Microsoft Threat Modeling Tool 2014: Identify & Mitigate

By Russ McRee – ISSA Senior Member, Puget Sound (Seattle), USA Chapter

Prerequisites/dependencies

—Windows operating system

I've long been deeply invested in the performance of threat modeling with particular attention to doing so in operational environments rather than limiting the practice to simply software. I wrote the *IT Infrastructure Threat Modeling Guide*[1] for Microsoft in 2009 with the hope of stimulating this activity. In recent months two events have taken place that contribute significantly to the threat modeling community. In February Adam Shostack published his book, *Threat Modeling: Designing for Security*,[2] and I can say without hesitation that it is a gem. I was privileged to serve as the technical proof reader for this book and found that its direct applicability to threat modeling across the full spectrum of target opportunities is inherent throughout. I strongly recommend you add this book to your library as it is, in and of itself, a tool for threat modelers and those who wish to reduce risk, apply mitigations, and improve security posture. This was followed in mid-April by the release of the Microsoft Threat Modeling Tool 2014.[3] The tool had become a bit stale, and the 2014 release is a refreshing update that includes a number of feature improvements that we'll discuss shortly. We'll also use the tool to conduct a threat model that envisions the *ISSA Journal's* focus for the month of May: Healthcare Threats and Controls.

First, I sought out Adam to provide us with insight regarding his perspective on operational threat modeling. As expected, he indicated that whether you're a system administrator, system architect, site reliability engineer, or IT professional, threat modeling is important and applicable to your job. Adam often asks four related questions:

1. What are you building?

He describes that building an operational system is more likely to be building additional components on top of an existing system, and that it's therefore important to model both what you have and how it's changing.

2. What can go wrong?

Adam reminds us that you can use any of the threat enumeration techniques, but that, in particular, STRIDE[4] relates closely to the "CIA" set of properties that are desirable for an operational system. I'll add OWASP Risk Rating Methodology to the tool's KB for good measure, given its direct integration of CIA.

3. What are you going to do about it?

Several frameworks can be used here, such as prevent, detect, and respond as well as available technologies.

4. Did you do a good job at 1-3?

Adam points out that assurance activities (which can include compliance) can help you. More importantly, you can also use approaches such as penetration testing and red teaming to help you determine if you did a good job. I am a strong proponent of this approach. My team at Microsoft includes both threat engineers for threat modeling and assessment as well as penetration testers for discovery and validation of mitigations.

To supplement the commitment to operational threat modeling, I asked Steve Lipner,[5] one of the founding fathers of Microsoft's Security Development Lifecycle and the Security Response Center (MSRC), for his perspective, which he eloquently provided as follows:

> "While threat modeling originated as an approach to evaluating the security of software components, we have found the techniques of security threat modeling to have wide applicability. Like software components, operational services are targets of attack and can exhibit vulnerabilities. Threat modeling and STRIDE have proven to be effective for identifying and mitigating vulnerabilities in operational services as well as software products and components."

With clear alignment around the premise of operational threat modeling, let's take a look at what it means to apply it.

Identifying threats and mitigations with TMT 2014

Emil Karafezov, who is responsible for the threat modeling component of the Security Development Lifecycle (SDL) at

1 http://technet.microsoft.com/en-us/library/dd941826.aspx.

2 http://www.amazon.com/Threat-Modeling-Designing-Adam-Shostack/dp/1118809998.

3 http://blogs.msdn.com/b/sdl/archive/2014/04/15/introducing-microsoft-threat-modeling-tool-2014.aspx.

4 http://msdn.microsoft.com/en-us/magazine/cc163519.aspx.

5 http://www.infosecurity-magazine.com/view/25012/interview-microsofts-steve-lipner.

Microsoft, wrote a useful introduction[6] to the Microsoft Threat Modeling Tool 2014 (TMT). Emil let me know that there are additional details and pointers in the *Getting Started Guide* and the *User Guide* which are part of the Threat Modeling Tool 2014 Principles SDK.[7] You should definitely read the introduction as well as the guides before proceeding here as I will not be revisiting the basic usage information for the TMT tool or how to threat model (read the book) and will instead focus more in-depth on some key new capabilities. I will do so in the context of a threat model for the operational environment of a fictional medical services company called MEDSRV.

Figure 1 includes a view of the MEDSRV operational environment for its web application and databases implementation.

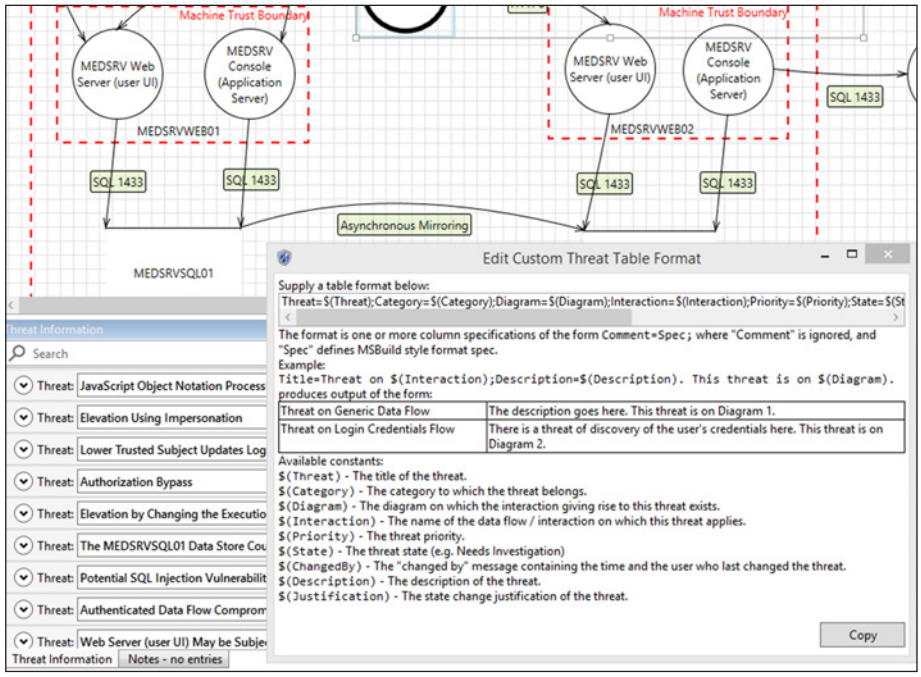

Figure 2: – TMT 2014's Copy Custom Threat Table feature

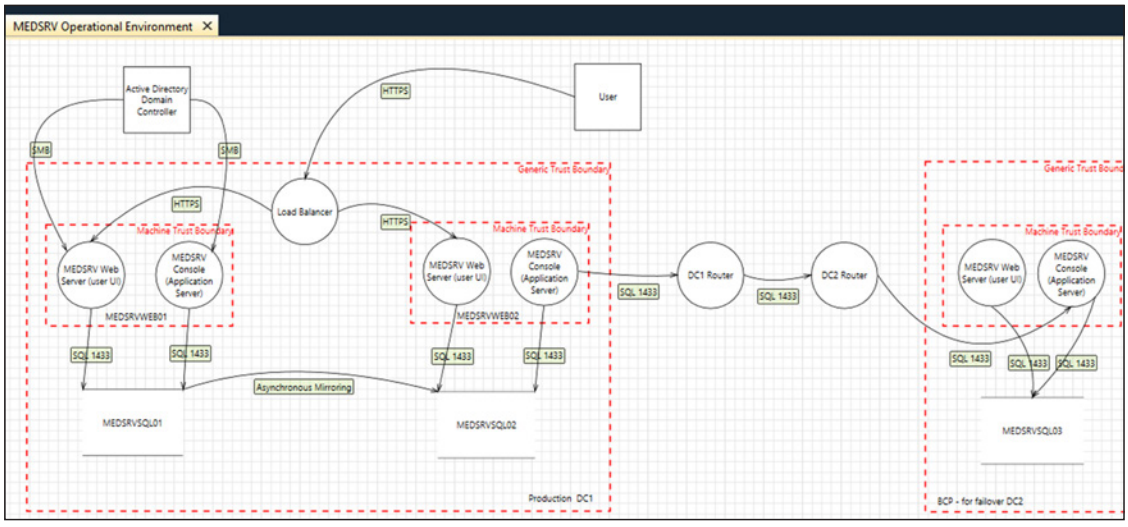

Figure 1 – A MEDSRV threat model with TMT 2014

Emil offered some additional pointers not shared in his blog post that we'll explore further with the MEDSRV threat model, specific to data extraction and search capabilities.

Data extraction

From a workflow perspective, the ability to extract information from the tool for record keeping or bug filing is quite useful. The previous version of the TMT included Product Studio and Visual Studio plugins for bug filing, but Emil describes them as rather rigid templates that were problematic for users syncing with their server. With TMT 2014 there is a simple right-click *Copy Threats* for each entry that can be pasted into any text editor or bug tracking system. For bulk threat entry manipulation there is another feature, *Copy Custom Threat Table*, which lets you dump results conveniently into Excel, which in turn can be imported into workflow management systems via automation. When in *Analysis View* with focus set in the *Threat Information* list, use the known Ctrl+A shortcut to select all threat entries; and with right-click you can edit the constants in the *Custom Threat Table* as seen in Figure 2.

Search for threat information

Emil also pointed out that TMT 2014's *Search for Threat Information* area, while seemingly a standard-to-have option, is new and worth mentioning. This feature is really important if you have a massive threat model with a plethora of threats; the threat list filter is not always the most efficient way to narrow down your criteria. I have found this to be absolute truth during threat modeling sessions of online services at Microsoft, where a large model may include hundreds or thousands of threats. To find threats that contained keywords specific to a particular implementation of your mitigations as an example, using *Search* is the way to go. You might be focusing on data store accessibility as seen in figure 3.

6 http://blogs.msdn.com/b/sdl/archive/2014/04/15/introducing-microsoft-threat-modeling-tool-2014.aspx.

7 http://aka.ms/By12as.

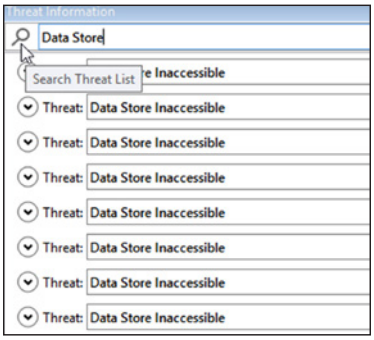

Figure 3 – Search for threat information

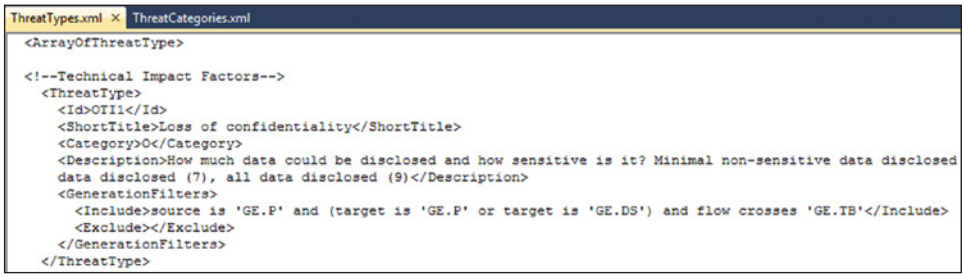

Figure 4 – Additions to ThreatTypes.xml

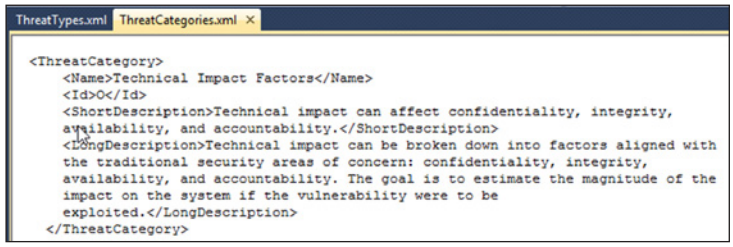

Figure 5 – Additions to ThreatCategories.xml

I also asked Ralph Hood, one of Microsoft Trustworthy Computing's group program manager for secure development policies and tools (the group that oversees the TMT), what stood out for him with this version of the tool. He offered two items in particular:

1. Migration capability of models from the old version of the tool
2. The ability to customize threats

Ralph indicated that the TMT tool has not historically supported any kind of migration to newer versions; the ability to migrate models from earlier versions to the 4.1 version is therefore a powerful feature for users who have already conducted numerous threat models with older versions. Threat models should always be considered dynamic (never static), as systems always change, and you'll likely update a model at a later date.

The ability to customize threats is also very important, particularly in the operations space. The ability to change the threat elements and information (mitigation suggestions, threat categories, etc.) for specific environments is of significant importance. Ralph points out as an example that if a specific service or product owner knows that certain threats are assessed differently because of specific characteristics of the service or platform, he can change the related threat information. Threat modelers can do so using a knowledge base (KB) created for all related models, so any user going forward can utilize the modified KB rather than having to always change threat attributes for each threat manually. According to Ralph, this is important functionality in the operations space where certain service dependencies and platform benefits and/or downfalls may consistently alter threat information. He's absolutely right, so I'll take the opportunity to tweak the imaginary MEDSRV KB here for your consideration, using Appendix II of the *User Guide* (read it). The KB is installed by default in `C:\Program Files (x86)\Microsoft Threat Modeling Tool 2014\KnowledgeBase`. Do not tweak the original; create a copy and modify that. I called my copy *KnowledgeBaseMEDSRV* and saved it in `C:\tmp`. I focused exclusively on *ThreatCategories.xml* and *ThreatTypes.xml*. Using the OWASP Risk Rating Methodology,[8] I added *Technical Impact Factors* to `ThreatCategories.xml` and `ThreatTypes.xml`. Direct from the OWASP site, "technical impact can be broken down into factors aligned with the traditional security areas of concern: confidentiality, integrity, availability, and accountability. The goal is to estimate the magnitude of the impact on the system if the vulnerability were to be exploited."

Loss of confidentiality

How much data could be disclosed, and how sensitive is it? Minimal non-sensitive data disclosed (2), minimal critical data disclosed (6), extensive non-sensitive data disclosed (6), extensive critical data disclosed (7), all data disclosed (9).

Loss of integrity

How much data could be corrupted, and how damaged is it? Minimal slightly corrupt data (1), minimal seriously corrupt data (3), extensive slightly corrupt data (5), extensive seriously corrupt data (7), all data totally corrupt (9).

Loss of availability

How much service could be lost and how vital is it? Minimal secondary services interrupted (1), minimal primary services interrupted (5), extensive secondary services interrupted (5), extensive primary services interrupted (7), all services completely lost (9).

Loss of accountability

Are the threat agents' actions traceable to an individual? Fully traceable (1), possibly traceable (7), completely anonymous (9).

Note: I renamed the original KnowledgeBase to `KnowledgeBase.bak`, then copied *KnowledgeBaseMEDSRV* back to the original destination directory and renamed it *KnowledgeBase*. This prevents corruption of your original files and eliminates the need to re-install TMT. If you'd like my changes to `ThreatCategories.xml` and `ThreatTypes.xml`, hit me over email or Twitter and I'll send them to you. That said, following are snippets (figures 4 and 5) of the changes I made.

8 https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

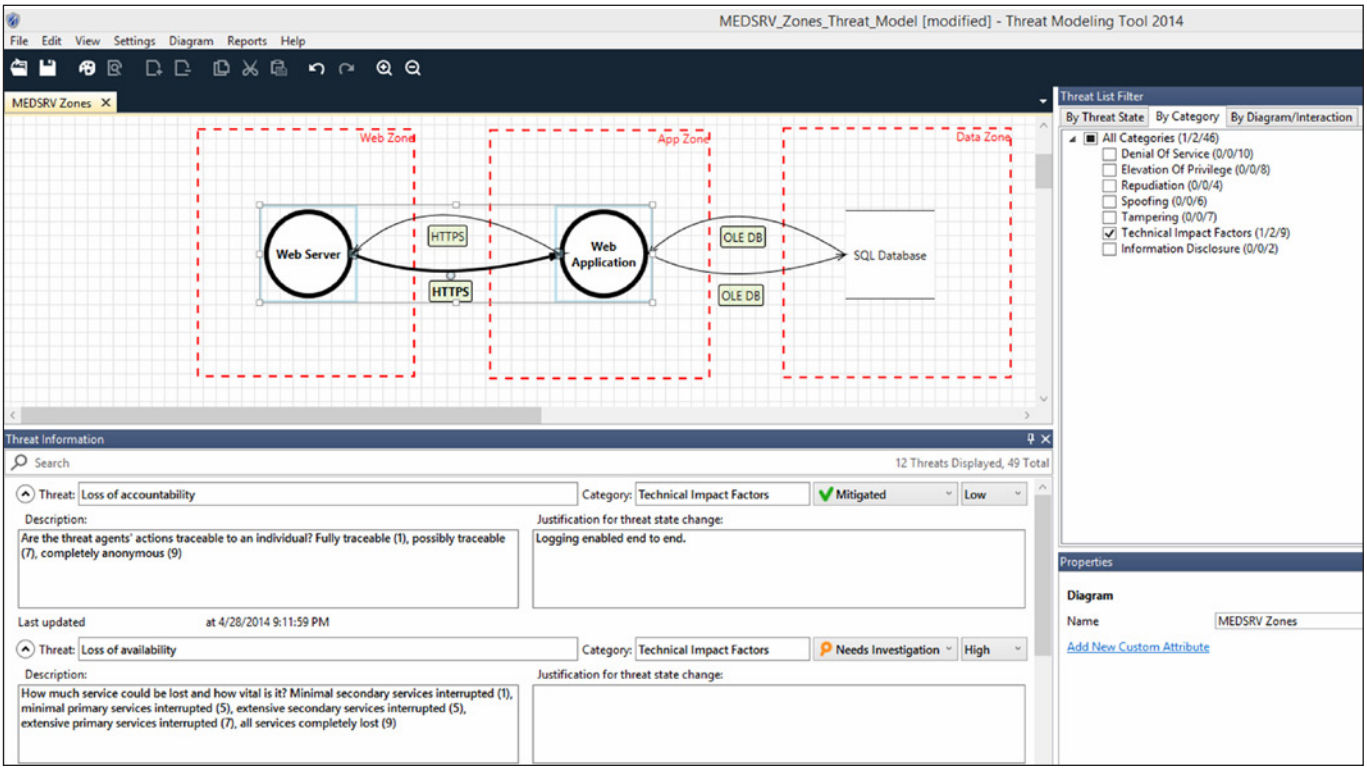

Figure 6 – A threat model of MEDSRV zones using technical impact factors

Take notice of a few key elements in the modified XML. I set `<Id>OTI1</Id>` for OWASP Technical Impact and `<Category>O</Category>` to O for OWASP. ☺ Remember that each subsequent `<Id>` needs to be unique. I declared `<Include>source is 'GE.P' and (target is 'GE.P' or target is 'GE.DS') and flow crosses 'GE.TB'</Include>` because GE.P defines a generic process, GE.DS defines a generic data store, and GE.TB defines a generic trust boundary. Therefore, per my modification, data subject to technical impact factors flows across trust boundaries between processes and data stores. Make sense? I used the resulting TMT KB update to provide a threat model of zones defined for MEDSRV as seen in figure 6.

I'm hopeful these slightly more in-depth investigations of TMT 2014 features entice you to utilize the tool and to engage in the practice of threat modeling. No time like the present to get started.

In conclusion

We've learned enough here to conclude that you have two immediate actions. First, purchase *Threat Modeling: Designing For Security* and begin to read it. Follow this by downloading the Microsoft Threat Modeling Tool 2014 and practice threat modeling scenarios with the tool while you read the book. Conducting these in concert will familiarize you with both the practice of threat modeling as well as the use of TMT 2014.

Remember that July's *ISSA Journal* will be entirely focused on the Practical Use of InfoSec Tools. Send articles or abstracts to editor at issa dot org.

Ping me via email if you have questions or suggestions for topic via russ at holisticinfosec dot org or hit me on Twitter @holisticinfosec.

Cheers…until next month.

Acknowledgements

—Microsoft's: Adam Shostack, author, *Threat Modeling: Designing for Security* and Principal Security PM, TwC Secure Ops

—Emil Karafezov, Security PM II, TwC Secure Development Tools and Policies

—Ralph Hood, Principal Security GPM, TwC Secure Development Tools and Policies

—Steve Lipner, Partner Director, TwC Management

About the Author

Russ McRee manages the Threat Intelligence & Engineering team for Microsoft's Online Services Security & Compliance organization. In addition to toolsmith, he's written for numerous other publications, speaks regularly at events such as DEFCON, Black Hat, and RSA, and is a SANS Internet Storm Center handler. As an advocate for a holistic approach to the practice of information assurance Russ maintains holisticinfosec.org. He serves in the Washington State Guard as the Cybersecurity Advisor to the Washington Military Department. Reach him at russ at holisticinfosec dot org or @holisticinfosec.