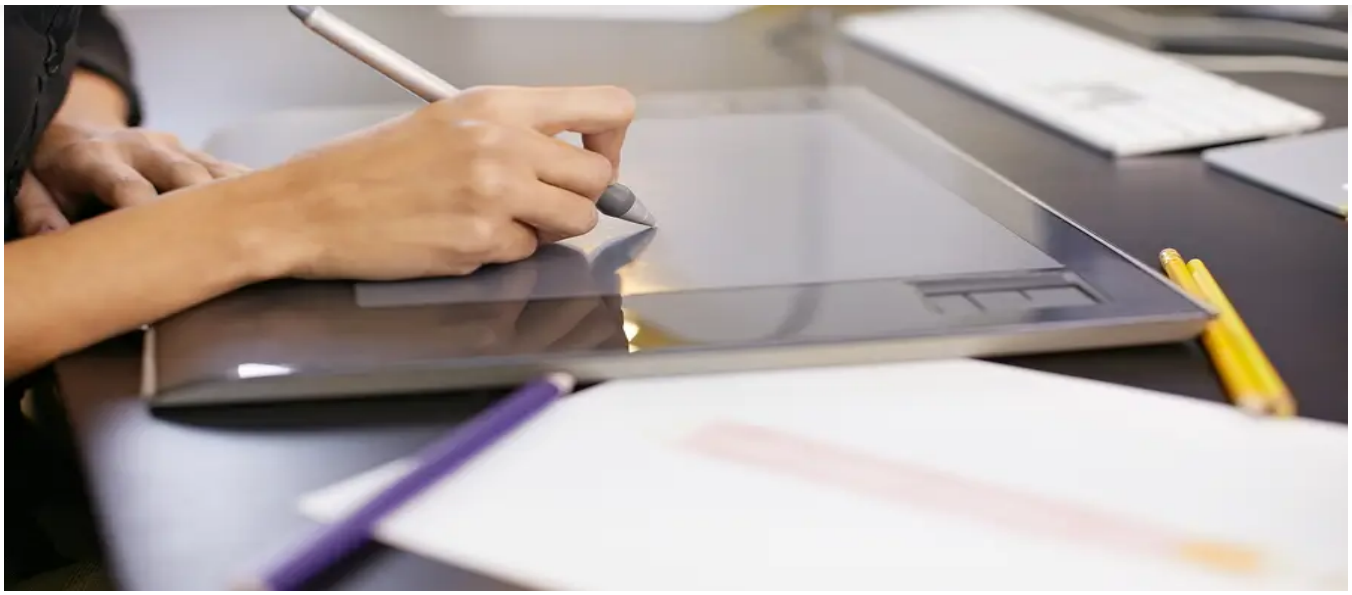


Light Dark

August 15, 2016

By Stiliyana Simeonova

3 min read

CISO

Risk Management

This is the second installment in a series on threat modeling. For the full story, read part 1 and part 3 as well.

Enterprise information security mangers need effective tools for prioritizing their efforts now more than ever. The first part of this series focused on why threat modeling can be a valuable weapon in your arsenal, even outside the initial phases of the system development life

modeling.

Threat Modeling: A Four-Step Process

There are many different threat modeling methodologies and practices. The three models that are probably the most widely adopted are Trike, PASTA and Microsoft STRIDE. PASTA and STRIDE were developed to integrate security in the software development methodologies, while Trike was developed as a tool to facilitate the security audit process.

All three methodologies have similarities in the way they approach the threat modeling process. The following four steps outline key activities that support the generic process:

1. Define your objectives and scope.
2. Decompose the system, usually using data flow diagrams (DFDs).
3. Identify the threats.
4. Priorities the threats.

1. Define Your Objectives and Scope

Before you start evaluating any system from a threat perspective, you need to have a clear understanding of the business objectives the system is designed to meet as well as security criteria it needs to fulfill. Otherwise, your threat modeling process will lack foundation and is likely to be ineffective.

Outline the business and security objectives concisely. This will help you, whether you are performing quick assessment by yourself or aiming to hold elaborate threat modeling sessions involving other team members.

Once you've defined the objectives, narrow down the technical scope. This enables you to keep your activity focused and avoid distractions. Threat modeling tends to be time-consuming, and defining a clear

PASTA methodology suggests the use of security architecture review questionnaires when defining the technical scope, but any high-level design document outlining the system components and interfaces is a good starting point. Make sure the documentation you gather is up to date and you are not missing vital bits of information about current and upcoming architectural changes.

2. Decompose the System

This step provides you with list of targets that an attacker could aim for. These might be data assets, communication channels, computing components, etc.

Detailed knowledge about your system is crucial. Generally, system architects, development team members and system administrators should all be involved. Their in-depth knowledge will guarantee that you have adequate input when reviewing all the system components and their internal relations or the way they relate with the external world.

DFDs can help you visualize the system components and their interactions while performing threat modeling. DFDs allow you to formally represent the trust level boundaries, which are essential when evaluating the possible attack paths an adversary could take.

3. Identify the Threats

After decomposing the system, enumerate the possible threats to each and every component. Taxonomies such as Microsoft STRIDE are extremely helpful starting points to enumerate common threats against the different elements of your DFD.

Keep in mind, however, that your system has unique properties. Maintain focus on your specific security goals to avoid producing a model

Related: Threat Modeling in the Enterprise, Part 3: Understanding the Context

As part of this step, create threat catalogs to document your findings. At this point, you are aiming for completeness. Do not shy away from including exotic threat vectors as long as they align with one or more system use cases. For large enterprise systems, you are likely to end up with a huge threat catalog filled with entries. That is where taxonomies come in handy as well: They allow you to focus on categories of threats rather than single entries.

Threats in the same category are likely to be subject to the same prioritization later on. Most importantly, these threats will probably be addressed by common security controls.

4. Prioritize Threats

At this point, you should already have a good view of the threat vectors and possible attack scenarios against your system. Now is the time to consider your security priorities and assign weights against categories of threats or particular threat vectors.

You can use any of the following as a starting point for your prioritization:

- Existing asset classification;
- Attack vector importance and likelihood; and
- Threat actor importance.

Your decision should be driven by your business priorities. If your business is concerned about particular categories of fraud, for example, these will usually be mapped to a certain attack path. These threats should be marked high priority. Threat prioritization plays an important role for obvious reasons; you do not want to spend too much money protecting assets with lesser value to your business.

controls selection process. It can provide peace of mind that the adequate controls are selected and ultimately save your business money in the long run.

Learn more about X-Force Red and IBM's specialized pen testing services

Advanced Threats | Modeling | Risk Management | Threat Intelligence | Threat Protection

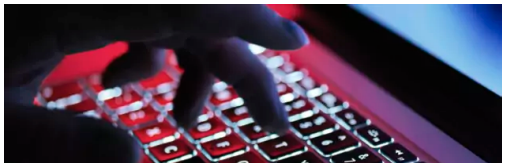
Stiliyana Simeonova
Senior Security Consultant, IBM

POPULAR

RISK MANAGEMENT | November 26, 2024

83% of organizations reported insider attacks in 2024

4 min read - According to Cybersecurity Insiders' recent 2024 Insider Threat Report, 83% of organizations reported at least one insider attack in the last year. Even more surprising than this statistic is that organizations that...



RISK MANAGEMENT | November 6, 2024

What Telegram's recent policy shift means for cyber crime