Mobile Application Threat Modeling

Threat modeling begins with a clear understanding of the system in question. There are several areas to consider when trying to understand threats to an application. The areas of concern include the mobile application structure, the data, identifying threat agents and methods of attack, and controls to prevent attacks. The threat model should be created with an outline or checklist of items that need to be documented, reviewed, and discussed when developing a mobile application.

In this project, you will create a threat model. There are seven steps that will lead you through this project, beginning with the scenario as it might occur in the workplace, and continuing with Step 1: “Describe Your Mobile Application Architecture.” Most steps in this project should take no more than two hours to complete, and the project as a whole should take no more than two weeks to complete.

The following are the deliverables for this project:

**Deliverables**

* **Threat Model Report**: An eight- to 10-page double-spaced Word document with citations in APA format. The report should include your findings and any recommendations for mitigating the threats found. The page count does not include figures, diagrams, tables, or citations.

Step 1: Describe Your Mobile Application Architecture

In your role as a cyber threat analyst, senior management has entrusted you to identify how a particular mobile application of your choosing conforms to mobile architecture standards. You are asked to:

1. Describe device-specific features used by the application, wireless transmission protocols, data transmission media, interaction with hardware components, and other applications.
2. Identify the needs and requirements for application security, computing security, and device management and security.
3. Describe the operational environment and use cases.
4. Identify the operating system security and enclave/computing environment security concerns, if there are any.

This can be fictional or modeled after a real-world application. This will be part of your final report. Click the following links and review the topics and their resources. These resources will guide you in completing this task:

* network security threats
* threat modeling
* mobile architectures
* application security
* operating system security
* enclave/computing environment

Begin by first reviewing the OWASP Mobile Security Project Testing Guide.

Architecture Considerations

Although mobile applications vary in function, they can be described in general as follows:

* wireless interfaces
* transmission type
* hardware interaction
* interaction with on device applications/services
* interaction with off device applications/services
* encryption protocols
* platforms

In Section 1 of your research report, you will focus your discussion on the security threats, vulnerabilities, and mitigations of the above considerations.

The following resources will continue to educate your management about mobile devices and mobile application security: mobile platform security, mobile protocols and security, mobile security vulnerabilities, and related technologies and their security. Related technologies can include the hardware and software needed to interoperate with mobile devices and mobile applications.

Include an overview of these topics in your report.

Use Mobile Application and Architecture Considerations to review the architectural considerations for mobile applications and architecture. Then, include those that are relevant to your mobile application in your report to senior management. Address the following questions:

1. What is the design of the architecture (network infrastructure, web services, trust boundaries, third-party APIs, etc.)?
2. What are the common hardware components?
3. What are the authentication specifics?
4. What should or shouldn't the app do?

You will include this information in your report.

When you have completed the work for Section 1, describing the architecture for your app, move on to the next step, where you will define the requirements for the app.

Step 2: Define the Requirements for Your Mobile Application

In the previous step, you described your app’s architecture. In Step 2, you will define what purpose the mobile app serves from a business perspective and what data the app will store, transmit, and receive. Include a data flow diagram to showing exactly how data are handled and managed by the application. You can use fictional information or model it after a real-world application. Here are some questions to consider as you define your requirements:

1. What is the business function of the app?
2. What data does the application store/process? (provide data flow diagram)
   1. This diagram should outline network, device file system, and application data flows
   2. How are data transmitted between third-party APIs and app(s)?
   3. Will there be remote access and connectivity? Read this resource about mobile VPN security, and include any of these security issues in your report.
   4. Are there different data-handling requirements between different mobile platforms? (iOS/Android/Windows/J2ME)
   5. Does the app use cloud storage APIs (e.g., Dropbox, Google Drive, iCloud, Lookout) for device data backups?
   6. Does personal data intermingle with corporate data?
   7. Is there specific business logic built into the app to process data?
3. What does the data give you (or an attacker) access to? Think about data at rest and data in motion as they relate to your app.
   1. Do stored credentials provide authentication?
   2. Do stored keys allow attackers to break crypto functions (data integrity)?
4. Are third-party data being stored and/or transmitted?
   1. What are the privacy requirements of user data? Consider, for example, a unique device identifier (UDID) or geolocation being transmitted to a third party.
   2. Are there user privacy-specific regulatory requirements to meet?
5. How do other data on the device affect the app? Consider, for example, authentication credentials shared between apps.
6. Compare between jailbroken (i.e., a device with hacked or bypassed digital rights software) and nonjailbroken devices.
   1. How do the differences affect app data? This can also relate to threat agent identification.

In this step, you defined the app’s requirements. Move to the next step, where you will identify any threats to the app’s operation.

Step 3: Identify Threats and Threat Agents

Now that you have identified the relevant requirements for your mobile app architecture and described the purpose and applicability of the app from a business perspective, you will define its threats in this step. Remember that it is your responsibility to present to senior executives about how integrating mobile app security into your strategy is essential to protecting your users and the overall network infrastructures.

In addition, your ability to identify threats and associated threat agents here is an important step to help you identify specific methods of attack, analyze mobile application threats, and discuss implementations of security controls in the remaining steps.

In Section 3 of the report, you will fulfill the following requirements:

* Identify possible threats and specific threat agents to the mobile application
* Outline the process for defining what threats apply to your mobile application

The major areas associated with these threat concepts are application vulnerabilities, server-side injection attacks, client-side attacks, secure coding principles, input validation, and applications hardening. Some common mobile app security threats that you should be aware of include reverse engineering, weak passwords, outdated encryption algorithms, and lack of multifactor authentication. However, it’s important to note that this list is by no means exhaustive. You would realize by completing this project that this is practically the case in real life.

An excellent source of information that is geared toward web applications security and that will help you complete this step is the Open Web Application Security Project (OWASP)—a nonprofit foundation that works to improve security of software applications. Particularly, the OWASP top 10 is a standard document for web application security awareness and represents a broad consensus about the most critical security risks to web applications (OWASP, 2021). In other words, the main goal is to provide specific details about web application security risks and mitigation strategies to prevent potential attacks.

To help you better appreciate threat model identification and mitigation strategies, review the following OWASP websites:

* Top 10 Web Application Security Risks
* Threat Modeling
* Threat Modeling Cheat Sheet

The OWASP standard awareness document throws more light on the OWASP Top 10 vulnerabilities list, including some common web application vulnerabilities an attacker might target — a critical component for the development of your project.

After you have identified threats and threat agents, move on to the next step, where you will consider the ways an attacker might compromise your app’s data.

Step 4: Identify Methods of Attack

In the previous step, you identified threat agents. In this step and in Section 4 of the report, you will identify different methods an attacker can use to reach the data. These data can be sensitive information to the device or something sensitive to the app itself.

Read these resources on cyberattacks.

Provide senior management an understanding of the possible methods of attack of your app.

When you have identified the attack methods, move to the next step, where you will analyze threats to your app.

Step 6: Consider Controls

You have identified the methods of attack, and now you will discuss the controls to prevent attacks. Consider the following questions:

**Note**: Not all of the following may apply. You will address only the areas that apply to the application you have chosen.

* What are the controls to prevent an attack? Conduct independent research and then define these controls by platform (e.g., Apple iOS, Android, Windows Mobile).
* What are the controls to detect an attack? Define these controls by platform.
* What are the controls to mitigate/minimize impact of an attack? Define these controls by platform.
* What are the privacy controls (i.e., controls to protect users’ private information)? An example of this would be a security prompt for users to access an address book or geolocation.
* Create a mapping of controls to each specific method of attack (defined in the previous step)
  + Create a level of assurance framework based on controls implemented. This would be subjective to a certain point, but it would be useful in guiding organizations that want to achieve a certain level of risk management based on the threats and vulnerabilities.

In the next step, you will complete work on the threat model.