Threat Modeling

What is Threat Modeling?

Threat modeling is an approach for analyzing the security of an application. It is a structured approach that enables you to identify, quantify, and address the security risks and potential vulnerabilities that are associated with an application. Essentially, threat modeling is designed to answer questions such as "*Where is my application most vulnerable to attacks?*", "*What are the key risks?*", and "*What should I do to reduce these risks?*".

Why should we do Threat Modeling?

Overall, threat modeling can provide a clear line of sight across a software project. When done correctly, a well-documented threat model provides assurances that are useful in explaining and defending the security posture of an application.

In essence, threat modeling is a very effective way to:

- Detect design flaws and other issues early in the SDLC, preferably before coding begins.
- Evaluate new forms of attack that might not otherwise have been considered.
- Identify security requirements.
- Think about threats beyond standard attacks to the security issues unique to an application.
- Highlight assets, threat agents, and controls to identify components that attackers will target.

How do I go about creating a Threat Model?

You will find that there are a various number of steps that are recommended to follow when creating a threat model. In this article though we will outline these 3 basic steps:

1. Decompose the application
2. Discover and rank the threats
3. Establish countermeasures and a mitigation strategy

Decompose the Application

The first step in the threat modeling process is to gain an understanding of the application and how it interacts with external entities. This involves creating use /cases to understand how the application is used. This will include identifying entry points to see where a potential attacker could interact with the application. It will also include identifying assets that the attacker would be interested in, and identifying trust levels which represent the access rights that the application will grant to external entities.

Goals for this step are to:

- ✓ Learn as much as possible about the application.
- ✓ Read and understand all of the available design materials.
- ✓ Determine system boundaries and data sensitivity/criticality.
- ✓ Study the code and other software artifacts if available.
- ✓ Identify threats and agree on relevant sources of attack.

Discover and Rank the Threats

In this step a threat categorization model is used to identify and rank potential threats in the application. One of the most popular models which can help to identify threats from an attacker is the *STRIDE* model which stands for: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege.

The security risk for each identified threat can be discovered using a value-based risk model such as *DREAD* which stands for: Damage, Reproducibility, Exploitability, Affected users and Discoverability.

There are other models that are used to discover and rank threats besides the STRIDE and DREAD models but they are the most popular ones in use today. A detailed description of these models is beyond the scope of this article. For more information on the STRIDE and DREAD models please visit:

STRIDE (security)
https://en.wikipedia.org/wiki/STRIDE_(security)

DREAD (risk assessment model)
https://en.wikipedia.org/wiki/DREAD_(risk_assessment_model)

Goals for this step are to:

- ✓ Discuss security issues surrounding the application.
- ✓ Identify possible vulnerabilities, sometimes making use of tools or lists of common vulnerabilities.
- ✓ Map out exploits and begin to discuss possible fixes.
- ✓ Gain an understanding of current and planned security controls.
- ✓ Determine probability of compromise.
- ✓ Map out attack scenarios for exploits of vulnerabilities.
- ✓ Perform an impact analysis.
- ✓ Determine impacts on assets and business goals.
- ✓ Consider impacts on the security posture.
- ✓ Rank risks.

Establish Countermeasures and a Mitigation Strategy

In this last step a lack of protection against a threat might indicate a vulnerability whose risk exposure could be mitigated with the implementation of a countermeasure. Such countermeasures can be identified using threat-countermeasure mapping lists.

The risk mitigation strategy might involve evaluating identified threats from the business impact that they pose and reducing the risk. Other options might include taking the risk, assuming the business impact is acceptable because of compensating controls, informing the user of the threat, removing the risk posed by the threat completely, or the least preferable option, that is, to do nothing.

Goals for this step are to:

- ✓ Develop a mitigation strategy.
- ✓ Recommend countermeasures to mitigate risks.
- ✓ Report findings.
- ✓ Carefully describe the major and minor risks, with attention to impacts.
- ✓ Provide basic information regarding where to spend limited mitigation resources.

The information that is gathered in each of the above steps must be documented as they are carried out. The resulting document will be the threat model for the application. The documented information can also be used to create data flow and process flow diagrams for the application. These diagrams will show the different paths through the application.

To Summarize

Threat modeling is a good investment and highly recommended because finding and mitigating threats in the design phase of our applications can help reduce the cost of mitigation down the road. Consistently implementing threat modeling can also improve our security posture over time. More specifically, threat modeling lp can identify cyber security threats and vulnerabilities and it can provide insights into what controls or defenses that should be put into place given the nature of the application, the high value assets to be protected and the potential attack paths to the high value assets.