## **Portfolio Project: Apply the PASTA threat model framework**

## **Activity Overview (Google Cybersecurity Analyst Certificate Program: Course 5)**

## 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**

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 One Details:**

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.

**Step Two Details:**

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 Three Details:**

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 Four Details:

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 Five Details:

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 Six Details:

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 Seven Details:

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.

## PASTA worksheet

|  |  |
| --- | --- |
| **Stages** | **Sneaker company** |
| **I. Define business and security objectives** | * Seamless Connection between Sellers and Shoppers: The primary goal of the application is to facilitate a seamless connection between sellers and shoppers. This indicates that the app should prioritize user-friendly features and functionalities for both buyers and sellers, such as easy sign-up, login, and account management. * Data Privacy and Responsible Information Handling: Data privacy is a significant concern for the company. This implies that the application must prioritize robust security measures to protect user data and ensure responsible handling of personal information. Compliance with data privacy regulations, such as GDPR or CCPA, may be necessary. * Efficient Transaction Processing and Payment Handling: The description highlights the importance of clear and quick sales processing, as well as providing multiple payment options for a smooth checkout process. This suggests that the app should prioritize efficient transaction processing and secure payment handling to avoid legal issues. Compliance with payment industry standards and regulations, such as PCI DSS, should be considered.   *These objectives indicate that the app will indeed process transactions, require significant back-end processing for transaction management, and need to adhere to industry regulations related to data privacy and payment handling.* |
| **II. Define the technical scope** | In Stage II of the PASTA framework, I would prioritize the evaluation of Public Key Infrastructure (PKI) over the other technologies listed. PKI plays a critical role in securing the exchange of online information and is crucial for ensuring the confidentiality and integrity of sensitive user data in the mobile app. The use of both symmetric (AES) and asymmetric (RSA) encryption algorithms within PKI indicates its central role in safeguarding data privacy and protecting against unauthorized access. PKI's proper implementation and management will be essential to mitigate risks associated with data breaches and unauthorized access to user information, making it a top priority for security assessment. |
| **III. Decompose application** | When analyzing the process of allowing buyers to search for shoes that are for sale, consider the following:  Data Flow: Understand how data flows within this process. What data is collected from users (e.g., search queries), and how is it processed and stored?  Data Storage: Identify where and how user data is stored during this process. Is SQL used to store information about shoes and sellers? How is sensitive data protected while at rest?  Data Transmission: Evaluate how data is transmitted between the user's device and the application's servers. Does PKI (Public Key Infrastructure) play a role in securing this data in transit, using encryption mechanisms like SSL/TLS?  Data Access: Consider how data access is controlled. Are API calls made during the search process, and how are they authenticated and authorized? Are user roles and permissions properly enforced?  Data Protection: How are sensitive data elements (e.g., user profiles, credit card information) protected? Is AES encryption used for encrypting data like credit card information? Is SHA-256 used for hashing sensitive data like passwords?  Data Retention and Deletion: Assess how long user data is retained and whether there are mechanisms in place for data deletion when it's no longer needed.  Logging and Monitoring: Determine whether logging mechanisms are in place to track user actions and potential security incidents during this process. How is security monitoring conducted?  *By considering these aspects in your analysis, you can identify potential security risks and how the previously evaluated technologies, such as PKI, AES, and SHA-256, contribute to protecting user data within the application's processes. It's crucial to ensure that data handling aligns with security best practices and compliances with relevant regulations to mitigate risks effectively.* |
| **IV. Threat analysis** | In the Stage IV row of the PASTA worksheet, here are two types of threats that are risks to the information being handled by the sneaker company's app:  Internal Threat: Insider Data Theft - An internal threat could involve a malicious employee or contractor with access to the system attempting to steal sensitive user data, such as credit card information or user profiles, for personal gain or to sell on the black market.  External Threat: Credential Stuffing Attack - An external threat could involve attackers attempting to gain unauthorized access to user accounts by exploiting weak or reused passwords. They might use stolen credentials from other breaches to carry out a credential stuffing attack, potentially compromising user accounts and sensitive information.  *These threats pose risks to the confidentiality and integrity of user data within the application and need to be addressed through security measures and controls.* |
| **V. Vulnerability analysis** | In Stage V of the PASTA worksheet, here are two types of vulnerabilities that could be exploited in the sneaker company's app:  Insecure Data Transmission: One vulnerability could be related to insecure data transmission. If the application fails to properly encrypt sensitive data, such as credit card information, during transmission over the network, it could be intercepted by attackers, leading to potential data breaches.  SQL Injection: Another vulnerability that could be exploited is SQL injection. If there are weaknesses in the application's handling of SQL queries (e.g., not properly sanitizing user inputs), attackers might inject malicious SQL code, potentially gaining unauthorized access to the database, exposing or manipulating sensitive data, and compromising the application's security.  These vulnerabilities could result from issues in the codebase and database design and may be exploited by attackers to compromise the application's security. It's essential to conduct thorough vulnerability assessments and implement proper security measures to mitigate these risks. |
| **VI. Attack modeling** | To build an attack tree for the sneaker company's app, you would typically start with a root node representing the main goal of an attacker, such as "Compromise User Data." Then, you would branch out into various attack vectors and sub-vectors. Here's a simplified textual representation of what an attack tree might look like for this scenario:  Root Node: Compromise User Data  Attack Vector 1: Exploiting Insecure Data Transmission  Sub-vector 1.1: Intercepting Unencrypted Data  Sub-vector 1.2: Man-in-the-Middle Attacks  Attack Vector 2: SQL Injection  Sub-vector 2.1: Gaining Unauthorized Database Access  Sub-vector 2.2: Extracting Sensitive Data  Attack Vector 3: Insider Data Theft  Sub-vector 3.1: Malicious Employee Access  Sub-vector 3.2: Unauthorized Data Exfiltration  Attack Vector 4: Credential Stuffing Attack  Sub-vector 4.1: Exploiting Weak Passwords  Sub-vector 4.2: Reusing Stolen Credentials  Each of these branches represents a possible attack scenario or vector that could lead to the compromise of user data. Sub-vectors further detail the specific methods or techniques that attackers might use within each vector.  It's important to remember that attack trees can become quite complex, and they should be tailored to the specific application and its unique threat landscape. Additionally, mitigations and security controls should be mapped to each node and sub-node of the attack tree to indicate how these threats can be mitigated or prevented. |
| **VII. Risk analysis and impact** | Access Control: Implement strong access control mechanisms to restrict access to sensitive data and systems. This includes role-based access control (RBAC), two-factor authentication (2FA), and least privilege access policies to ensure that only authorized individuals can access critical resources.  Encryption: Employ strong encryption protocols for data both at rest and in transit. This includes using encryption algorithms like AES for data encryption and TLS/SSL for securing data during transmission over networks.  Intrusion Detection and Prevention Systems (IDS/IPS): Implement IDS/IPS solutions to monitor network and system activity for suspicious behavior and potential threats. These systems can help detect and prevent unauthorized access or attacks in real-time.  Security Patch Management: Establish a robust patch management process to regularly update and patch software, operating systems, and third-party components. Timely patching can address known vulnerabilities and reduce the risk of exploitation by attackers.  *These security controls, when properly implemented and maintained, can significantly reduce the risk of security incidents and enhance the overall security posture of an application, like the sneaker company's app, helping to protect user data from breaches and unauthorized access.* |