Activity Overview

In this activity, you will practice using the Process of Attack Simulation and Threat Analysis (PASTA) threat model framework. You will determine whether a new shopping app is safe to launch.

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

Scenario

Review the following scenario. Then complete the step-by-step instructions.

You're part of the growing security team at a company for sneaker enthusiasts and collectors. The business is preparing to launch a mobile app that makes it easy for their customers to buy and sell shoes.

You are performing a threat model of the application using the PASTA framework. You will go through each of the seven stages of the framework to identify security requirements for the new sneaker company app.

Step-By-Step Instructions

`

Follow the instructions and answer the included questions to complete the activity.

Part 1 - Access the resources

PASTA worksheet

Stages

Sneaker company

I. Define business and security objectives

Make 2-3 notes of specific business requirements that will be analyzed.

- Will the app process transactions?
- Does it do a lot of back-end processing?
- Are there industry regulations that need to be considered?

II. Define the technical scope

List of technologies used by the application:

- API
- PKI
- AES
- SHA-256
- SQL

Write 2-3 sentences (40-60 words) that describe why you choose to prioritize that technology over the others.

III. Decompose application

Sample data flow diagram

IV. Threat analysis

●

V. Vulnerability analysis

List 2 vulnerabilities in the PASTA worksheet that could be exploited.

● Could there be things wrong with the codebase?
● Could there be weaknesses in the database?
● Could there be flaws in the network?

VI. Attack modeling

Sample attack tree diagram

VII. Risk analysis and impact

List 4 security controls that you've learned about that can reduce risk.

Step2: Access the supporting materials.

The following supporting materials will help you complete this activity. Keep them open as you proceed to the next steps.

Part 2 - Complete the PASTA stages

Step 1: Identify the mobile app's business objectives

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

Note: Stage I typically requires gathering input from many individuals at a business.

First, review the following description of why the sneaker company decided to develop this new app:

Description: Our application should seamlessly connect sellers and shoppers. 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're being responsible with their information. Buyers should be able to directly message sellers with questions. They should also have the ability to rate sellers to encourage good service. Sales should be clear and quick to process. Users should have several payment options for a smooth checkout process. Proper payment handling is really important because we want to avoid legal issues.

In the Stage 1 row of the PASTA worksheet, make 2-3 notes of business objectives that you've identified from the description.

English

To pass this course item, you must receive at least 100%, or 1 out of 1 points, by completing the following activity. You can learn more about the graded and practice items in the course overview.

Activity Overview

In this activity, you will practice using the Process of Attack Simulation and Threat Analysis (PASTA) threat model framework. You will determine whether a new shopping app is safe to launch.

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

Scenario

Review the following scenario. Then complete the step-by-step instructions.

You're part of the growing security team at a company for sneaker enthusiasts and collectors. The business is preparing to launch a mobile app that makes it easy for their customers to buy and sell shoes.

You are performing a threat model of the application using the PASTA framework. You will go through each of the seven stages of the framework to identify security requirements for the new sneaker company app.

Step-By-Step Instructions

Follow the instructions and answer the included questions to complete the activity.

Part 1 - Access the resources

Step 1: Access the template

To use the template for this course item, click the following link and select Use Template.

Link to template: PASTA worksheet

OR

If you don't have a Google account, you can download the template directly from the following attachment.

PASTA worksheet
DOCX File

Step 2: Access supporting materials

The following supporting materials will help you complete this activity. Keep them open as you proceed to the next steps.

To use the supporting materials for this course item, click the following link and select Use Template.

Link to supporting materials:

· PASTA data flow diagram
· PASTA attack tree

OR

If you don't have a Google account, you can download the supporting materials directly from the following attachment.

PASTA data flow diagram
PPTX File

PASTA attack tree
PPTX File

Part 2 - Complete the PASTA stages

Step 1: Identify the mobile app's business objectives

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

Note: Stage I typically requires gathering input from many individuals at a business.

First, review the following description of why the sneaker company decided to develop this new app:

Description: Our application should seamlessly connect sellers and shoppers. 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're being responsible with their information. Buyers should be able to directly message sellers with questions. They should also have the ability to rate sellers to encourage good service. Sales should be clear and quick to process. Users should have several payment options for a smooth checkout process. Proper payment handling is really important because we want to avoid legal issues.

In the Stage 1 row of the PASTA worksheet, make 2-3 notes of business objectives that you've identified from the description.

Step 2: Evaluate the apps components

In Stage II, the technological scope of the project is defined. Normally, 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 evaluate the application's architecture for security risks.

For example, the app will be exchanging and storing a lot of user data. These are some of the technologies that 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 online information. 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 a user's device.

· SHA-256: SHA-256 is a commonly used hash function that takes an input of any length and produces a digest of 256 bits. The sneaker app will use SHA-256 to protect sensitive user data, like passwords and credit card numbers.

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

Consider what you've learned about these technologies:

· Which of these technologies would you evaluate first? How might they

present risks from a security perspective?
In the Stage II row of the PASTA worksheet, write 2-3 sentences (40-60 words) that describe why you choose to prioritize that technology over the others.

Step 3: Review a data flow diagram
During Stage III of PASTA, the objective is to analyze how the application is handling information. Here, each process is broken down.
For example, one of the app's processes might be to allow buyers to search the database for shoes that are for sale.
Open the PASTA data flow diagram resource. Review the diagram and consider how the technologies you evaluated relate to protecting user data in this process.
Note: Software developers usually have detailed data flow diagrams available for security teams to use and verify that information is being processed securely.

Step 4: Use an attacker mindset to analyze potential threats
Stage IV is about identifying potential threats to the application. This includes threats to the technologies you listed in Stage II. It also concerns the processes of your data flow diagram from Stage III.
For example, the apps authentication system could be attacked with a virus. Authentication could also be attacked if a threat actor social engineers an employee.
In the Stage IV row of the PASTA worksheet, list 2 types of threats that are risks to the information being handled by the sneaker company's app.
Pro tip: Internal system logs that you will use as a security analyst are good sources of threat intel

Step 5: List vulnerabilities that can be exploited by those threats
Stage V of PASTA is the 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 might be vulnerable if it fails to encrypt data.
In Stage V of the PASTA worksheet, list 2 types of vulnerabilities that could be exploited.
Pro tip: Resources like the CVE® list and OWASP are useful for finding common software vulnerabilities.

Step 6: Map assets, threats, and vulnerabilities to an attack tree
In Stage VI of PASTA, the information gathered in the previous two steps are 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 like this normally have large, complex attack trees with many branches.

Step 7: Identify new security controls that can reduce risk

PASTA threat modeling is commonly used to reduce the likelihood of security risks. In Stage VII, the final goal is to implement defenses and safeguards that mitigate threats.
In Stage VII of the PASTA worksheet, list 4 security controls that you have learned about that can reduce the chances of a security incident, like a data breach.

Stage I: Define business and security objectives
.Will the app process transactions?
.Does it do a lot of back-end processing?
.Are there industry regulations that need to be considered?

Stage II: Define the technical scope.
List of technologies used by the application:
- API
- PKI
- AES
- SHA-256
- SQL

. why do you choose to prioritize that technology over the others?

Stage III: Decompose the application based on data flow diagram.

Stage IV: Threat analysis
List 2 types of threats in the PASTA worksheet that are risks to the information being handled by the application.
.What are the internal threats?
.What are the external threats?

Stage V: Vulnerability analysis
Please List 2 vulnerabilities in the PASTA worksheet that could be exploited.
.Could there be things wrong with the codebase?
.Could there be weaknesses in the database?
.Could there be flaws in the network?

Stage VI: Attack modeling based on sample attack tree below

Stage VII: Risk analysis and impact

Stage I: Define Business and Security Objectives
Will the app process transactions?

Summary: Yes, the app will process transactions as part of its functionality.
Recommendation: Implement secure payment handling mechanisms, encryption, and regular audits of transaction processes.
Does it do a lot of back-end processing?
Summary: The app involves significant back-end processing, including user account management and transaction handling.
Recommendation: Ensure robust back-end security, implement proper access controls, and conduct thorough testing of back-end functionalities.
Are there industry regulations that need to be considered?
Summary: Yes, data privacy is a significant concern, suggesting the need to comply with industry regulations.
Recommendation: Conduct a comprehensive review of data protection regulations, implement necessary measures for compliance, and regularly update security protocols.

Stage II: Define the Technical Scope
List of Technologies:
API, PKI, AES, SHA-256, SQL
Why prioritize:
Summary: Prioritize API and PKI due to their critical roles in data exchange and encryption.
Recommendation: Focus on securing API endpoints, implementing strong PKI practices, and continuously monitoring and updating encryption protocols.

Stage III: Decompose the Application Based on Data Flow Diagram
Summary: Examine the data flow diagram to understand how information is processed within the application.
Recommendation: Collaborate with development teams to ensure secure data handling at each processing stage.

Stage IV: Threat Analysis
List 2 types of threats:
Internal Threats:
Summary: Internal threats could involve unauthorized access by employees or contractors.
Recommendation: Implement strict access controls, conduct employee training on security best practices, and monitor internal activities.
External Threats:
Summary: External threats could include attacks on authentication systems or social engineering.
Recommendation: Strengthen authentication mechanisms, implement multi-factor authentication, and conduct regular security awareness training for users.

Stage V: Vulnerability Analysis
List 2 vulnerabilities:
Codebase Vulnerabilities:

Summary: Code vulnerabilities may exist, exposing the application to exploitation.
Recommendation: Conduct regular code reviews, use automated tools to identify vulnerabilities, and patch any discovered issues promptly.
Database Weaknesses:
Summary: Database weaknesses could lead to unauthorized access or data manipulation.
Recommendation: Implement strong database encryption, regular security audits, and least privilege access controls.

Stage VI: Attack Modeling Based on Sample Attack Tree
Summary: Develop an attack tree based on identified threats and vulnerabilities to understand potential attack vectors.
Recommendation: Use the attack tree to prioritize security measures and allocate resources effectively.
: Implement multi-factor authentication and enforce strong password policies.

Stage VII: Risk Analysis and Impact
List 4 Security Controls:
Regular Security Audits:
Summary: Periodic audits help identify vulnerabilities and weaknesses.
Recommendation: Implement regular security audits and penetration testing.
Intrusion Detection Systems:
Summary: IDS helps detect and respond to potential security breaches.
Recommendation: Deploy and configure IDS to monitor network activities.
Data Encryption:
Summary: Encryption safeguards sensitive data.
Recommendation: Implement end-to-end encryption for user data.
User Authentication Controls:
Summary: Strong authentication mechanisms enhance overall security.

Top of Form
Bottom of Form