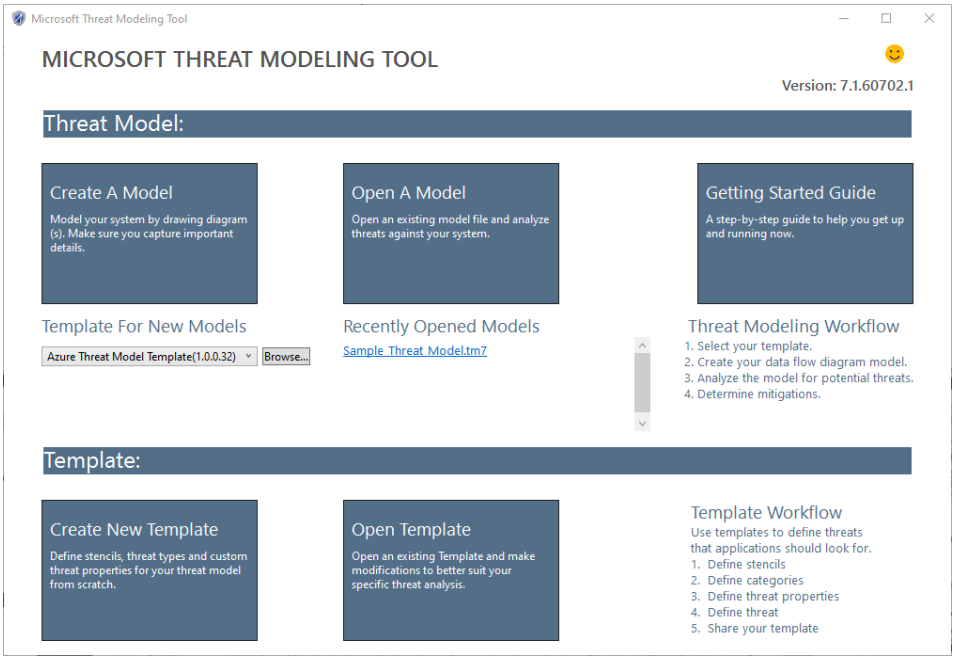
Introduction to Microsoft Threat Modeling Tool

Overview



In this lab, you are going to learn how to use Microsoft Threat Modeling Tool to draw Threat Model Diagram.

The Microsoft Threat Modeling Tool makes threat modeling easier for all developers through a standard notation for visualizing system components, data flows, and security boundaries. It also helps threat modelers identify classes of threats they should consider based on the structure of their software design. We designed the tool with non-security experts in mind, making threat modeling easier for all developers by providing clear guidance on creating and analyzing threat models.

The Threat Modeling Tool allows software architects to identify and mitigate potential security issues early, when they are relatively easy and cost-effective to resolve. As a result, it greatly reduces the total cost of development.

The tool enables anyone to:

1. Communicate about the security design of their systems
2. Analyze those designs for potential security issues using a proven methodology
3. Suggest and manage mitigations for security issues

Outcomes

Upon completion of this session, you should be able to

- Use Microsoft Threat Modeling Tool to draw Threat Models;
- Apply Threat Model in the project

Required Resources

Please download the tool via LMS, or https://aka.ms/threatmodelingtool

- Microsoft Windows 10 Anniversary Update or later
- .NET Version Required
- .NET 4.7.1 or later
- Additional Requirements
- An Internet connection is required to receive updates to the tool and templates.

1: Building a model

In this section, we follow:

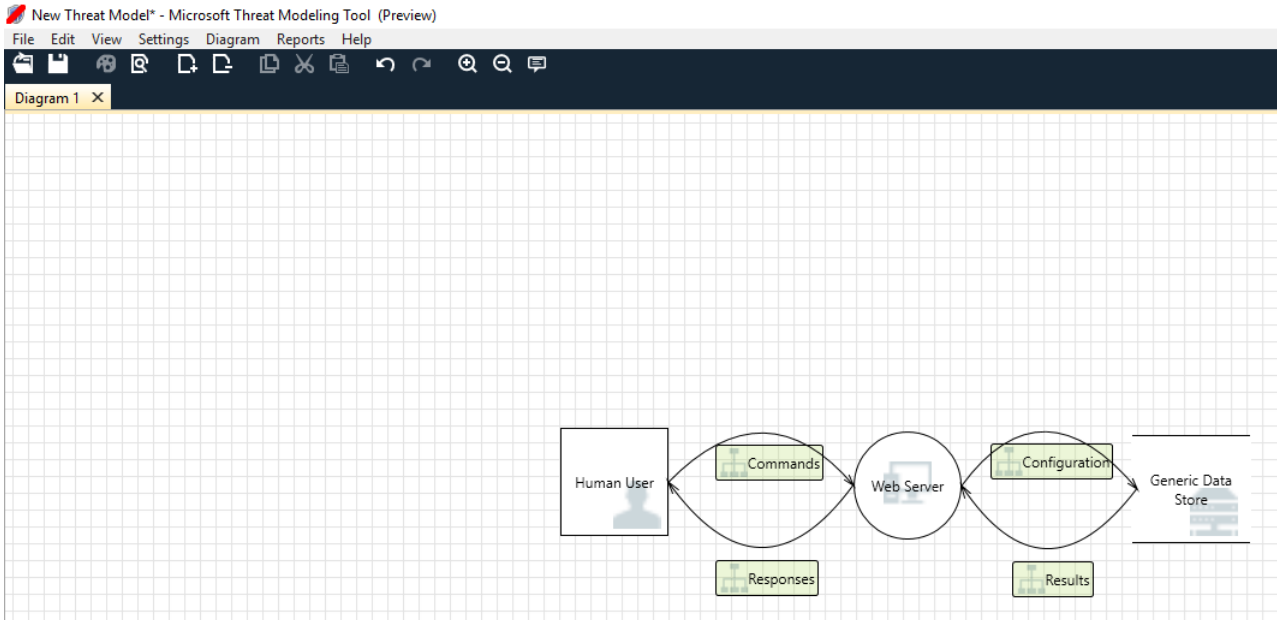
- **Cristina** (a developer) and
- **Ricardo** (a program manager)

They are going through the process of developing their first threat model:

Ricardo: Hi Cristina, I worked on the threat model diagram and wanted to make sure we got the details right. Can you help me look it over?

Cristina: Absolutely. Let's take a look.

Ricardo opens the tool and shares his screen with Cristina.



Cristina: Ok, looks straightforward, but can you walk me through it?

Ricardo: Sure! Here is the breakdown:

- Our human user is drawn as an outside entity—a square
- They're sending commands to our Web server—the circle
- The Web server is consulting a database (two parallel lines)

What Ricardo just showed Cristina is a DFD, short for **Data Flow Diagram**.

The Threat Modeling Tool allows users to specify trust boundaries, indicated by the red dotted lines, to show where different entities are in control.

For example, IT administrators require an Active Directory system for authentication purposes, so the Active Directory is outside of their control.

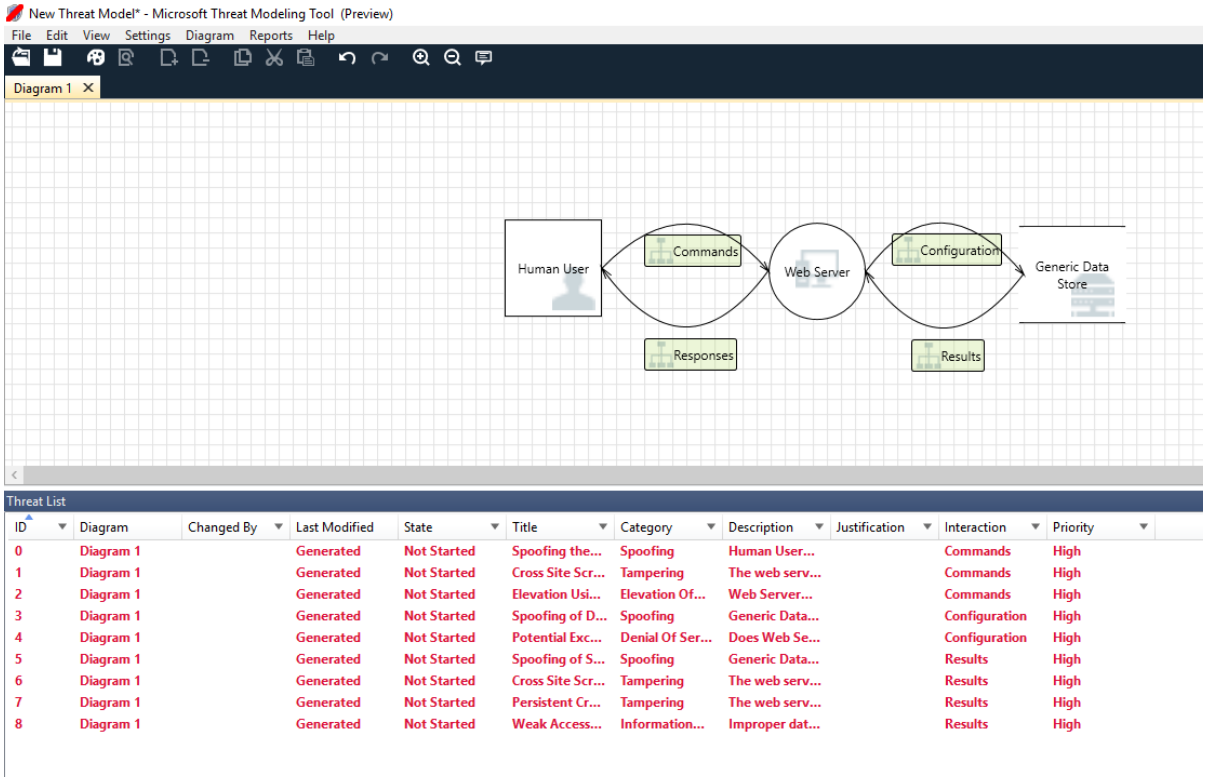
Cristina: Looks right to me. What about the threats?

Ricardo: Let me show you.

2: Analyzing threats

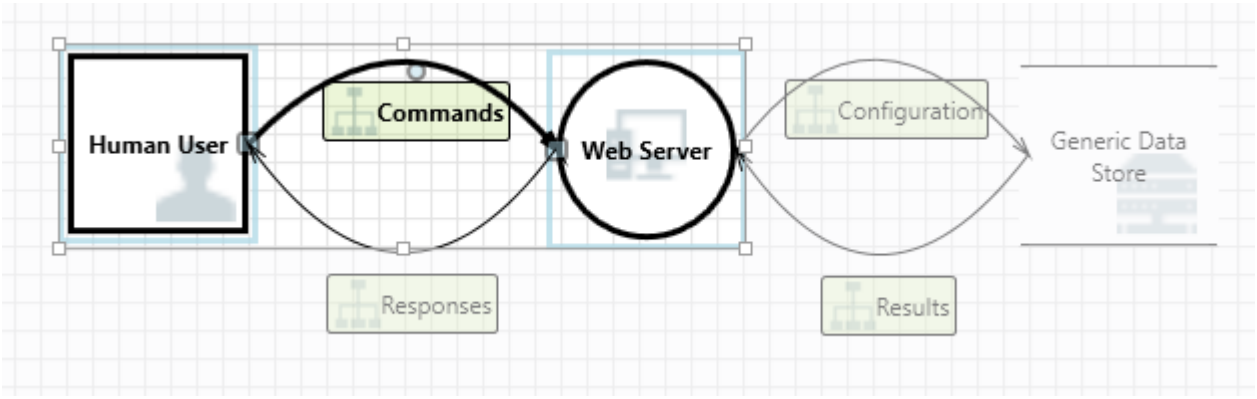
Once he clicks on the analysis view from the icon menu selection (file with magnifying glass), he is taken to a list of generated threats the Threat Modeling Tool found based on the default template, which uses the SDL approach called **STRIDE (Spoofing, Tampering, Info Disclosure, Repudiation, Denial of Service and Elevation of Privilege)**. The idea is that software comes under a predictable set of threats, which can be found using these 6 categories.

This approach is like securing your house by ensuring each door and window has a locking mechanism in place before adding an alarm system or chasing after the thief.

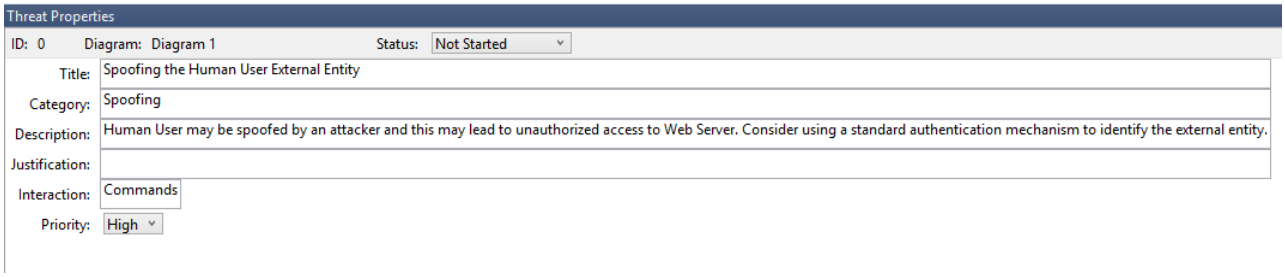


Ricardo begins by selecting the first item on the list. Here's what happens:

First, the interaction between the two stencils is enhanced



Second, additional information about the threat appears in the Threat Properties window



The generated threat helps him understand potential design flaws. The STRIDE categorization gives him an idea on potential attack vectors, while the additional description tells him exactly what's wrong, along with potential ways to mitigate it. He can use editable fields to write notes in the justification details or change priority ratings depending on his organization's bug bar.

The description made him realize the importance of adding an authentication mechanism to prevent users from being spoofed, revealing the first threat to be worked on. A few minutes into the discussion with Cristina, they understood the importance of implementing access control and roles. Ricardo filled in some quick notes to make sure these were implemented.

As Ricardo went into the threats under Information Disclosure, he realized the access control plan required some read-only accounts for audit and report generation. He wondered whether this should be a new threat, but the mitigations were the same, so he noted the threat accordingly. He also thought about information disclosure a bit more and realized that the backup tapes were going to need encryption, a job for the operations team.

Threats not applicable to the design due to existing mitigations or security guarantees can be changed to “Not Applicable” from the Status drop-down. There are three other choices: Not Started – default selection, Needs Investigation – used to follow up on items and Mitigated – once it’s fully worked on.

3: Reports & sharing

Once Ricardo goes through the list with Cristina and adds important notes, mitigations/justifications, priority and status changes, he selects Reports -> Create Full Report -> Save Report, which prints out a nice report for him to go through with colleagues to ensure the proper security work is implemented.

4: Tasks

- Discuss in your team, draw the data flow diagram using the Microsoft Threat Modelling Tool for your project application.
- Address and discuss how your team are going to design the application based on **STRIDE** (Spoofing, Tampering, Info Disclosure, Repudiation, Denial of Service and Elevation of Privilege)

Threat Modeling Report

Created on 7/31/2017 12:35:42 PM
Threat Model Name:
Owner:
Reviewer:
Contributors:
Description:
Assumptions:
External Dependencies:

Threat Model Summary:

Not Started	9
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	9
Total Migrated	0

Diagram: Diagram 1

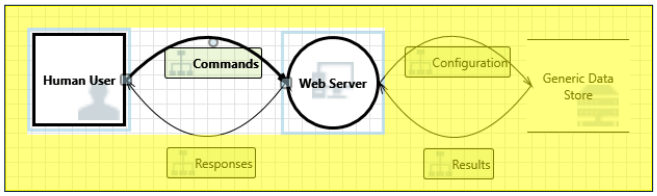
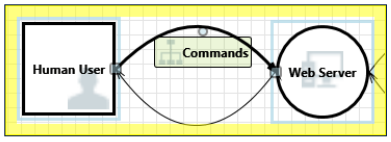


Diagram 1 Diagram Summary:

Not Started	9
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	9
Total Migrated	0

Interaction: Commands



1. Spoofing the Human User External Entity [State: Not Started] [Priority: High]

Category:	Spoofing
Description:	Human User may be spoofed by an attacker and this may lead to unauthorized access to Web Server. Consider using a standard authentication mechanism to identify the external entity.
Justification:	<no mitigation provided>
Possible Mitigation(s):	
SDL Phase:	Design

2. Cross Site Scripting [State: Not Started] [Priority: High]

Category:	Tampering
Description:	The web server 'Web Server' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
Justification:	<no mitigation provided>
Possible Mitigation(s):	
SDL Phase:	Design

Sample of the Threat Modeling Report

4: Reference

https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-getting-started

https://www.youtube.com/watch?v=ITYg6JMz7iE

END OF DOCUMENT