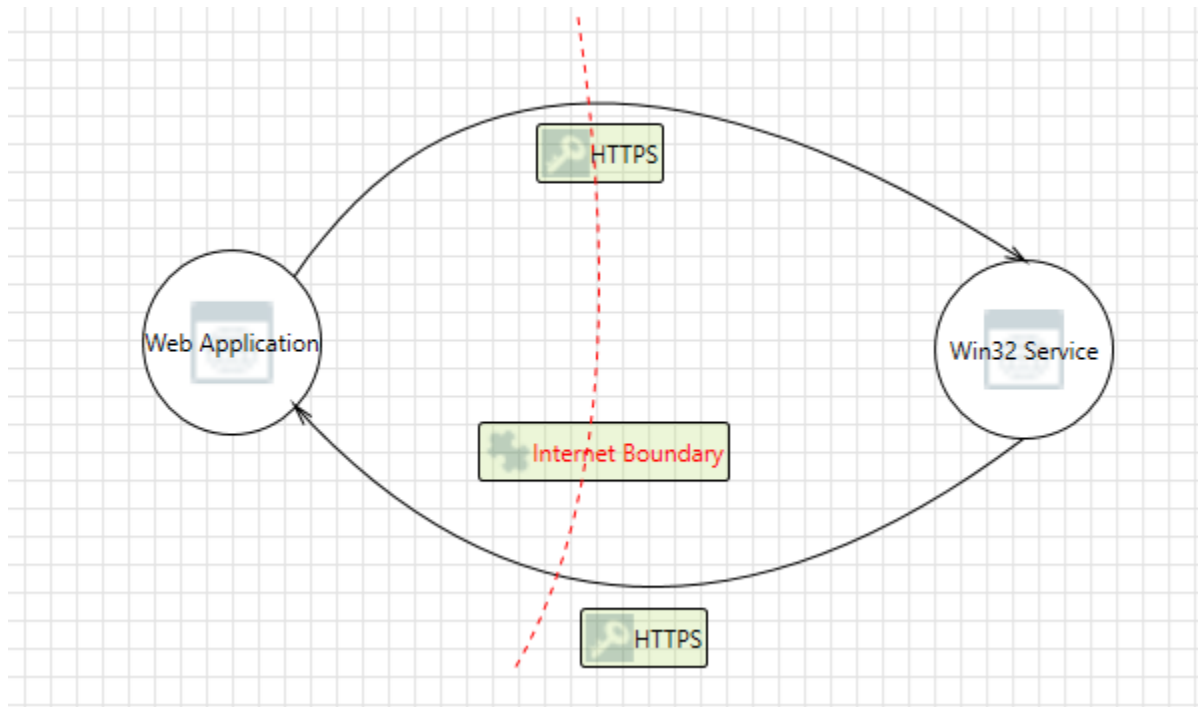


Figure 5 System Design

4. Analyze Design: After creating the design analyze potential threats that might occur.

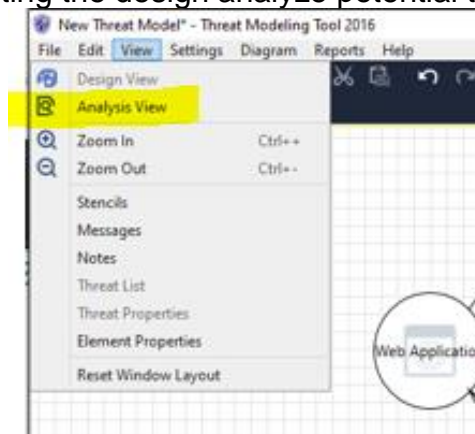


Figure 6 Click View and then Analyze View.

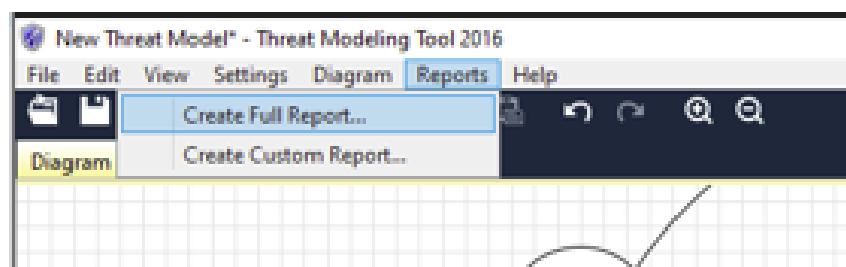
Threat List											
ID	Diagram	Changed By	Last Modified	State	Title	Category	Description	Justification	Interaction	Priority	
0	Diagram 1		Generated	Not Started	Web Applicati...	Tampering	If Web Applica...		HTTPS	High	
1	Diagram 1		Generated	Not Started	Elevation Usin...	Elevation Of Pr...	Win32 Service...		HTTPS	High	
4	Diagram 1		Generated	Not Started	Win32 Service...	Tampering	If Win32 Servic...		HTTPS	High	
5	Diagram 1	DESKTOP-P1D...	7/25/2023 8:35:...	Not Started	Cross Site Scri...	Tampering	The web server...		HTTPS	High	
6	Diagram 1		Generated	Not Started	Elevation Usin...	Elevation Of Pr...	Web Applicati...		HTTPS	High	
7	Diagram 1		Generated	Not Started	Spoofing the...	Spoofing	Web Applicati...		HTTPS	High	
18 Threats Displayed, 18 Total											
Threat Properties											
ID: 8	Diagram: Diagram 1		Status: Mitigated		Last Modified: DESKTOP-P1						
Category:	Repudiation										
Description:	Win32 Service claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.										
Justification:	This issue has been sorted										
Interaction:	HTTPS										
Priority:	High										
Threat Properties Notes - no entries											

Figure 7 Threat List with Description

- Mitigate: A risk can be mitigated with proper justification after analysis by security teams.

Threats in scope			
ID: 8	Diagram: Diagram 1	Status: Mitigated	Last Modified: DESKTOP-P1DD
Category:	Repudiation		
Description:	Win32 Service claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.		
Justification:	This issue has been sorted by implementing Strong authentication and collaborating with trusted third parties.		
Interaction:	HTTPS		
Priority:	High		
Threat Properties	Notes - no entries		

- Generate Report: Now you can download full or custom reports after analyzing lists of threats.



Threat Modeling Report

Created on 7/25/2023 10:43:06 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	17
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	1
Total	18
Total Migrated	0

Diagram: Diagram 1

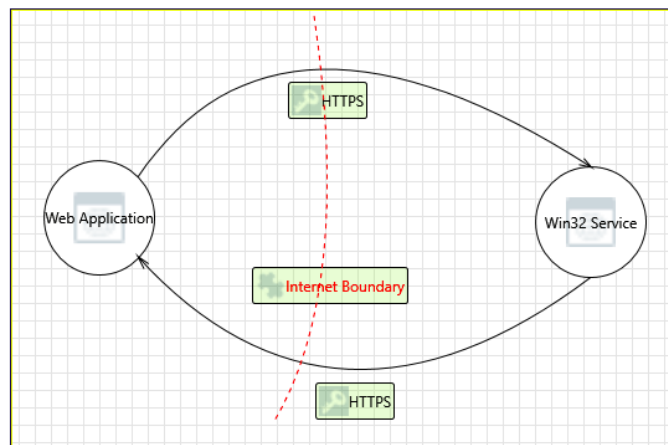
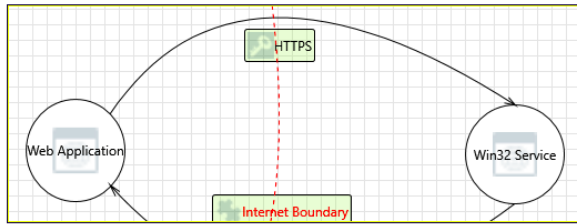


Diagram 1 Diagram Summary:

Not Started	17
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	1
Total	18
Total Migrated	0

Interaction: HTTPS



1. Web Application Process Memory Tampered [State: Not Started] [Priority: High]

Category: Tampering

Description: If Web Application is given access to memory, such as shared memory or pointers, or is given the ability to control what Win32 Service executes (for example, passing back a function pointer), then Web Application can tamper with Win32 Service. Consider if the function could work with less access to memory, such as passing data rather than pointers. Copy in data provided, and then validate it.

Justification: <no mitigation provided>

2. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: Win32 Service may be able to impersonate the context of Web Application in order to gain additional privilege.

Justification: <no mitigation provided>

7. Review and Iterate: Review the model with stakeholders and iterate as necessary to improve security.

By following these steps, you can effectively use the Microsoft Threat Modeling Tool to enhance the security of your software applications and systems.

CONCLUSION

Microsoft Threat Modeling Tool 2016 is an easy-to-use tool for creating data flow diagrams, identifying threats, suggesting mitigations, and producing reports. It promotes proactive cybersecurity and helps visualize and address risks during software development. Integrates well with Microsoft security solutions for convenience.