Introduction to Software Security

Chapter 2.2:
Threat Modeling Overview and Goals

Elisa Heymann
elisa@cs.wisc.edu

Barton P. Miller
bart@cs.wisc.edu

Loren Kohnfelder
loren.kohnfelder@gmail.com

DRAFT — Revision 1.3, March 2020.

Objectives

- Understand the purpose and goals of Threat Modeling.

Threat modeling happens frequently in many facets of our lives. Everytime we think "what can go wrong?" and plan accordingly, we are performing Threat Modeling. For example, perhaps you need to catch a flight out of Chicago-O'Hare early on a Monday evening and you live 150 miles away. You try to anticipate the different issues that may happen on the way to your flight, such as traffic, construction, a flat tire, or long security lines. To mitigate the different threats, you determine that you need to leave for the airport 5 hours before your flight. That time might give you slack in case that any of those threats became real, but will not have you waiting at the airport for an excessive amount of time. Note that those 5 hours would not be enough in the worst case scenario, if all those threats became real such as an accident causing 70 miles of heavy traffic, then having a flat tire, and then more traffic because of road work. However, you determine that the likelihood of all those threats happening on the same trip is low, so your mitigation strategy consists of leaving 5 hours before your flight.

In the systems area, Threat Modeling consists of identifying the potential threats that can affect your system, with the outcome being a list of the possible threats. Ideally, that list would be prioritized, sorted by the risk associated with the threats. As we saw in the introductory chapter (1.2 Basic Concepts and Terminology), risk depends on the likelihood of that threat becoming real times the impact that threat would have if it became real.

Before any human or tool can identify any threats, we need a model of the system. That means representing the processes, resources (such as database and files), and the interactions between them. The next step is to identify threats associated with the design of your system. There are tools that help designers to do that, but tools have limitations. Even with their limitations, tools can be a good starting point. After the threats have been identified, the designer/analyst needs to come up with ways of mitigating the relevant threats.

There is always a trade-off between how secure our system will be and the amount of resources we are willing to commit to security. We could try to mitigate every possible threat we can think could affect our system, no matter how low the associated risk value. However, such an effort would require a huge amount of resources in terms of time and personnel, which means that it would be very expensive. The

other extreme would be to not care about mitigating any risks. Neither of those two approaches is sensible. Threats that may result in harming your system if they became real need to be mitigated. It is not a trivial task to decide where to draw the line between those that are likely to become real and those that are not.

There are several tools that help the designer with the non-trivial task of performing Threat Modeling. One of them is Microsoft's Threat Modeling Tool, which follows Microsoft's Threat Modeling Methodology.

The rest of this chapter consist of reading some of Microsoft's guides to Threat Modeling:

- https://docs.microsoft.com/en-us/azure/security/azure-security-threat-modeling-tool : (1 short page of introduction to MS Threat Modeling).
- https://docs.microsoft.com/en-us/azure/security/azure-security-threat-modeling-tool-getting-started . Basic tutorial on the MS Threat Modeling Tool.
- https://docs.microsoft.com/en-us/azure/security/azure-security-threat-modeling-tool-threats. Short review of STRIDE that covered that in the introductory Chapter 1.2 Basic Concepts and Terminology.
- https://docs.microsoft.com/en-us/azure/security/azure-security-threat-modeling-tool-mitigations. A description of how to mitigate the threats that you found with the Threat Modeling Tool.