MOBILE APPLICATION SECURITY GUIDE

From development to operations

pradeo

INDEX

INTRODUCTION

Mobile applications are the cornerstone of our mobile-first world. They are now a necessity for companies to communicate and offer services to their workforce, clients and partners. But with that necessity comes risk. Mobile apps are trusted with sensitive data, while not always being prepared to face the hostile environment they'll run in.

Indeed, mobile applications are cybercriminals favored vector to compromise smartphones, with 78% of data breaches on mobile originating from them. The mobile app attack surface is composed of malwares, representing the tip of the iceberg, and numerous silent leaky behaviors and vulnerabilities.

Today, governments and authorities are reinforcing the legal framework applying to mobility, with data protection laws that precisely require to protect mobile applications to prevent data theft and exfiltration. In the meantime, consumers are getting more concerned about how their personal information is handled, expecting companies to implement the means necessary to avoid their leakage.

Organizations releasing a mobile application are responsible for its protection across its lifecycle. Although, implementing the proper security practices at the right moment isn't always easy, as applications' time-to-market is often rushed by urgent business needs and are not conducted as thoroughly as developers and security teams want.

This guide goes through the risks an unsecure mobile app is exposed to, the legal framework it has to comply with and finally how to secure an app from development to operation stages.

Mobile application security is about delivering leakage free, vulnerability free, tamper proof and self-protecting mobile apps.

MOBILE APPLICATION ATTACK SURFACE

Mobile apps can feature a malware, hence being inherently malicious or they can be sane and either leak the data they manipulate or be vulnerable to attacks. In all these cases, and whether they are developed in-house or by third parties, mobile applications have the power to strongly hurt data privacy.

The statistics below are extracted from Pradeo's global mobile security report 2021.

Internal threats

Unexpected behaviors

A mobile application can perform unwanted actions because of the external libraries it hosts (79% of mobile applications embed third-party libraries) or as a result of a development negligence between testing and production. Both can lead to silent data leakage and potentially unwanted actions.

Vulnerabilities

A vulnerability comes from either the application's source code or from the libraries it hosts. To help developers, hundreds of code vulnerabilities are referenced by the US National Vulnerability Database, the OWASP mobile security project, US-CERT, etc. However, 57% of apps have vulnerabilities exposing them to data leakage and attacks such as Man-In-The-Middle, Denial of Service, etc.

External threats

Malwares

A malware is specifically designed to disrupt, damage, or gain access to a device or data. A malware's lifecycle has different stages: At first, its combination of functionalities is new and not classified in any antivirus database. Then, it starts getting recognition and is attributed with a name and a viral signature. To stay under the radar, cybercriminals keep renewing their malwares. 94% of the malwares detected by Pradeo Security in 2020 are unknown to antivirus databases.

Targeted attacks

Mobile applications can be specifically targeted by cybercriminals. It is often the case for mobile banking apps that are mimicked by banking trojan to coax users into providing sensitive details, or that are cloned and used to illicitly communicate with the bank's server.

Popular applications are also often cloned and tampered to create MOD (modified applications) that are copies of original applications to which code is injected by third-party/unofficial developers to unlock premium subscription and divert them to malicious activities.

MOBILE APPLICATION LEGAL FRAMEWORK

Organizations are expected to ensure the integrity and confidentiality of any sensitive data they process and transactions they perform. Mobile applications, as any other system processing sensitive information, are required to comply with data privacy laws and specific security standards enforced in highly regulated industries such as finance or healthcare. Here are some key requirements that apply to mobile applications.

Personal data

Personal data privacy regulations are in effect in various regions of the world, such as the GDPR (EU), FTC Act (USA), PIPEDA (Canada), DPA (UK), NDB (Australia), etc. These regulations tend to converge towards the same global guidelines, by asking organizations to protect personal data processed by mobile applications by:

- Deploying risk mitigation practices
- Implementing security in mobile application development cycles (privacy by design)
- Having visibility on personal data flows and their level of security
- Monitoring data processing activities

Financial data

The Payment Service Directive 2 (PSD2) is a European law dedicated to enforcing the security of mobile banking / payment applications, mobile wallets and all shopping apps that offer a payment functionality. It will be enforced in 2022 and requires developers to enable apps with:

- A strong authentication mechanism
- A mean to secure their execution environment

The Payment Card Industry Data Security Standard (PCI DSS) requires all merchants that use mobile payments to protect cardholder data by maintaining a secure environment, by:

- Protecting mobile devices against malicious programs
- Auditing and fixing mobile application's vulnerabilities

Health data

Laws regulating the healthcare sector are mostly domestic, such as the HIPAA (USA), HSCIC (UK), CNIL (France), etc. Most of them share the same key guidelines and require to:

- Regularly review information system activities
- Implement solutions to detect and mitigate security incidents (including malicious software)
- Alert in case of security incident

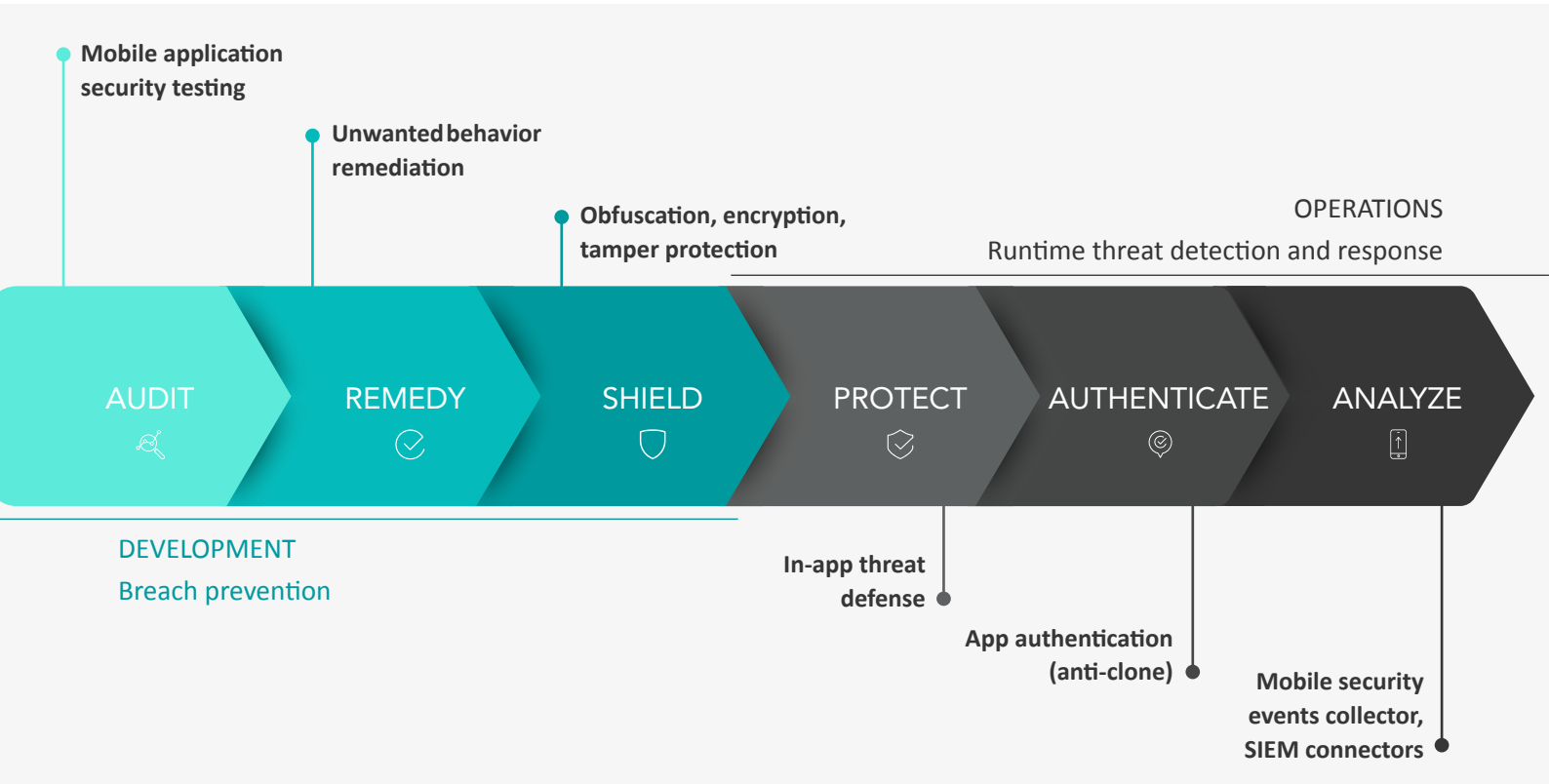
SECURING A MOBILE APPLICATION

To protect an application, every step of its lifecycle must be handled with a security perspective, from its development to operations: this is what is called a **DevSecOps approach**. Failing to secure one of the steps of an application's lifecycle endangers all the others and cancels the benefits of the security measures implemented.

The timeline below gathers the security needs of a mobile application through its life, combined with the services that meets them.

pradeo

Pradeo's **mobile application security platform** supports teams' DevSecOps approach by **centralizing various AppSec services** to fully secure mobile applications from development to operations.



SECURING A MOBILE APPLICATION

1 Development
Breach prevention

Audit your mobile application security

Before releasing a mobile application, organizations must ensure it does not embed any unwanted behavior or vulnerability that jeopardizes its privacy. **Mobile Application Security Testing (MAST)** solutions audit mobile apps for potential internal threats and conclude on their security level against a chosen security policy. Many MAST solutions are available on the market, making it difficult for security teams to make a comparison. Here are the key functionalities to aim for, associated to the needs they answer.

Organization's need		Functionality required
Compliance	Monitoring of compliance with data protection laws and industry standards.	• Identification of data manipulation per type • Non-compliance flagging
Accuracy	Identifying behaviors (data sending, connection...) and vulnerabilites.	• Static, dynamic and behavioral analysis • Vulnerability assessment • Third-party library analysis
Flexibility	Adaptability to any context's requirement and obligation.	• Customizable security policy • One tool for both Android and iOS
Ease of use	Responsiveness and smooth integration into the development environment.	• Ready-to-use online platform • Integration APIs (CI/CD)

Pradeo's Mobile Application Security Testing tool is recognized as market leader in **IDC MAST MarketScape** and **Gatner MAST Market Guide.** Learn more about Pradeo's MAST service in this datasheet

SECURING A MOBILE APPLICATION

Remedy unwanted behaviors

Once the audit phase has highlighted all the unwanted behaviors performed by an application, the logical next step is to correct them. To ease the remediation phase, MAST tools provide detailed security reports that are more or less exhaustive according to the vendor. Here are a few options and functionalities to look for in MAST services to facilitate this remediation phase.

Organization's need		Functionality required
Structure	Well-organized report providing visibility on key security points.	• Detection of behaviors • Identification of vulnerabilities • Precise classification
Guidelines	Actionable recommendations to correct unwanted behaviors and vulnerabilities.	• Indicators of criticality • Explanation of detected flaws
Automation	Automatic remediation according to defined security levels.	• Automatic remediation feature • Customizable security policy

Pradeo's Mobile Application Security Testing tool provides **detailed security reports**, patching **recommendations** and an **automatic remediation service**.

Learn more about Pradeo's MAST service in this datasheet

SECURING A MOBILE APPLICATION

Shield the code of your mobile application

Application shielding plays its part primarily in the **prevention of attacks** by making it extremely complex to understand, decipher and penetrate the code of an application. This phase consists in using a combination of techniques to prevent an application's code from being cloned, injected with code and tampered. Application shileding is essential to ensure the safety of an application at runtime.

Organization's need		Functionality required
Code secrecy	Protection of my application's intellectual property by preventing reverse-engineering	• Obfuscation • Encryption
Fraud prevention	Neutralization of clones and fake applications mimicking my application	• Anti-tamper features
Time	Ready-to-use shielding services with no development involved	• One-click shielding, from application's executable file (no source code)

Pradeo provides an **application shielding service** that combines the latest **obfuscation, encryption and anti-tamper techniques**.

Learn more about Pradeo's application shielding in this datasheet

SECURING A MOBILE APPLICATION

2 Operations
Runtime threat detection and response

Protect mobile application runtime

If not properly prepared to face external threats, an application does not resist to attacks and eventually leaks the data it manipulates or worst, provides an access to the information system it is connected to. It is recommended to embed an **In-App Threat Defense SDK** in mobile applications so they can autonomously respond to threats evolving in their execution environment.

Organization's need		Functionality required
App authentication	Confirmation that the application communicating with the server is the right one.	• Token authentication
Threat detection	Detection of all types of mobile threats, coming from applications, the network and the OS.	• App behavioral analysis • Network monitoring • OS integrity check
Automation	Automatic threat responses to prevent data theft and leakage.	• Automatic security checks • Reliable threat detection
Optimal UX	Ensure a smooth and enjoyable user experience.	• Low battery consumption • Background security checks

Pradeo's **In-App Threat Defense** SDK protects mobile applications' data and sessions by detecting threats operating on users' devices and responding accordingly, in real-time.

Learn more about Pradeo's In-App Threat Defense SDK in this datasheet

SECURING A MOBILE APPLICATION

Monitor surrounding cyberthreats

Each company has its own mobile threat landscape. As a result, the most efficient security measures are the ones customized to this specific environment. By monitoring threats surrounding and targeting their own application, organizations can get powerful mobile threat intelligence, deploy relevant countermeasures and perform effective incident investigation.

Organization's need		Functionality required
Data collection	Collect anonymous security events from the pool of users.	• Mobile security event collector • SIEM connectors
Threat Intelligence	Create evidence-based knowledge and actionable intelligence about existing or emerging threats.	• Access to current data • Detailed security reports • Comprehensive dashboards

Pradeo's **Mobile Security Event Collector** has **can be connected to the following SIEM: I**BM QRadar, Splunk, ArcSight, LogRythm, SmartEvent, RSA, McAfee, Fortinet and AlienVault.

Learn more about our mobile security event collector in this article

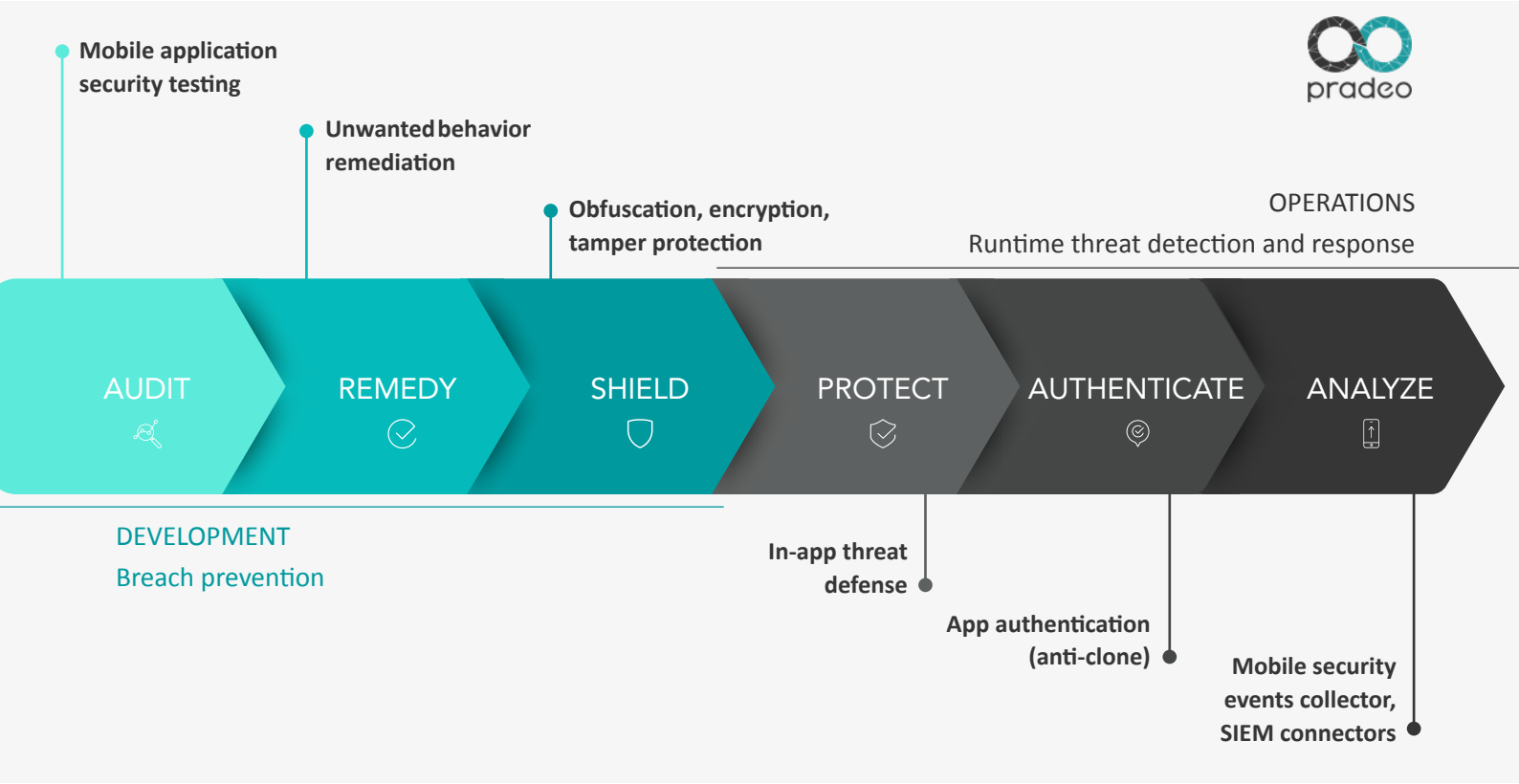
ABOUT pradeo

Pradeo is a global leader of mobile security, with **10+ years of experience in mobile application security.** The company ensures the protection of all mobile usages, by offering services dedicated to securing applications and devices.

Pradeo's AI-based technology, Pradeo Security, is recognized as one of the most advanced mobile security technologies by **Gartner, IDC, Frost & Sullivan and Forrester.** It provides a reliable protection from mobile threats to prevent data leakage and reinforce compliance with data privacy regulations.

Pradeo's mobile application security platform **supports teams' DevSecOps approach** by centralizing various AppSec services to fully secure mobile applications from development to operations.

REINFORCE YOUR DEVSECOPS INITIATIVE WITH **PRADEO'S APPSEC TOOLKIT**



In 2021, Frost & Sullivan recognized Pradeo Security with the **"Best global mobile security enabling technology award".** More details in the analyst report.