

|  |  |
| --- | --- |
| Microsoft Threat Modeling Tool 2014  User Guide | |
| Microsoft Trustworthy Computing  2014 |  |

Contents

[Overview 2](#_Toc384991832)

[Threat Modeling with STRIDE 2](#_Toc384991833)

[Standard Threat Mitigations 5](#_Toc384991834)

[Purpose of Tool 6](#_Toc384991835)

[Installation 6](#_Toc384991836)

[Analysis of Threat Modeling Output 6](#_Toc384991837)

[Features 6](#_Toc384991838)

[The Initial Screen 7](#_Toc384991839)

[Design View 7](#_Toc384991840)

[Analysis View 24](#_Toc384991841)

[Troubleshooting 27](#_Toc384991842)

[Automation 27](#_Toc384991843)

[Support 27](#_Toc384991844)

[Appendices 28](#_Toc384991845)

[Appendix I — Creating Bugs for Tracking Systems 28](#_Toc384991846)

[Appendix II — Extending the Threat Knowledge Base 29](#_Toc384991847)

[Appendix III — Drawing Surface Keyboard Navigation and General Keyboard Shortcuts 36](#_Toc384991848)

# Overview

Microsoft Threat Modeling Tool 2014 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

A threat model is (1) a representation of the software or device components in a system, (2) the data flows between them and (3) the trust boundaries in the system. When threat-modeling, potential design vulnerabilities can be discovered by analyzing the system’s security properties and identifying potential threats to the information assets in the system.

Unlike pure verification techniques, such as penetration testing or fuzzing, threat-modeling can be performed before a product or service has been implemented; this helps ensure that a product or service is as much as possible secure by design.

Software-centric threat-modeling can be summarized as:

* Diagram
* Draw the system architecture
* Add details and draw the trust boundaries
* Identify threats
* Find threats using a methodology, such as STRIDE per interaction
* Address threats
* Redesign the component to use a standard mitigation
* When necessary, create a custom mitigation
* Validate
* Validate that the threat-model diagram matches what is implemented
* Validate that each potential threat has a mitigation

The SDL threat-modeling approach starts with a data flow diagram. From the diagram, potential threats are identified. For each threat, mitigations are proposed. In some cases, the mitigation takes the form of changing the design itself, in which case the new or changed elements must be analyzed in an additional iteration.

When the mitigations have been implemented, the product or service is validated against the threat model to ensure that the mitigations work and that design functionality and performance are sufficient. If the design has serious security issues, revisiting the design and the threat model may be appropriate.

## Threat Modeling with STRIDE

The Microsoft Threat Modeling Tool for SDL applies a particular threat-modeling approach called *STRIDE per Interaction.* STRIDE is an acronym for the threat types of **S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service, and **E**levation of privilege. STRIDE is a way to find a wide variety of threats using these easy-to-remember threat types. Not all threats fit easily into a STRIDE category and some threats may fit into more than one category. More important than fitting a threat to a category is using the model to help you describe the threat and design an effective mitigation. With its matching of threats to mitigating features, STRIDE is also convenient way of moving the focus from threat to mitigation. Each threat is matched to the feature or property that should be present in the software to mitigate the threat, shown in Table 1.

| **Threat** | **Property** | **Threat Definition** | **Examples** |
| --- | --- | --- | --- |
| **Spoofing** | Authentication | Spoofing threats involve an adversary creating and exploiting confusion about who is talking to whom. Spoofing threats apply to the entity being fooled, not the entity being impersonated. Thus, external elements are subject to a spoofing threat when they are confused about what or whom they are talking to. | * Accounts.contoso.com is spoofed when it thinks that a user is giving it authorized credentials. * An adversary may have poisoned the DNS cache so accounts.contoso.com now points at a malicious system that looks exactly like the real accounts.contoso.com. |
| **Tampering** | Integrity | Tampering threats involve an adversary modifying data, usually as it flows across a network, resides in memory, on disk, or in databases. | * An adversary tampers with network packets, and changes commands after the user has logged in. * An adversary tampers with a registry key, making us run any program they choose. * An adversary tampers with a DLL, inserting the code into executable memory. * An adversary installs an unauthorized program on a computer. |
| **Repudiation** | Non-repudiation | Repudiation threats involve an adversary denying that something happened. | * Joe denies that he clicked on that link, for example to deny that he has benefited from a financial transaction. * Amy receives an email from Joe in which he agrees to a contract between the two. Later, Joe denies ever having sent that email. |
| **Information disclosure** | Confidentiality | Exposing information to someone not authorized to see it. | * Examples include passwords for known or unknown users, copies of emails, and names and social security numbers in a database.   As the last example makes clear, some information disclosure issues are also privacy issues. However, not all privacy issues are information disclosure issues. For example, the “Fair Information Practices” at the heart of most privacy and data protection laws usually include items such as notice, meaning that people should be informed that you are collecting certain data, and choice, meaning that users should get options about what data they provide, and how it will be used. For more on privacy issues, see the [Microsoft Privacy and Foundations of Trustworthy Computing.](http://www.microsoft.com/about/twc/en/us/privacy.aspx) |
| **Denial of service** | Availability | Deny or degrade service to users. | * An adversary prevents customers from connecting to a web site. * An adversary prevents the client from getting a DNS response. * An adversary prevents the client from speaking SSL, and forces a downgrade to an insecure connection. * An adversary can cause a program to crash. |
| **Elevation of privilege** | Authorization | Gain capabilities without proper authorization. | * An adversary who starts as an anonymous internet user can send commands to an application that execute as the web server. * An adversary with a web server can make code run as the local user. * An adversary who has the ability to log onto the machine as a standard user can become an administrator. |

Table STRIDE Definitions and Examples

STRIDE per Interaction is an approach that analyzes threats in the context of the interaction between two elements in the model.

## Standard Threat Mitigations

The following chart gives examples of standard mitigations for the threats in STRIDE. Standard mitigations, if practicable, are preferred over custom mitigations:

| **Threat** | **Property** | **Mitigations** |
| --- | --- | --- |
| **Spoofing** | Authentication | To authenticate principals:   * Windows authentication (NTLM) * Kerberos authentication * Windows or Live ID authentication * PKI systems such as SSL/TLS and certificates * IPsec * Digitally signed packets   To authenticate code or data:   * Digital signatures * Message authentication codes * Hashes |
| **Tampering** | Integrity | * Windows Discretionary Access Control Lists * Windows Mandatory Integrity Controls * Digital signatures * Message authentication codes |
| **Repudiation** | Non-repudiation | * Strong authentication * Secure logging and auditing * Digital signatures * Time stamps * Trusted third parties |
| **Information disclosure** | Confidentiality | * Encryption * ACLS |
| **Denial of service** | Availability | * Windows Discretionary Access Control Lists * Filtering * Quotas and rate limits * Authorization * High-availability designs |
| **Elevation of privilege** | Authorization | * Windows Discretionary Access Control Lists * Group or role membership * Privilege ownership * Permissions * Input validation |

Table STRIDE Threat Mitigations

# Purpose of Tool

The Microsoft Threat Modeling Tool for SDL is intended to assist in analyzing the design of a system for security risks and assist in mitigating the identified threats.

# Installation

For installation instructions and systems requirements, please see the *Threat Modeling Tool Getting Started Guide* available in the installation folder of Microsoft Threat Modeling Tool 2014.

# Analysis of Threat Modeling Output

For information about viewing analysis output from TMT, see “Analysis View".

# Features

For a walkthrough of TMT, see the *Threat Modeling Tool Getting Started Guide,* available in the installation folder of Microsoft Threat Modeling Tool 2014. That document will identify and explain the basic steps of creating a threat model.

## The Initial Screen

In Windows 7, from the Windows Start menu, select **Microsoft Threat Modeling Tool 2014.** In Windows 8, from the Windows Start screen, click the **Microsoft** **Threat Modeling Tool 2014** icon. The Initial screen will appear. From the initial screen, choose the **Create a Model** tile to create a new model. Click **Open a Model** to show the open file dialog so you can select a model to open. Click **Getting Started Guide** to see the*Threat Modeling Tool**Getting Started Guide*, which explains creating and analyzing a threat model.

**The Recently Opened Models** section will list the last 10 models opened with the tool. You can quickly select any of them to open and continue your work.

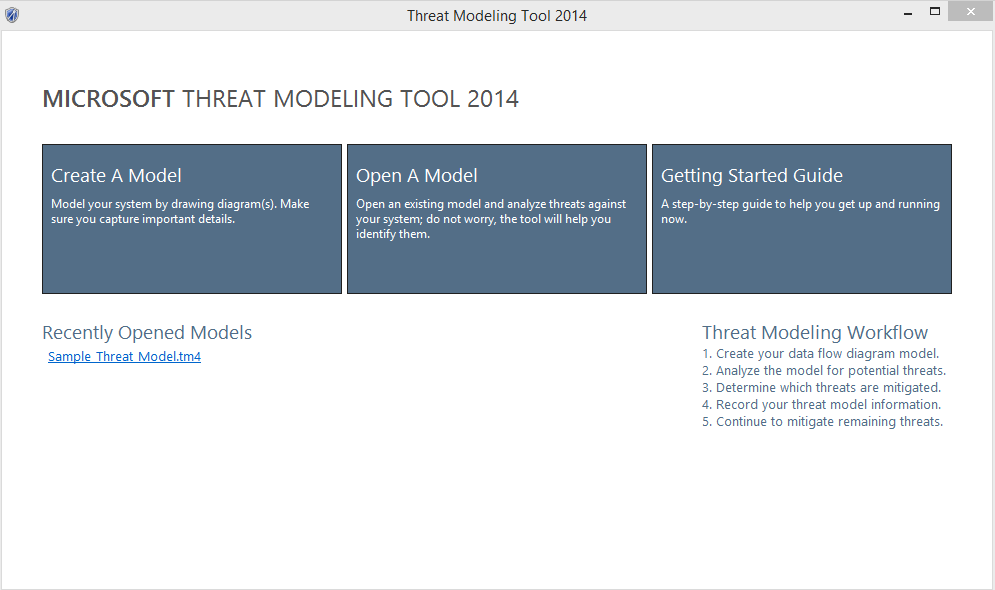


Figure Initial Threat Modeling Tool Screen

## Design View

**Design** view allows you to draw your diagram and provides objects and properties to allow you to adequately represent the design of your component.

All diagrams should minimally contain:

* One or more processes.
* The directional data flows between external interactors and processes, and among the processes themselves.
* Important data stores.
* An external interactor (often a user) that communicates with the processes.
* A trust boundary or boundaries

The example below shows a basic diagram:

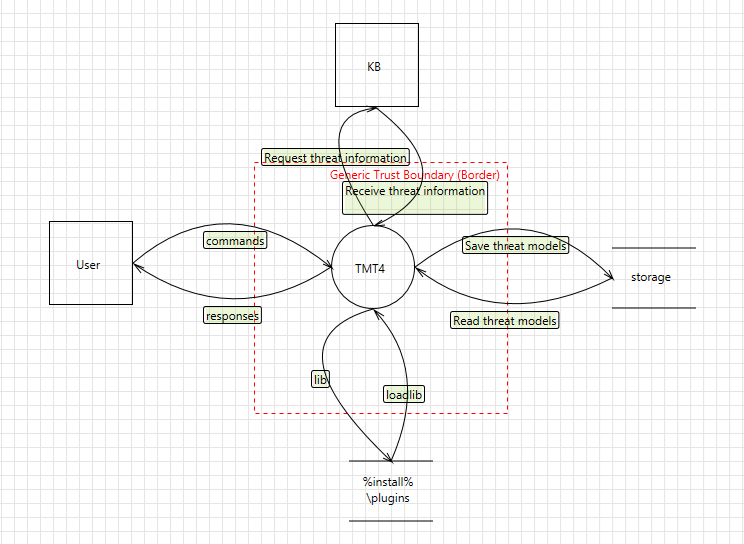


Figure Sample Diagram

To help you create a good diagram, the tool has certain heuristics that are based on a review of many threat models. These heuristics are intended to guide you in drawing the data flow diagram, and when violated, will show warnings or errors in the **Messages** pane.For example, if the data flow **Read threat models** were removed from the sample diagram, the tool would complain that the element **storage**, representing a data store, never provides data to anything outside the system.

***Self-check:*** *See if you can tell a story about someone using your product with the diagram. A good diagram will have the key elements you talk about.*

When first instantiated, elements will have names like **Generic Process.** The name should be replaced by a unique, descriptive name that uses a consistent pattern. It is very helpful to use the real technical names where possible. For example, use process names, such as **tmt4.exe**, **AnalysisOutput.xslt**, data store names, such as **HKLM\...\Currentversion\Userdata\** or **HKCU\Software\SDLTm\,** anddata flow names, such as **Read Configuration Data** or **Write Configuration Data**.

Use logical names like **lexical analysis**, **marshal data** when representing functional elements inside a process.

If your design is large or complex, you can represent it using multiple diagrams in the threat model file.

### The Drawing Canvas

The diagram is the basis of all threat information automatically generated by the tool. The recommended process is to begin with a simple diagram and add details to explain the system and show all the trust boundaries. If you use child diagrams, you can extend designs laterally into multiple sheets and expand high level elements into their internal component elements.

### Menu Choices

The **File** menu provides options to create, open, save, or close models:

* **New Model** creates a new model.
* **New from Template** creates a new model based on a threat model template (.tmt).
* **Open** opens an existing threat model.
* **Save** saves the current model using current name.
* **Save As** saves the current model with option to change name or location.
* **Save as Template** saves the current model as a threat model template (.tmt).
* **Threat Model Information** shows displays the **Threat** **Model Information** dialog. You should provide the background information and answer the scoping questions.
* **Close Model** closes the current model.
* **Exit** exits the tool.

The **Edit** menu provides options to interact with the clipboard:

* **Undo** undoes the last operation.
* **Redo** redoes the most recent operation.
* **Copy** copies the current selection into clipboard.
* **Paste** pastes the current clipboard contents onto drawing surface.
* **Cut** places the current selection into clipboard and removes from drawing surface.

The **View** menu provides options to view different functional windows within the tool:

* **Design View** switches to **Design** view.
* **Analysis View** switches to **Analysis** view.
* **Zoom In** increases magnification.
* **Zoom Out** decreases magnification.
* **Stencils** shows the drawing stencils in **Design** view. (Enabled only if currently hidden.)
* **Messages** showsthe **Message** window. (Enabled only if currently hidden.)
* **Notes** shows the **Notes** window**.** (Enabled only if currently hidden.)
* **Threat List Filter** shows the threat list filter in analysis view. (Enabled only if currently hidden.)
* **Threat Information** showsthe **Threat** **Information** window in **Analysis** view.
* **Properties** shows the **Properties** window. (Enabled only if currently hidden.)

The **Settings** menu exposes settings for the tool:

* **Enable Threat Generation** enables automatic threat generation. (ON by default.)
* **Disable Threat Generation** disables automatic threat generation. (Improves performance for large models.)

The **Diagram** menu provides options for switching between diagram windows. The menu options are generated dynamically based on your diagram names.

The **Reports** menu provides methods for creating HTML reports for the threat model.

* **Create Full Report** creates a threat model report with information on all threats.
* **Create Custom Report** creates a threat model report for a subset of threats based on state.

The **Help** menu displays options for user assistance.

### Toolbar

|  |  |
| --- | --- |
| **Open** opens explorer file open prompt | **Save** saves current open model file |
| **Design View** switches to **Design** view. | **Paste** pastes the clipboard contents onto surface. |
| **Analysis View** switches to **Analysis** view. | **Cut** cuts the current element from surface. |
| **New Diagram** creates a new blank diagram. | **Undo** undoes the last operation. |
| **Delete Diagram** deletes the current diagram | **Redo** redoes the most recent operation. |
| **Copy** copies the current element to the clipboard. | **Zoom in** increases magnification. |
|  | **Zoom out** decreases magnification. |

### Context (Right–Click) Menu

Right-click on the drawing canvas or an element, to choose from a set of actions will vary depending on the context and whether you are in Design view or Analysis view.

Actions available by right-clicking the drawing canvas:

* **Connect** connects the last two elements from the first to the second element.
* **Bi-directional Connect** creates a two-way connection between last two elements.
* **New Process** adds a new generic process.
* **New External Interactor** adds a new generic external interactor.
* **New Data Store** adds a new generic data store.
* **New Arc Boundary** adds a new generic arc boundary (legacy boundaries).
* **New Border Boundary** adds a new generic border boundary (preferred boundaries).
* **New Data Flow** adds a new generic (unconnected) data flow.
* **Add User-Defined Threat** adds a custom threat unassociated with any interaction.
* **Copy** copies the current selection to the clipboard.
* **Cut** places the current selection into clipboard and removes from drawing surface.
* **Paste** pastes an element onto drawing surface.
* **Add Annotation** adds a free-text annotation on the diagram.
* **Properties** shows the properties window.

Actions available by right-clicking an element:

* **Add User-Defined Threat** adds a custom threat. (Available on data-flows only.)
* **Delete** removes the element.
* **Copy** copies the current selection to the clipboard.
* **Cut** places the current selection into clipboard and removes from drawing surface.
* **Convert To** converts to or from generic element types and specific types.
* **Properties** shows the properties window.

### Elements

The **Stencils** pane displays a large set of icons and drawing tools that help you to intuitively create models that can be evaluated for security vulnerabilities before you begin coding. Using more specific elements allows for more precise threats to be generated.

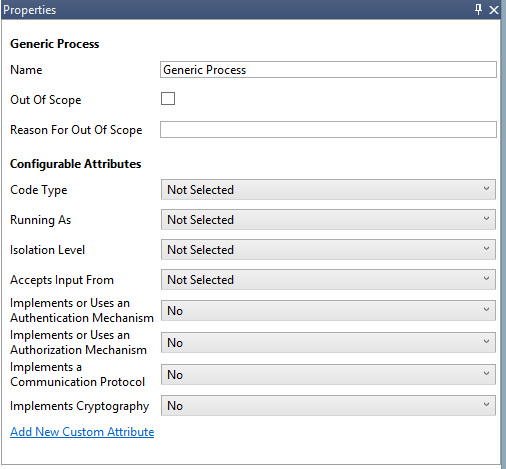
The **Stencils** pane displays five tabs: **Process**, **External**, **Store**, **Flow**, and **Boundary**. The elements available in each tab are listed in the following table.

| **Element Type** | **Name** | **Description** |
| --- | --- | --- |
| **Process** | Generic Process | A representation of a generic process. |
| **Process** | Applications Running on a non-Microsoft OS | Microsoft applications running on operating systems from Google or Apple. |
| **Process** | Browser and ActiveX Plug-ins | A representation of a browser plugin. |
| **Process** | Browser Client | A representation of a browser client. |
| **Process** | Kernel Thread | A thread of execution in the Windows kernel. |
| **Process** | Managed Application | A representation of a .NET application. |
| **Process** | Native Application | A representation of a Win32 or Win64 application. |
| **Process** | OS Process | A Windows process. |
| **Process** | Thick Client | A representation of a thick client. |
| **Process** | Thread | A thread of execution in a Windows process. |
| **Process** | Virtual Machine | A virtual machine running in a Hyper-V partition. |
| **Process** | Web Application | Delivers web content to a human user. |
| **Process** | Web Server | A representation of a Web Server Process. |
| **Process** | Web Service | Exposes a programmatic interface. |
| **Process** | Win32 Service | A representation of a network process or service. |
| **Process** | Windows Store Process | A representation of a Windows Store process. |
| **Store** | Generic Data Store | A representation of a data store. |
| **Store** | Cache | A representation of a local data cache. |
| **Store** | Cloud Storage | A representation of a cloud storage. |
| **Store** | Configuration File | A configuration file, such as XML, INI, and INF files. |
| **Store** | Cookies | A representation of cookie storage. |
| **Store** | Device | A representation of device local storage. |
| **Store** | File System | A representation of a file system. |
| **Store** | HTML5 Local Storage | A representation of HTML5 local storage. |
| **Store** | Non-Relational Database | A representation of a non-relational database. |
| **Store** | Registry Hive | A representation of the registry. |
| **Store** | SQL Database | A representation of a SQL database. |
| **Data Flow** | Generic Data Flow | A unidirectional representation of the flow of data between elements. |
| **Data Flow** | ALPC | Inter-process communication using an (Advanced) Local Procedure Call (ALPC) port. |
| **Data Flow** | Binary | A representation of a binary data flow. |
| **Data Flow** | HTTP | A representation of an HTTP data flow. |
| **Data Flow** | HTTPS | A representation of a HTTPS, TLS, or SSL data flow. |
| **Data Flow** | IOCTL Interface | An interface for an application to communicate to a device driver. |
| **Data Flow** | IPsec | A representation of an IPsec dataflow. |
| **Data Flow** | Named Pipe | A representation of a named pipe data flow. |
| **Data Flow** | RPC / DCOM | Remote Procedure Call (RPC) or Distributed COM (DCOM) data flow. |
| **Data Flow** | SMB | A representation of a Server Message Block (SMB) 1.0 or SMB 2.0 data flow. |
| **Data Flow** | UDP | User Data Protocol transport. |
| **External Interactor** | External Interactor | A representation of an external interactor. |
| **External Interactor** | Authentication Provider | A representation of an external authorization provider. Examples include Microsoft ID and Facebook. |
| **External Interactor** | Browser | A representation of an external web browser. |
| **External Interactor** | Human User | A representation of a user. |
| **External Interactor** | Megaservice | A large service that has only one instance on the Internet, such as Outlook.com or Xbox Live. |
| **External Interactor** | Web Application | A representation of an external web application (such as a portal or front end) that delivers web content to a human user. |
| **External Interactor** | Web Service | A representation of an external web service that exposes a programmatic interface. |
| **External Interactor** | Windows .NET Runtime | Represents the point where an application calls into the .NET Framework. |
| **External Interactor** | Windows RT Runtime | Represents the point where an application calls into WinRT. |
| **External Interactor** | Windows Runtime | Represents the point where an application calls into an unmanaged runtime library such as the CRT. |
| **Trust Boundary** | Generic Trust Boundary (arc and border) | A border representation of a trust boundary. There is no functional difference between an arc boundary and a border boundary, use whichever one provides the most clarity for your diagram. |
| **Trust Boundary** | AppContainer Boundary | A border representation for a Window Store AppContainer boundary. |
| **Trust Boundary** | CorpNet Trust Boundary (border) | A border representation of a corporate network trust boundary. |
| **Trust Boundary** | Internet Boundary (arc) | An arc representation of an Internet trust boundary. |
| **Trust Boundary** | Internet Explorer Boundaries | Describes the types of trust boundaries implemented by Internet Explorer. |
| **Trust Boundary** | Machine Trust Boundary (arc) | An arc representation of a machine trust boundary. |
| **Trust Boundary** | Other Browsers’ Boundaries | Describes the types of trust boundaries implemented by Google Chrome and Mozilla Firefox. |
| **Trust Boundary** | Sandbox Trust Boundary Border | A border representation of a sandbox trust boundary. |
| **Trust Boundary** | User-mode/Kernel-mode Boundary | A border representation of user-mode/kernel-mode separation. |

Table Elements

### Element Properties

The specific properties vary by element type within the threat model. The only common property for every type in the model is **Name**, which identifies each element. All elements except **Boundary** also have **Out of Scope** property**,** which removes the interaction(s) and element from the threat generation matrix. Use the related **Reason For Out of Scope** property to record why it is excluded.

  
Figure Properties for Generic Process

Here are the additional element properties by element type:

#### Properties for Processes

| Element Type | **Attribute Name** | **Additional Attribute Values** | **Modifiable?** |
| --- | --- | --- | --- |
| Generic Process | **Code Type** | **Managed** | Yes |
| **Unmanaged** |
| **Running As** | **Kernel** | Yes |
| **System** |
| **Network Service** |
| **Local Service** |
| **Administrator** |
| **Standard User With Elevation** |
| **Standard User Without Elevation** |
| **Windows Store App** |
| **Isolation level** | **AppContainer** | Yes |
| **Low Integrity Level** |
| **Microsoft Office Isolated Conversion Environment (MOICE)** |
| **Sandbox** |
| **Accepts Input From** | **Any Remote User or Entity** | Yes |
| **Kernel, System, or Local Admin** |
| **Local or Network Service** |
| **Local Standard User With Elevation** |
| **Local Standard User Without Elevation** |
| **Windows Store Apps or App Container Processes** |
| **Nothing** |
| **Other** |
| **Implements or uses an Authentication Mechanism** | **No** | Yes |
| **Yes** |
| **Implements or uses an Authorization Mechanism** | **No** | Yes |
| **Yes** |
| **Implements a Communication Protocol** | **No** | Yes |
| **Yes** |
| **Implements Cryptography** | **No** | Yes |
| **Yes** |
| Applications Running on a non-Microsoft OS | **No additional properties.** | **[None]** | [Not Applicable] |
| Browser and ActiveX Plug-ins | **ActiveX** | **No** | Yes |
| **Yes** |
| **Browser Plug-in Object (BHO)** | **No** | Yes |
| **Yes** |
| Browser Client | **Code Type** | **Unmanaged** | No |
| Kernel Thread | **No additional properties.** | **[None]** | [Not Applicable] |
| Managed Application | **Code Type** | **Managed** | No |
| OS Process | **No additional properties.** | **[None]** | [Not Applicable] |
| Thick Client | **Code Type** | **Unmanaged** | This value cannot be changed |
| Thread | **No additional properties.** | **[None]** | [Not Applicable] |
| Virtual Machine | **No additional properties.** | **[None]** | [Not Applicable] |
| Web Server | **Code Type** | **Managed** | Yes |
| **Unmanaged** |
| **Implements Input Sanitizers From Clients** | **Yes** | Yes |
| **No** |
| **Implements Output Sanitizers To And From Storage Devices** | **Yes** | Yes |
| **No** |
| Web Application | **No additional properties.** | **[None]** | [Not Applicable] |
| Web Service | **No additional properties.** | **[None]** | [Not Applicable] |
| Win32 Service | **Code Type** | **Unmanaged** | Yes |
| **Managed** |
| Windows Store Process | **Code Type** | **Managed** | No |
| **Context** | **Local** | Yes |
| **Web** |
| **'Documents Library' capability** | **Yes** | Yes |
| **No** |
| **'Enterprise Authentication' capability** | **Yes** | Yes |
| **No** |
| **Internet (Client & Server)' capability** | **Yes** | Yes |
| **No** |
| **'Internet (Client)' capability** | **Yes** | Yes |
| **No** |
| **'Location' capability** | **Yes** | Yes |
| **No** |
| **'Microphone' capability** | **Yes** | Yes |
| **No** |
| **'Music Library' capability** | **Yes** | Yes |
| **No** |
| **'Pictures Library' capability** | **Yes** | Yes |
| **No** |
| **'Private Networks (Client & Server)' capability** | **Yes** | Yes |
| **No** |
| **'Proximity' capability** | **Yes** | Yes |
| **No** |
| **'Removable Storage' capability** | **Yes** | Yes |
| **No** |
| **'Shared User Certificates' capability** | **Yes** | Yes |
| **No** |
| **'Text Messaging' capability** | **Yes** | Yes |
| **No** |
| **'Videos Library' capability** | **Yes** | Yes |
| **No** |
| **'Webcam' capability** | **Yes** | Yes |
| **No** |

Table Element Properties for Processes

#### Properties for Data Storage

| Element Name | **Attribute Name** | **Additional Attribute Values** | **Modifiable?** |
| --- | --- | --- | --- |
| Generic Data Store | **Stores Credentials** | **No** | Yes |
| **Yes** |
| **Stores Log Data** | **No** | Yes |
| **Yes** |
| **Encrypted** | **No** | Yes |
| **Yes** |
| **Signed** | **No** | Yes |
| **Yes** |
| **Write Access** | **Yes** | Yes |
| **No** |
| **Removable Storage** | **Yes** | Yes |
| **No** |
| **Backup** | **Yes** | Yes |
| **No** |
| **Shared** | **Yes** | Yes |
| **No** |
| Cookies | **HTTP Only** | **Yes** | Yes |
| **No** |
| Devices | **GPS** | **Yes** | Yes |
| **No** |
| **Contacts** | **Yes** | Yes |
| No |
| **Calendar Events** | **Yes** | Yes |
| **No** |
| **SMS messages** | **Yes** | Yes |
| **No** |
| **Cached Credentials** | **Yes** | Yes |
| **No** |
| **Enterprise Data** | **Yes** | Yes |
| **No** |
| **Messaging Data (Mail, IM, SMS…)** | **Yes** | Yes |
| **No** |
| **SIM Storage** | **Yes** | Yes |
| **No** |
| **Other Data** | **Yes** | Yes |
| **No** |
| File System | **File System Type** | **NTFS** | Yes |
| **ExFAT** |
| **FAT** |
| **ReFS** |
| **IFS** |
| **UDF** |
| **Other** |

Table Properties for Storage

#### Properties for Data Flow

| Element Name | **Attribute Name** | **Additional Attribute Values** | **Modifiable?** |
| --- | --- | --- | --- |
| Generic Data Flow | **Physical Network** | **Wire** | Yes |
| **Wi-Fi** |
| **Bluetooth** |
| **2G - 4G** |
| **Source Authenticated** | **No** | Yes |
| **Yes** |
| **Destination Authenticated** | **No** | Yes |
| **Yes** |
| **Provides Confidentiality** | **No** | Yes |
| **Yes** |
| **Provides Integrity** | **No** | Yes |
| **Yes** |
| **XML Encoded** | **No** | Yes |
| **Yes** |
| ALPC | **No additional properties.** | **[None]** | [Not Applicable] |
| Binary | **No additional properties.** | **[None]** | [Not Applicable] |
| HTTP | **No additional properties.** | **[None]** | [Not Applicable] |
| HTTPS | **No additional properties.** | **[None]** | [Not Applicable] |
| IOCTL Interface | **No additional properties.** | **[None]** | [Not Applicable] |
| IPsec | **No additional properties.** | **[None]** | [Not Applicable] |
| Named Pipe | **No additional properties.** | **[None]** | [Not Applicable] |
| RPC / DCOM | **No additional properties.** | **[None]** | [Not Applicable] |
| SMB | **No additional properties.** | **[None]** | [Not Applicable] |
| UDP | **No additional properties.** | **[None]** | [Not Applicable] |

Table Properties for Data Flow

#### Properties for External Interactors

| Element Name | **Attribute Name** | **Additional Attribute Values** | **Modifiable?** |
| --- | --- | --- | --- |
| External Interactor | **Authenticates Itself** | **No** | Yes |
| **Yes** |
| **Type** | **Code** | Yes |
| **Human** |
| Authentication Provider | **Microsoft** | **No** | Yes |
| **Yes** |
| Browser | **Type** | **Code** | No |
| Human User | **Type** | **Human** | No |
| Megaservice | **No additional properties.** | **[None]** | [Not Applicable] |
| Web Application | **Type** | **Code** | No |
| **Microsoft** | **No** | Yes |
| **Yes** |
| Web Service | **Type** | **Code** | No |
| **Microsoft** | **No** | Yes |
| **Yes** |
| Windows .NET Runtime | **Type** | **Code** | No |
| Windows RT Runtime | **Type** | **Code** | No |
| Windows Runtime | **Type** | **Code** | No |

Table Properties for External Interactor

#### Properties for Trust Boundaries

| Element Name | **Attribute Name** | **Additional Attribute Values** | **Modifiable?** |
| --- | --- | --- | --- |
| Generic Trust Boundary (arc and border) | **No additional properties.** | **[None]** | [Not Applicable] |
| AppContainer Boundary | **Boundary Type** | **AppContainer** | No |
| Corpnet Trust Boundary (Border) | **Boundary Type** | **Corporate Network** | No |
| Internet Boundary (arc) | **Boundary Type** | **Internet** | No |
| Internet Explorer Boundaries | **Boundary Type** | **Internet Explorer Boundary** | No |
| **Low Integrity Level Sandbox** | **Yes** | Yes |
| **No** |
| **App Container Sandbox** | **Yes** | Yes |
| **No** |
| **JavaScript Sandbox** | **Yes** | Yes |
| **No** |
| **Flash Sandbox** | **Yes** | Yes |
| **No** |
| Machine Trust Boundary (Arc) | **Boundary Type** | **Machine Boundary** | No |
| Other Browser’s' Boundaries | **Boundary Type** | **Other Browser** | No |
| **Chrome JavaScript Sandbox** | **Yes** | Yes |
| **No** |
| **Chrome Sandbox** | **Yes** | Yes |
| **No** |
| **Firefox JavaScript Sandbox** | **Yes** | Yes |
| **No** |
| Sandbox Trust Boundary Border | **Boundary Type** | **Sandbox Boundary** | No |
| User-mode/Kernel-mode Boundary | **Boundary Type** | **Kernel** | No |

Table Properties for Trust Boundary

In addition to the above built-in properties, additional properties can be added through changes to the Knowledge Base. For instructions on extending the Knowledge Base, please see “Appendix II — Extending the Threat Knowledge Base”**.**

### Threat Model Information

The **Threat** **Model Information** dialog contains basic information about the threat model and asks a series of security questions to help establish the risk of the component. You can select this dialog from the **File** menu.

### Messages

The **Messages** window allows the tool to identify any errors, warnings or inconsistencies in the drawing or the Knowledge Base.

### Notes

The **Notes** window provides a place to record notes and comments during the threat model discussion. These are included in the report, but not used for threat generation or analysis.

## Analysis View

The **Analysis** view allows you to analyze the threats generated for your diagram, identify which threats are not applicable, require investigation, require mitigation, or have been mitigated and verified. For models that have multiple diagrams, the threat list displayed is global and includes threat entries for all diagrams.

### Threat Information

After a model is drawn, you will be presented with a list of threats. You’ll find the list of threats organized in a grid that shows for each threat:

* Threat Title
* Threat (STRIDE) Category
* Threat State
* Threat Priority

Each threat will have a **Description** field**,** which will have content for every auto-generated threat and a **Justification** field in which mitigation information can be entered by the user.

For newly generated threat models, the setting for auto-generation threat mode is enabled by default. For migrated threat models created with Threat Modeling Tool 3.1.8, the auto-generation threat mode is set to off. To turn it on go to **Settings** and select **Enable Threat Generation**. Each threat will have options that enable you to manage the identified threats. By default, the state of all newly generated threats is **Not Started**.

|  |  |
| --- | --- |
| Default state for newly generated threat    Mitigation implemented and verified | Mark threat as needs mitigation    Mark threat as not applicable |

Threats are generated using STRIDE per interaction. An interaction is defined by two elements connected by a data flow, and may include a boundary. If an element is marked **Out of Scope** threats will still be auto-generated for that interaction but the element itself will have visual feedback that is marked **Out of Scope**. You can also add a user-defined or custom threat by right-clicking on the desired data flow in the interaction and selecting **Add User-defined Threat**. When you do so you’ll find your custom threat at the end of the existing threat list.   
  
Threat priority is by default set to **High.** As applicable, it can be changed to **Medium** or **Low**.   
  
There is a basic **Search** functionality available for the **Threat Information** area only in **Analysis** view. The number of threats displayed and total number of threats is listed in the **Search** field and they will dynamically adjust based on results for the search criteria entered.

### Threat List Filter

The **Threat List** **Filter** window allows you to filter threats on the current diagram based on their state, category, or interaction.

To filter the threats by threat state, click the **By Threat State** tab in the **Threat List** **Filter** window and select the desired state or states. The threats in the **Threat Information** window will then be limited to only threats in the selected state. To reset the view, click **Threat States**.

To filter the threats for a category, click the **By Category** tab in the **Threat List** **Filter** window and select the desired category or categories. The threats in the **Threat Information** window will then be limited to only threats of that category. To reset the view, click **All Categories**.

To filter the threats for a particular interaction or diagram, you can either click the data flow or flows you are interested in or click the **By Diagram/Interaction** tab in the **Threat List** **Filter** window and select the desired data flow. The threats in the **Threat Information** window will then be limited to only threats for that interaction. To reset the view, click **All Diagrams**.

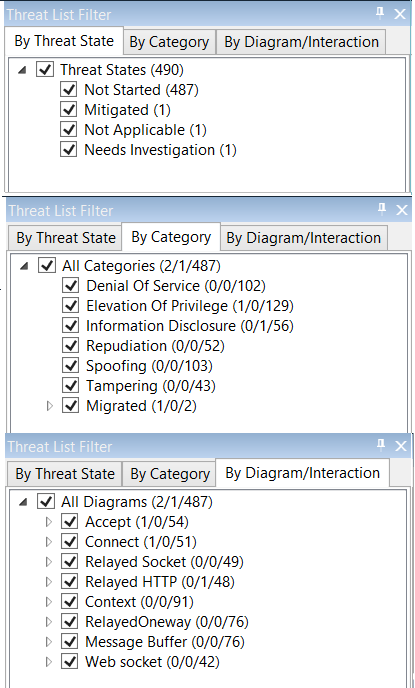


Figure Using Threat List Filters

**By Threat State** threats are listed in four groups: **Not Started**, **Mitigated**, **Not Applicable**, and **Needs Investigation**.

**By Category** threats are listed starting with user-defined threats and then in alphabetical order for each STRIDE category.   
**By Diagram/Interaction** threats show the threats’ completion state in **n/n/n** format where (Threats Mitigated or Not applicable #/Threat Needing Investigation #/Threats Not Started #).

# 

# Troubleshooting

Please see the links listed below in “Support”.

# Automation

Microsoft Threat Modeling Tool 2014 is not scriptable.

# Support

For support, please visit the following links:

* [Microsoft Security Development Lifecycle](http://www.microsoft.com/security/sdl/default.aspx)
* [Microsoft Trustworthy Computing Blog](http://blogs.technet.com/b/trustworthycomputing)
* [MSDN Forums for SDL](http://social.msdn.microsoft.com/Forums/en-US/home?forum=sdlprocess)

# Appendices

## Appendix I — Creating Bugs for Tracking Systems

To create a bug from **Analysis** view:

1. Select a threat to create a bug for.
2. Right-click the threat and select **Copy threat(s)**.

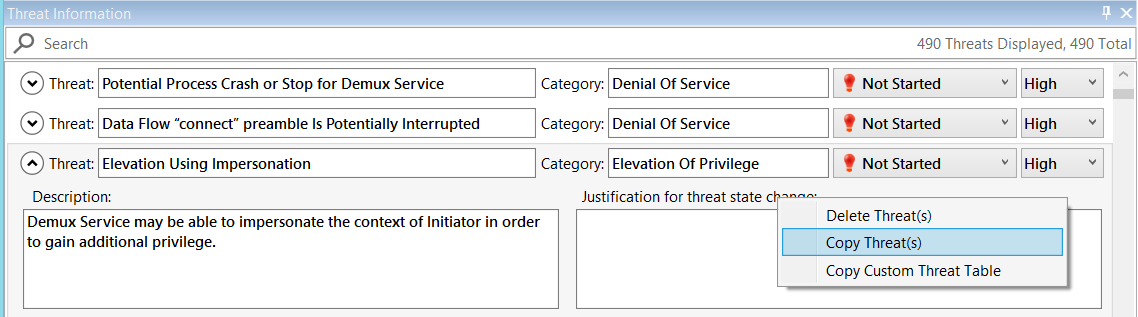


Figure Copying a Threat

1. Your threat information is copied to the clipboard in the following format:

* THREAT: Data Flow Generic Data Flow1 Is Potentially Interrupted
* CATEGORY: Denial Of Service
* DIAGRAM: Diagram1
* INTERACTION: Generic Data Flow1
* PRIORITY: <none provided>
* STATE: Not Started
* Last updated by User at m/d/yyyy hh:mm:ss AM/PM
* DESCRIPTION: An external threat agent interrupts data flowing across a trust boundary in either direction.
* JUSTIFICATION: Provide mitigation for DoS attack.

1. You can now paste the copied information in a bug tracking system of your choice.

**NOTE**: You can select all threats in your list to be copied to the clipboard by pressing CTRL+A then and right-clicking **Copy Threat(s).**

Select **Copy Custom Threat Table** to use the clipboard content to paste into Microsoft Excel and then bulk-import into a bug tracking system of your choice. You can do so for a single threat or all of them by selecting all entries using CTRL+A.

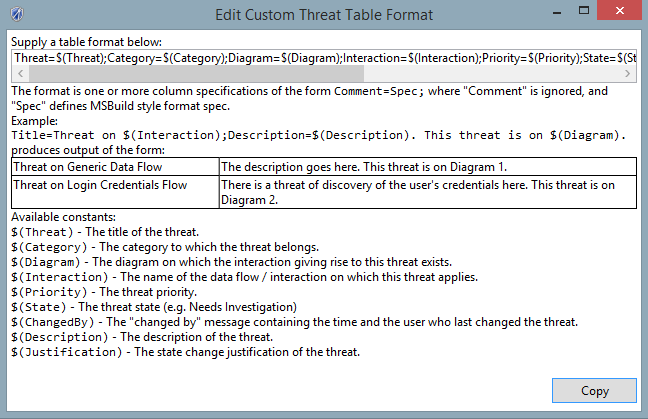


Figure Edit Custom Threat Table Format

## Appendix II — Extending the Threat Knowledge Base

Microsoft Threat Modeling Tool 2014 allows customization of the Threat Knowledge Base. The Threat Knowledge Base specifies the set of elements, attributes, and threat definitions used by the Threat Modeling Tool. Customization is an advanced feature and should be done with care and in consultation with the SDL team.

The TMT installation directory a contains standard Threat Knowledge Base (Threat KB) called **KnowledgeBase** which contains all KB XML files and a copy of the Threat KB files from the TMT, which is used for backwards compatibility. There are two ways to customize the Threat KB:

* You can extend the SDL Knowledge Base by adding or removing elements, attributes, and threat definition files.
* You can define a new Threat KB by specifying your own set of elements, attributes, and threat definitions.

To extend the Threat KB, create your extension and place it in the **%LocalAppData%\TMT4\KnowledgeBaseExtensions** directory. Detailed instructions for extending the Threat KB are below.

To define a new Threat KB for your group you can replace **<installation directory>\KnowledgeBase** with your own XML files. Instructions are very similar to extending the Threat KB and exceptions are noted inline below.

When extending a Threat Knowledge Base, start with a small Threat KB extension, create a threat model using that Threat KB extension, extend the Threat KB some more, extend the threat model, and iterate until you are finished. Since the Threat KB is saved with a threat model there is no way to upgrade a threat model to a later version of the KB. Instead, create a new threat model using your updated KB, and then copy all of the elements from your prior threat model into the new threat model. Iterate this process until your Threat KB is finished.

### Contents of a Threat Knowledge Base

A Threat Knowledge Base contains five types of XML files:

* A **manifest** file that describes the collection of files in the Threat KB.
* An **element** file that specifies the elements and attributes to be added or removed from the collection of Threat KBs. The element file can contain either: (1) base elements (also known as generic elements), which are elements without parents, that are to be added, removed, or modified; or (2) standard elements, which are elements inherited from other standard elements or from the generic elements. Elements appear in the list of stencils that can be added to your diagram (Process, External, Store, Flow, or Boundary). (**GenericElements** and **StandardElements** in the manifest file.)
* A **threat category** file, which lists the threat categories that appear in the Threat List and can be used to filter the collection of potential threats. (**ThreatCategories** in the manifest file.)
* A **threat definition** file, which describes additional potential threats that are evaluated as part of automatic threat generation and displayed in the Threat List and threat model reports. (**ThreatTypes** in the manifest file.)

The Threat KB must have one manifest file and otherwise can contain one or more of any other file type.

### Customizing a Threat KB

The remainder of this section describes how to customize a Threat KB.

In the manifest file, there is a unique manifest name, author name, version, and a GUID identifier that are attributes to the **<Manifest>** element.

For the **<id>** attribute, if you are extending the base SDL KB included with the tool, use the same identifier as the SDL KB manifest, **CC62EBAE-3748-431E-B1DF-F4220DC9003F**. If you are extending another KB, include the value of the other Knowledge Base’s ID. If you are creating a completely new Threat KB, then use a new GUID.

In the **<kbfiles>** element, for each **<file>** element specify the type of file and file name that will be included in the Threat KB directory location.

As an example, here is the manifest file from TMT 2014. In your own manifest only include the file types that you used for your Threat KB. If you did not use a file type (for example, you didn’t add or change any threat categories) then omit that line. You can also modify the **ScopingQuestions** file.

<?xml version="1.0" encoding="utf-8" ?>

<Manifest name="SDL TM Knowledge Base (Core)" author="TwC MSEC" version="4.0.2.1" id="CC62EBAE-3748-431E-B1DF-F4220DC9003F">  
 <kbfiles>

<file type="GenericElements" name="GenericElementCollection.xml"/>

<file type="StandardElements" name="StandardElementCollection.xml"/>

<file type="ThreatCategories" name="ThreatCategories.xml"/>

<file type="ThreatTypes" name="ThreatTypes.xml"/>

</kbfiles>

</Manifest>

Note that XML is case-sensitive, but the values of the **<ID>** and **<Name>** elements are not. The element file specifies an element collection that will be added or removed from the Threat KB. The format for generic collection and standard collection element files is the same except that **GenericElements** do not include a **ParentElement**.

Any number of **<ElementType>** elements may be defined. For new element types, all values must be specified. For modified elements, only the necessary values are specified. It is not possible to remove elements although it is possible to hide them by modifying the value of the **<Hidden>** node. If you must remove elements then you will need to create a new Threat KB without those elements.

Here is the structure of an element collection:

<ArrayOfElementType>

<ElementType>

<Name/>

<ID/>

<Description/>

<Hidden/>

<ParentElement/>

<Representation/>

<Image/>

<Attributes>

<Attribute>

<DisplayName/>

<Name/>

<Type/>

<Mode/>

<Inheritance>Virtual</Inheritance>

<AttributeValues>

<Value/>

</AttributeValues>

</Attribute>

</Attributes>

</ElementType>

</ArrayOfElementType>

The value for the **<Name>** attribute will be the name of the custom element that appears on the **Stencil** pane of the drawing surface.

The value for the **<ID>** attribute should begin with the prefix of **GE.** for generic elements or **SE.** for standard elements. Next is **P.**, **DF.**, **DS.**, **EI.**, or **TB.** if the element is, respectively, a type of process, data flow, data store, external interactor, or trust boundary. The next part of the identifier should be the name of the technology or team. For example, the extended elements that are part of the SDL Threat KB include **TMCore** as part of their <**ID>** attribute. <**ID>** attributes are not case-sensitive so just be consistent in your casing to improve readability

The value for the **<Description>** attribute should be a short description suitable for a tool tip.

The value for the **<Hidden>** attribute should be set to false to display the element or true to hide the element. The value for the **<ParentElement>** attribute for a standard element should be the identifier of the element that this element is derived from; typically this will be one of **GE.P**, **GE.DS**, **GE.DF**, **GE.EI**, or **GE.TB.L GE.TB.B** if the custom element is inherited directly from, a type of process, data flow, data store, external interactor, or trust boundary (arc or border). If your element is based on a custom or extended element then use the value of the **<ID>** element from the other element as the value of the **<ParentElement>** attribute.

The value for the **<Representation>** attribute for generic elements should use the values found in GenericElementCollection.xml. For standard elements it should always be set to **Inherited**.

The **<Images>** attribute points to .png file located in TMT installation directory, such as **/Images/ImageHumanUser7.PNG**. If you must use your own image, a hard-coded full path can be used. Environment variables and relative path are not currently supported.

When specifying attributes for an element, the **<DisplayName>** attribute will be the text that appears in the **Properties** pane, and the **<Name>** attribute is used as part of threat rule evaluation. The value of **<Name>** is not case-sensitive, that is, an attribute named **XMLenc** will match **xmlenc** when included in a threat generation include or exclude clause. The value of **<Type>** attribute should be **list**. The value of the **<Inheritance>** element should be **Virtual**. If you want users to be able to select a value for an attribute, then the value for **<Mode>** should be **Dynamic**. Otherwise it must be **Static**. The **<AttributeValues>** element specifies the list of attribute values that will appear in the **Properties** pane. The first value is the default value. Use **Not Selected** as the first value if you want to make a value optional.

To modify an element that was previously defined in the base KB, include **extype="append"** as an XML attribute in the **<ElementType>** that modifies the element specified by **<ID>**. You can modify the **<Hidden>** value or the attributes of the element. To modify the attributes, include **extype="remove"**, **extype="new"**, or **extype="replace"** as an XML attribute in the **<Attribute>** node. For new or replace, specify the complete attribute definition. For remove, only specify the attribute name.

For example, the following XML will remove the **XMLenc** attribute from the generic data flow.

<ElementType extype="append">

<ID>GE.DF</ID>

<Attributes>

<Attribute extype="remove">

<Name>XMLenc</Name>

</Attribute>

</Attributes>

</ElementType>

Modifying or removing an attribute may cause consistency problems if a threat generation rule has an **Include** or **Exclude** clause that references the attribute. You can search for the attribute name in the Threat KB to check if it is referenced.

The threat categories file specifies threat categories to be added, removed, or replaced. The structure of a threat category file is:

<ArrayOfThreatCategory>

<ThreatCategory>

<Name/>

<Id/>

<ShortDescription/>

<LongDescription/>

</ThreatCategory>

</ArrayOfThreatCategory>

Any number of **<ThreatCategory>** can be specified. **<Name/>** is the name of the threat category displayed in the Threat List and Threat Information. **<Id/>** is the case-insensitive ID of the threat category referenced by threats, which is described further below. The **<ShortDescription/>** is included in the threat model report. **<LongDescription/>** is not currently used.

To add new threat categories, specify a new **<Id>**. To remove a threat category, add the XML attribute **extype=”remove”** to the **<ThreatCategory>** node, and only specify the **<Id>** to be removed. If you attempt to remove a threat category which threat definitions refer to, then TMT will fail to open and will display the threat definitions which refer to the missing category. To replace a threat category, specify the **<Id>** to remove and add the XML attribute **extype=”remove”** to the **<ThreatCategory>** node.

The **threat definition** file specifies additional threats that are included when TMT automatically generates threat suggestions.

The structure of a threat definition file is:

<ArrayOfThreatTypes>

<ThreatType/>

<Id/>

<ShortTitle/>

<Description/>

<Category/>

<GenerationFilters>

<Include/>

<Exclude/>

</GenerationFilters>

<ThreatType>

<ArrayOfThreatTypes>

Any number of **<ThreatType>** can be specified. The value for the **<Id>** attribute should begin with the prefix **S.**, **T.**, **R.**, **I.**, **D.**, **E.** or a custom threat category. The next part of the identifier should be the name of the technology or team followed by a numeric identifier. For example, the first repudiation threat defined by a team would begin with **R.TeamName.1**. You can also define new categories. In that case use your own prefix and otherwise follow the rules above.

The value of the **<ShortTitle>** element is the name of the threat rule and appears in the **Threat Information** pane.

The value of the **<Description>** element is text that appears in the **Threat Information** field for a threat on the Information Pane.

The value of the **<Category>** element is one of **S.**, **T.**, **R.**, **I.**, **D.**, **E.** values are defined by the ThreatCategories.xml document in the SDL Threat KB, or a category specified in a custom threat category file. Select the category that most closely aligns with the type of threat you are describing.

The values for the **<Include>** and **<Exclude>** elements specify the circumstances in which TMT will automatically suggest a potential threat. If **<Include>** evaluates to true then **<Exclude>** is evaluated if it is present. If **<Exclude>** evaluates to true then the threat is not suggested as a potential threat. The grammar in Backus-Naur Form (BNF) for these elements is:

<rule> ::= <expression> { <op> <expression> }

<expression> ::= <object>[.<attribute>] IS <value> | Flow crosses <entity\_id> | [ NOT ] ( <expression> )

<object> ::= Source | Target | Flow

<attribute> ::= <alpha\_numeric>

<value> ::= <entity\_id> | <attr\_value>

<attr\_value> ::= 'Yes' | 'No' | <literal>

<entity\_id> ::= 'GE.P' | 'GE.TB' | <literal>

<op> ::= AND | OR  
<literal> ::= ' <text> '

Where **Source** is the source entity, **Target** is the destination entity and **Flow** is the data flow in a STRIDE entity/entity/data flow interaction. ‘Entity ID’ is the value of the **<ID>** attribute for an entity. Standard entities, which are derived from generic entities, will inherit rule evaluation from their parent; for example, a rule defined for a generic process (**GE.P**) will also apply to a Windows user-mode thread (**SE.P.TMCore.Thread**). If a rule refers to an entity ID that does not exist in the KB then **IS** expressions referencing that entity ID will always evaluate to false, e.g., **Source is ‘nonexistentID’** will always be false and **NOT Source is ‘nonexistentID’** will always be true.

The **Source**, **Target**, and **Flow** variables also expose the values of attributes. For example, the **Source.Name** parameter contains the value of the **<Name>** entity element and the value of **Flow.authenticationDestination** indicates whether or not the end-point of a data flow is authenticated. Such a rule would be expressed as **Flow.authenticationDestination** **is** '***Yes***'. If a rule refers to an attribute that does not exist in the KB then **IS** expressions referencing that attribute will always evaluate to false, e.g., **Source.nonexistentAttribute is ‘Yes’** will always be false and **NOT Source.nonexistentAttribute is ‘Yes’** will always be true.

Expressions can be combined using the **and** and **or** operators. Groups of expressions can be combined and nested within parentheses TMT evaluates expressions using case-insensitive comparisons.

As an example, here are sample rule definitions that identify a potential risk for cross-site scripting and risk of untrusted input data:

<ThreatType>

<Id>T13.1</Id>

<ShortTitle>Cross Site Scripting</ShortTitle>

<Category>T</Category>

<Description>The web server {target.Name} could be a subject to a cross-site scripting attack because it does not implement client input sanitizers.</Description>

<GenerationFilters>

<!-- 2/19/2013 changed 'SE.DF.WebServer' to SE.DF.TMCore.WebServer'-->

<Include>target is 'SE.P.TMCore.WebServer'</Include>

<Exclude>target.hasInputSanitizers is 'Yes'</Exclude>

</GenerationFilters>

</ThreatType>

<ThreatType>

<Id>T1</Id>

<ShortTitle>Potential Lack of Input Validation for {target.Name}</ShortTitle>

<Category>T</Category>

<Description>Data flowing across {flow.Name} may be tampered by an attacker. This may lead to a denial of service attack against {target.Name} or an elevation of privilege attack against {target.Name} or an information disclosure by {target.Name}. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an “approved list” input validation approach.</Description>

<GenerationFilters>

<Include>(source is 'GE.P' or source is 'GE.EI') and target is 'GE.P' and (flow crosses 'GE.TB')</Include>

<Exclude></Exclude>

</GenerationFilters>

</ThreatType>

To add new threat types, use the format above with a new **<Id>**. To remove a threat type, add the XML attribute **extype=”remove”** to the **<ThreatType>** element, and only specify the **<Id>**. To replace a threat type, use the format above with an existing **<Id>** and add the XML attribute **extype=”append”** to the **<ThreatType>** element.

## Appendix III — Drawing Surface Keyboard Navigation and General Keyboard Shortcuts

The Microsoft Threat Modeling Tool 2014 provides the ability to navigate throughout the tool and the drawing surface by using the keyboard. Keyboard shortcuts provide an accessibility option to those who are impaired, as well as anyone who wants to save time by combining key commands with mouse control.   
Since the windows and panes in Threat Modeling Tool are organized into focus scopes, the drawing surface keeps track of the currently focused element. When keyboard focus leaves a focus scope, the focused element will lose keyboard focus but will retain logical focus. When keyboard focus returns to the focus scope, the focused element will obtain keyboard focus. This allows for keyboard focus to be changed between multiple focus scopes but ensures that the focused element in the focus scope regains keyboard focus when focus returns to the focus scope.

|  |  |
| --- | --- |
| **To do this** | **Press** |
| Move from element to element on the drawing surface. A dotted rectangle indicates the shape that has the focus. The focus is moving in the order the elements were created. No change to the selection state of elements. | TAB |
| Move from element to element on the drawing surface in reverse order. | SHIFT+TAB |
| Select a currently focused element.  **NOTE**: If the focused element is already selected it retains selection. Any other previously selected elements are unselected. | ENTER |
| To select multiple elements, press the TAB key to bring focus to the first element you want to select, and then press ENTER. Press the TAB key to bring focus to another element. When the focus rectangle is over the element you want, press SHIFT+ENTER to add that shape to the selection. Repeat for each element you want to select.  NOTE: Selected element is removed from the selection group if there is more than one element in the group, otherwise the last selected element is kept selected. Focus is preserved on the same element. | SHIFT+ENTER |
| Select all elements on a diagram. | CTRL+A |
| Clear selection of or focus on an element or group. | ESC |

Figure Focus Navigation and Element Selection

| **To do this** | **Press** |
| --- | --- |
| Move a selected element or group of elements. | Arrow keys |
| Move a selection group 1 pixel at a time.  **NOTE**: SCROLL LOCK must be turned off. | SHIFT+Arrow keys |
| Delete selected element(s) | DEL |
| Copy/Cut/Paste  **NOTE**: Elements pasted onto a diagram should be selected by default. Previous selection group is cleared. | CTRL+C/X/V |
| Resize selected element(s). | ALT+Arrow keys |
| Switch focus between source anchor/middle point/target anchor of a selected line to allow movement of an individual point of the line. | CTRL+1/2/3 |
| Bring focus back to the selected line if in anchor manipulation mode | ESC |
| Connect/disconnect a selected dataflow anchor to/from a border anchor in proximity  **NOTE**: Focus moves immediately to another anchor of the dataflow | ENTER |

Figure Manipulating Selected Elements

|  |  |
| --- | --- |
| **To do this** | **Press** |
| Switch witch between diagrams. | CTRL+TAB |
| Scroll a diagram. | CTRL+Arrow Keys |
| Zoom in. | CTRL+PLUS |
| Zoom out. | СTRL+MINUS |
| Open file. | CTRL+O |
| Zoom in/Zoom out. | CTRL+Mouse wheel up/down |

Figure Other Actions

Copyright © 2014 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Some examples are for illustration only and are fictitious. No real association is intended or inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.