Introduction to Software Security

Chapter 2.5:
PASTA Threat Modeling Methodology

Elisa Heymann
elisa@cs.wisc.edu

Barton P. Miller
bart@cs.wisc.edu

DRAFT — Revision 3.0, August 2023.

Objectives

- Learn about the PASTA Threat Modeling Methodology and its seven stages.
- Understand PASTA's relationship to the Microsoft methodologies.

Overview

PASTA is the Process for Attack Simulation and Threat Analysis. It was presented in 2015[1] as an alternative to the Microsoft Threat Modeling methodology and Security Development Lifecycle.

We will discuss the seven "stages" of the PASTA methodology, briefly explain each one and then map it onto the Microsoft approach.

The Seven Stages of PASTA

1. Define the Objectives

The PASTA methodology broadly interprets objectives to mean the business objectives of what is being modeled; security objectives; compliance, regulatory, and standards requirements (such as HIPAA for healthcare data[2], EU-GDPR for computer systems in the European Union[3], and PCI DSS for credit card companies[4]); and analysis of data to be protected.

This stage has many similarities to the Requirements step in the Microsoft SDL software development lifecycle.

2. Define the Technical Scope

The technical scope of the model defines what are the components in the system, their relationship with other systems and software (including dependency chains), and the attack surface.

---

[1] Tony Uceda Vélez and Marco M. Morana, **Risk Centric Threat Modeling**, John Wiley & Sons, 2015.
[2] U.S. Department of Health and Human Services, "The HIPAA Privacy Rule", https://www.hhs.gov/hipaa/for-professionals/privacy/
[3] B. Wolford, "What is GDPR, the EU's new data protection law?", https://gdpr.eu/what-is-gdpr/
[4] PCI Security Standards Council, https://www.pcisecuritystandards.org/

This stage corresponds to the Design step of the Microsoft SDL where Threat Modeling takes place.

3. Decompose the Application

In this stage, we drill down to the internal structure of the software system, understanding its internal components and how they interact. This stage includes both the computational and data components of the system. As part of this analysis, we describe the use cases for the system and user roles and permissions.

This stage corresponds to the Create an Application Diagram in Microsoft Threat Modeling.

4. Analyze the Threats

This stage focuses on the threats and how they relate to the attack surface. In PASTA, the threats are based on insights of the analysts, threat intelligence reports, and lists of known attacks. They emphasize addressing threats that have been demonstrated in the real world.

Such an approach has its advantages and disadvantages. Working from known threats means that you are addressing issues that have been encountered previously (and presumably succeeded somewhere) based on the experiences of others. However, such an approach will not address new and unique threats that are created based on the unique design characteristics of the software system you are analyzing, but there is nothing stopping you from extending your analysis to consider these as well. Vulnerabilities based on these unique characteristics are more difficult to find, for both the creators of the system and the attackers, but far from impossible to find.

This stage corresponds to the Identify Threats step in Microsoft Threat Modeling.

5. Vulnerability Analysis

The next stage is to understand the vulnerabilities in the system. At this stage, we have gone beyond the design and are now looking at the implementation. We are looking for vulnerabilities in the code, using penetration testing, and databases of known vulnerabilities.

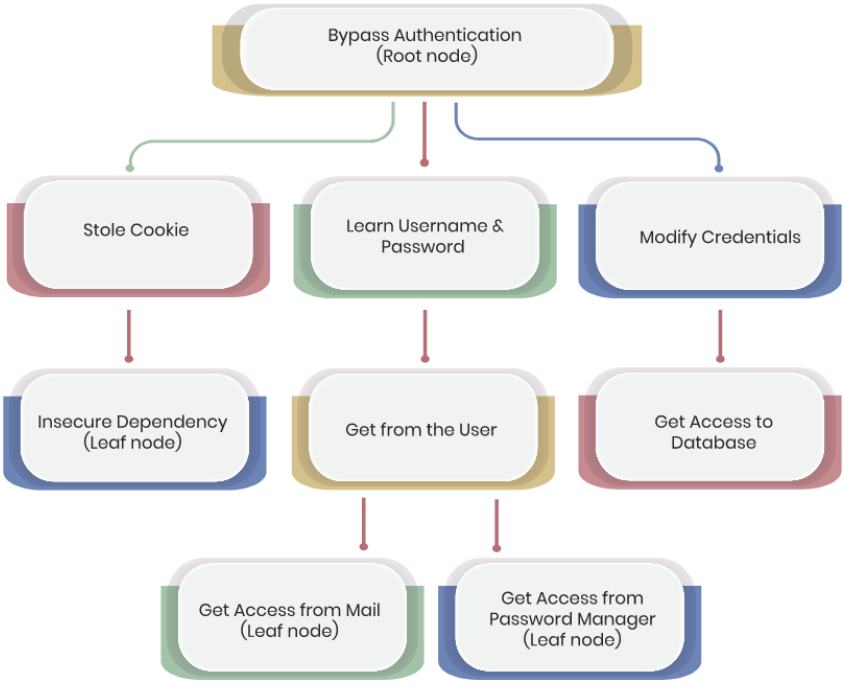
This stage corresponds to the Implementation and Verification steps in Microsoft's SDL.

In addition, doing code analysis can be part of an in-depth vulnerability assessment process, such as the First Principles Vulnerability Assessment methodology that we describe in Module 5.

6. Attack Analysis

The fifth stage tries to link the threats to the vulnerabilities by means of an Attack Tree[5]. An attack tree is a diagram that shows the conditions that must be satisfied for an attack to be accomplished. The root of the tree describes the final result. Below is an example from the British National Cyber Security Centre[6].

[5] https://en.wikipedia.org/wiki/Attack_tree
[6] "Using Attack Trees to Understand Cyber Security Risk", National Cyber Security Centre, UK, https://www.ncsc.gov.uk/collection/risk-management/using-attack-trees-to-understand-cyber-security-risk



7. Risk and Impact Analysis

This final stage attempts to summarize the information from all the previous steps. In this stage, there is an attempt to understand the risk to the business practices, find gaps in the security controls, and understand how the risks will be mitigated.

Summary

Like the Microsoft Threat Modeling methodology, the PASTA methodology is supported by a threat modeling tool[7]. This tool can provide an organizational structure for the PASTA process, help with the diagram construction, and automatically include many known threats for the design. It can also help with report preparation and organization.

Exercises

1. For a new or existing software project, work through the steps of PASTA Threat Modeling using the PASTA tool. Identify the objectives and scope of your project, develop the diagram, use the tool to identify potential threats, and then evaluate these to decide what kind of response is needed.
2. Pick a real world situation such as securing a bank. Develop an attack tree that represents the threats that are presenting when trying to secure that situation.

[7] N. Kirtley, “Threat Modeling Tool”, November 2022, https://threat-modeling.com/threat-modeling-tool/