PASTA Threat Model 2024-11-04 #1

Globe Systems

Summary

The use of the Process for Attack Simulation and Threat Analysis (PASTA) threat model framework will be applied. It will be determined whether it is safe to launch a new shopping application.

Threat modeling is an important part of secure software development. Security teams often perform threat modeling to identify vulnerabilities before malicious actors do. PASTA is a commonly used framework to assess the risk profile of new applications.

Scenery

As part of the security team of the startup Globe Sistemas, we are preparing to launch an AI-powered mobile application for HelpDesk assistance.

You are performing application threat modeling using the PASTA framework. You will go through each of the seven stages of the framework to identify the security requirements of the enterprise's new application.

PASTA STAGES

Identify the business objectives of the APP

The main objective of Stage I of the PASTA framework is to understand why the application has been developed and what it is expected to do.

Note: Stage I typically requires gathering information from many people within a company.

First, review the following description of why the systems company decided to develop this new application:

Description: Our app needs to seamlessly connect users and support. It should be easy for users to sign up, log in, and manage their accounts. Data privacy is a big concern for us. We want users to feel confident that we are being responsible with their information.

Technicians should be able to send messages directly to customers with their answers. They should also have the ability to rate technicians to encourage good service. Service tickets should be clear and quick to process. Users should be provided with multiple payment options to make the support process smooth. Proper payment management is really important because we want to avoid legal issues.

Evaluate application components

In Stage II, the technological scope of the project is defined. Typically, the application development team is involved in this stage because they have the most knowledge about the code base and application logic. Your responsibility as a security professional would be to assess the application architecture for security risks.

For example, the app will exchange and store a lot of user data. Here are some of the technologies it uses:

Application programming interface (API): An API is a set of rules that define how software components interact with each other. In application development, third-party APIs are commonly used to add functionality without having to program it from scratch.

Public Key Infrastructure (PKI): PKI is an encryption framework that secures the exchange of information online. The mobile app uses a combination of symmetric and asymmetric encryption algorithms: AES and RSA. AES encryption is used to encrypt sensitive data, such as credit card information. RSA encryption is used to exchange keys between the app and the user's device.

SHA-256: SHA-256 is a commonly used hash function that takes an input of any length and produces a 256-bit hash. The app will use SHA-256 to protect sensitive user data such as passwords and credit card numbers.

Structured Query Language (SQL): SQL is a programming language used to create, interact with, and query information from a database. For example, the mobile app uses SQL to store information about the services that are for sale, as well as the technicians who sell them. It also uses SQL to access that data during a purchase.

Review a data flow diagram

During Stage III of PASTA, the goal is to analyze how the application handles information. Each process is broken down here.

For example, one of the application processes could be to allow customers to search the database for services that are for sale.

Open the PASTA data flow diagram resource. Review the diagram and consider how the technologies you have evaluated relate to protecting user data in this process.

Note: Software developers often provide detailed data flow diagrams for security teams to use to verify that information is processed securely.

Use attacker mentality to analyze potential threats

Stage IV involves identifying potential threats to the application. This includes threats to the technologies you listed in Stage II. It also affects the processes in your Stage III data flow diagram.

For example, the application's authentication system could be attacked with a virus. Authentication could also be attacked if a threat actor social engineers an employee.

Pro Tip: Internal system logs that you will use as a security analyst are good sources of threat intelligence.

List of vulnerabilities that can be exploited by these threats

Stage V of PASTA is vulnerability analysis. Here, you need to consider the attack surface of the technologies listed in Stage II.

For example, the app will use a payment system. The form used to collect credit card information could be vulnerable if you don't encrypt the data.

In Stage V of the PASTA worksheet, list 2 types of vulnerabilities that could be exploited.

Pro Tip: Resources like the Common Software Vulnerabilities and Exposures List

(CVE®) and OWASP are useful for finding common software vulnerabilities.

Map of resources, threats and vulnerabilities in an attack tree

In Stage VI of PASTA, the information gathered in the previous two stages is used to build an Attack Tree.

Open the PASTA Attack Tree resource. Review the diagram and consider how threat actors can potentially exploit these attack vectors.

Note: Applications of this type typically have large, complex attack trees with many branches.

Identify new security controls that can reduce risk

The PASTA Threat Model is commonly used to reduce the likelihood of security risks occurring. In Stage VII, the ultimate goal is to implement defenses and safeguards that mitigate the threats.

In Stage VII of the PASTA worksheet, list 4 security controls that you are aware of that can reduce the chances of a security incident, such as a data breach, occurring.

PASTA Worksheet

| PASTA Stages | Globe Systems APP |
| --- | --- |
| I. Define business and security objectives | Make 2-3 notes of special business requirements that will be analyzed.   * Will the app process transactions? * Does the app do a lot of backend processing? * Are there industrial regulations that must be taken into account? * Users can create member profiles internally or by connecting external accounts. * The application must process financial transactions. * The application must comply with PCI-DSS. |
| II. Define the technical scope | List of technologies used by the application:   * Application programming interface (API) * Public key infrastructure (PKI) * SHA-256 * SQL   APIs facilitate the exchange of data between customers, partners and employees, so they should be prioritized.  They handle a large amount of sensitive data while connecting multiple users and systems to each other.  However, details such as which APIs are being used should be considered before prioritizing one technology over another.  Therefore, they may be more prone to security vulnerabilities because there is a larger attack surface. |
| III. Break down the application | [Sample data flow diagram](https://docs.google.com/presentation/d/1ol7y79popTFfNHM-90ES-H-i1Lpd0YNvPShxBlXozjg/template/preview?resourcekey=0-DZAkf7Vzh2PXsP-j3oXV-g) |
| IV. Threat analysis | List 2 types of threats in the PASTA spreadsheet that are risks to the information being handled by the application.   * What are internal threats? * What are external threats? List 2 types of threats in the PASTA spreadsheet that represent risks to the information handled by the application. * Injection * Session hijacking |
| V. Vulnerability analysis | List 2 vulnerabilities in PASTA WorkSheet that can be exploited.   * Could there be a problem with the codebase? * Could there be weaknesses in the database? * Could there be network failures? * Lack of prepared statements * Corrupted API Token |
| VI. Attack modeling | [Sample attack tree diagram](https://docs.google.com/presentation/d/1FmWLyHgmq9XQoVuMxOym2PHO8IuedCkan4moYnI-EJ0/template/preview?usp=sharing&resourcekey=0-zYPY7AhPJdcClXamlAfOag) |
| VII. Risk and impact analysis | List four security controls you have learned that can reduce risk.   * SHA-256, * Incident response procedures * Password Policy * Principle of least privilege |