WHITE PAPER

# MOBILE BANKING

## REGULATIONS, THREATS & FRAUD PREVENTION

pradeo

# INDEX

# MOBILE BANKING USAGES

**79%**

**of US internet users had downloaded their bank's mobile application in 2017**

**50%**

**increase in mobile banking usage from 2017 to 2018**

**91%**

**of mobile banking users prefer using their app over going to a physical branch**

Mobile banking is a 24/7 remote service offered by banks and financial institutions to their clients. It is delivered through **mobile applications** and allows to monitor account balances, follow transactions, make fund transfers, etc. Mobile banking is widely implemented in the financial industry as it lowers the amount of customers visiting local branches, hence reducing overall expenses.

The mobile banking service has quickly been embraced by consumers, as 79% of US internet users had downloaded their bank's mobile application in 2017, according to a study by Market Force Information. In 2018, **Mobile banking usage keeps skyrocketing** with a nearly 50% increase in usage year over year, according to The Citi Mobile Banking Survey. Furthermore, the survey state that 91% of mobile banking users prefer using their applications over going to a physical branch.

**With 2 billion users forecasted by 2020, mobile banking logins are becoming more significant than web logins**

Increasing mobile banking adoption and customer expectations put banks under pressure and the question is no longer to offer an application, but to **feature cutting-edge services** and ensure the best **protection from data theft and fraud**. To stay ahead of the competition, major banks as well as community banks and credit unions quickly developed their mobile applications, which they frequently update with new capabilities.

One of the main causes of mobile application breaches is **internal flaws**. Banking applications have an **average of 20 vulnerabilities**, coming from either the source code of the application itself or from a library it embeds. Hundreds of code vulnerabilities are referenced by the US National Vulnerability Database, the OWASP mobile security project, US-CERT, etc. Such flaws expose applications to data leakage and attacks such as Man-In-The-Middle, Denial of Service, etc.

The other main cause compromising mobile application is the lack of adapted security measures to face **environmental threats**. In 2017, the Pradeo Lab carried out a study aiming at assessing mobile banking security by analyzing randomly 50 banks' mobile application ranked among the TOP 100 worldwide banking establishment. All together, the 50 Android and iOS applications covered 22 countries and half a billion users.

Our researchers challenged the banking applications using twenty techniques, from sophisticated to basic ones, commonly used in cyberattacks targeting mobile devices. The results were unequivocal: 100% of the applications failed the test. At that time, none of the mobile banking applications analyzed was able to resist the mobile threats frequently found on users' devices.

> **We studied 50 banks' mobile application ranked among the TOP 100 worldwide banking establishment. None of them was able to resist the mobile threats frequently found on users' devices.**

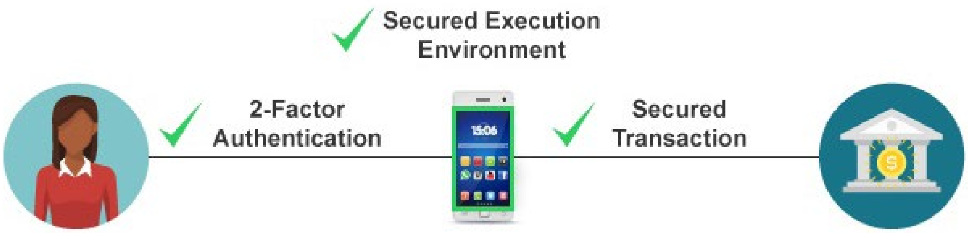
# MOBILE BANKING REGULATORY FRAMEWORK

Mobile banking involves the manipulation of sensitive data (financial, personal…) by a mobile application. At a time where governments and authorities around the world highly promote personal data protection and start regulating the mobile banking field specifically, mobile banking applications are required by law to satisfy a number of criteria.

## Regulations specific to mobile banking

In **Europe**, the second Payment Service Directive (PSD2) and its associated Regulatory Technical Standards (RTS) have been published by the European Banking Authority and validated by the European Parliament in early 2018. The new directive aims at harmonizing the protection of electronic payments and consumers' financial data while promoting innovation and offering better experience to users. RTS's articles 4, 7, 8 and 9 require, inter alia, Europe's banks, payment service providers (PSP) and any other company that handles financial data to:

- Implement strong authentication
- Secure the execution environment



In the **USA** unlike in other G10 countries, banking is regulated at both Federal and State level. The Federal Financial Institutions Examination Council (FFIEC) is the US government interagency body that promotes uniformity in the supervision of financial institutions. Recently, it has issued an appendix to the Retail Payment Systems booklet of the FFIEC Information Technology Handbook dedicated to mobile banking, called "Mobile Financial Services". The section 5.B of the appendix advises, inter alia, organizations to mitigate mobile applications' risks by:

- Implementing strong authentication (§2)
- Rigorously testing for vulnerabilities (§3)
- Embed anti-malware capabilities (§3)
- Tracking security changes and anomalous behaviors (§7)

# MOBILE BANKING REGULATORY FRAMEWORK

## Regulations specific to personal data privacy

Financial institutions' mobile applications, as they handle personal data, are controlled by personal data privacy regulations such as the GDPR (Europe), FTC Act (USA), PIPEDA (Canada), DPA (UK), etc. These regulations tend to converge towards the same global guidelines, by asking organizations to:

- Protect data
- Implement risk mitigation practices
- Prevent data loss and breach
- Monitor data processing

Some of these laws provide massive fines in case of non compliance. For example, the credit reporting agency Equifax was fined of £500,000 over its 2017 data breach by the UK Information Commissioner's Office.

***As every country has its own mobile banking and personal data privacy rules, this list is not exhaustive and it is advised to get acquainted with any local laws that may apply.***

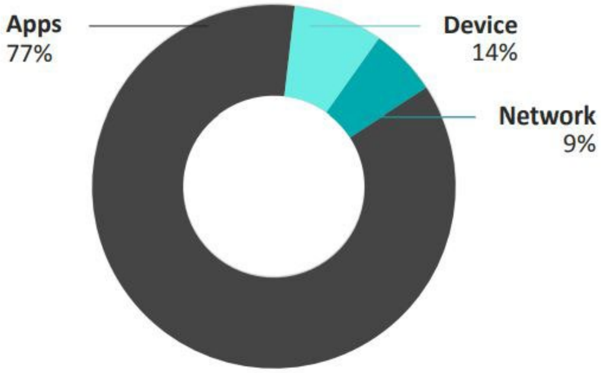
The Data Protection Act
The Act on the Protection of Personal Information
The Personal Information Protection and Electronic Documents Act
GDPR
Health Insurance Portability and Accountability Act
The Payement Card Industry Data Security Standard
Notifiable Data Breach scheme
Federal Trade Commission Act

# ENVIRONMENTAL THREATS TARGETING MOBILE BANKING

Fraudsters target the mobile banking industry and financial data through three potential vectors: Applications (malware, spyware, adware…), the network (Man-In-The-Middle attack…) and the device (OS vulnerabilities exploitation…).

There are plenty of techniques used to compromise mobile banking applications, from the most common ones to the unknown “0-days”. **Here is the presentation of 5 of the most common threats lurking on mobile banking applications.**

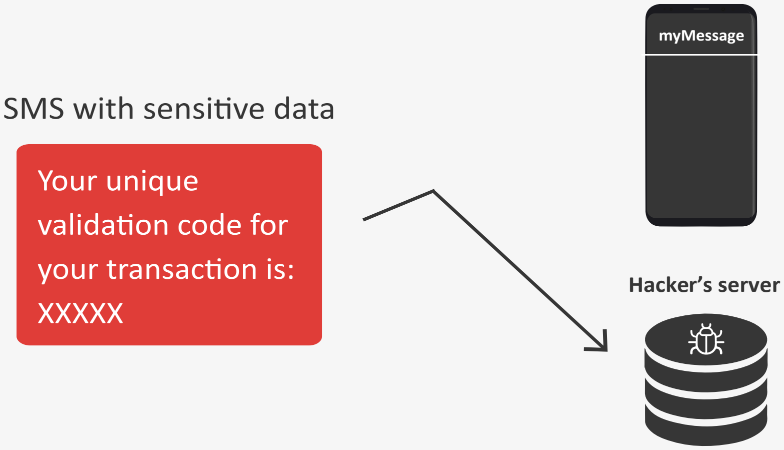
**The current repartition of mobile threat vectors:**



## OTP Interceptor

Most online transactions require a two-step authentication, and the One-Time-Password (OTP) sent by SMS is often one of those two steps. The purpose of an OTP is to prevent fraud by confirming that the person making the transaction and the credit card owner are one and the same. To do so, a temporary code is automatically sent by SMS to the phone number associated with the bank account used. Once the OTP SMS is received, the user types it in the transaction interface and he is only then able to finalize his purchase.

Regrettably, this authentication process is nowadays easily bypassed by malicious mobile applications that intercept OTP in order to commit banking fraud.



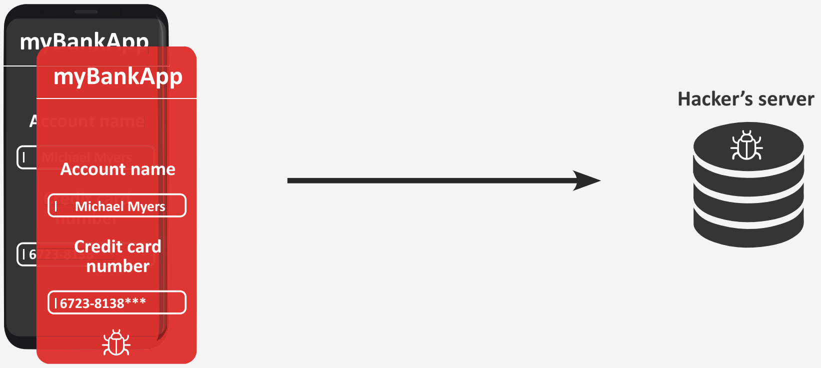
Your unique validation code for your transaction is: XXXXX

# ENVIRONMENTAL THREATS TARGETING MOBILE BANKING

## Overlay

An overlay malware allows attackers to create an overlay to be displayed on top of legitimate Android applications. The overlay mimics the real app user interface to trick users into entering sensitive data into a fake window that will collect and forward them to a remote attacker.

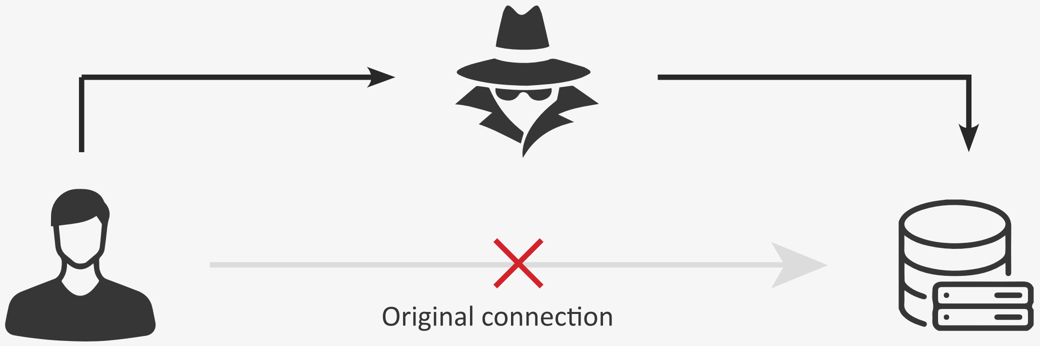
Overlay attacks only affect Android devices by using the SYSTEM_ALERT_WINDOW permission, which is sometimes automatically granted when applications are downloaded from the Play store. Their main purpose is to secretly steal financial credentials to commit fraud.



## Man-In-The-Middle

A Man-In-The-Middle attack happens when a communication between two parties is intercepted by an outside entity. The perpetrator either eavesdrops on the communication or impersonates one of the two parties, making it appear as a regular exchange of data.

A MITM attack targets users of business email accounts, financial applications, e-commerce websites in order to steal account details, credentials, bank account or credit card numbers. The final purpose is to perform identity theft, illicit money transfers or password modifications.

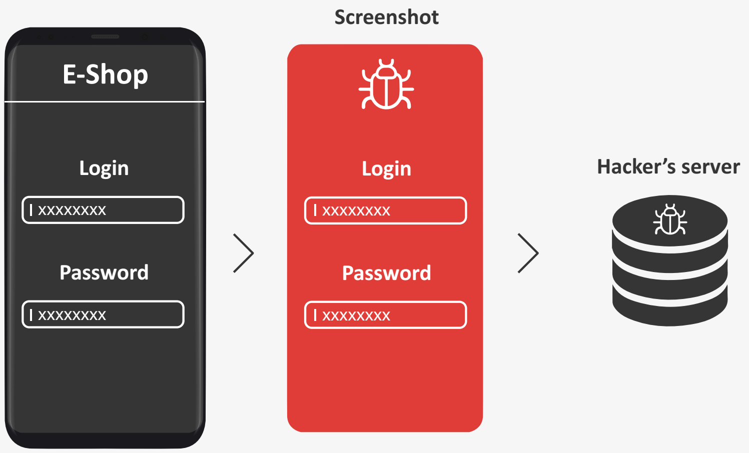


## Keylogger and Screenlogger

A keylogger malware records the content typed on a keyboard, via the original one or via its own keyboard displayed on top of the real one. On the other hand, a screenlogger records what's displayed on the mobile device screen.

Then, both send the data retrieved to a distant server owned by the hacker. Most of the time, these malwares are silent and users are unaware that their data are being exfiltrated.

Keyloggers and screenloggers are widely used to steal credit card details and banking credentials.



# CONSEQUENCES OF MOBILE BANKING COMPROMISE

## Regulations non-compliancy

Most data privacy regulations require companies to communicate to the authorities and to the users about any security breach that happened on the data they collect and manipulate. The authorities are then in a position to potentially fine the financial organizations.

## Data leakage

When hackers attack mobile banking, they intercept the data initially collected by the bank through their application, causing a data breach that the financial institution is responsible for, according to the law.

## Financial loss

When banking data are stolen, hackers' main purpose is to monetize the theft by committing fraud. As a result, it causes great financial loss to the bank.

## Reputational damages

When a mobile application leaks the data it handles, it usually ends up in the news and its users get worried about the privacy of their own data, resulting in a drop in users trust.

# RUNTIME APPLICATION SELF-PROTECTION TO WARD OFF ENVIRONMENTAL THREATS

Security heads are looking for solutions that will prevent their mobile banking applications from being attacked and breached, while maintaining users agility.

Pradeo Security Runtime Application Self-Protection (RASP) technology was designed to protect mobile applications from the wide spectrum of mobile threats. It comes as a ready-to-use SDK to be embedded within an application source code. Once set, it detects threats running on end-users mobile devices and offers a real-time protection from malwares and data leakage.

Additionally, Pradeo Security RASP solution collects mobile security data to enrich SIEM databases with precise and current threat intelligence.

Several companies of the Fortune 500 trust Pradeo Security Application Self-Protection and Threat Intelligence module to proactively protect their mobile banking applications and to reinforce their compliance with data protection regulations.

## Benefits of Pradeo Security Runtime Application Self-Protection

### 360° PROTECTION

Pradeo Security self-protection SDK protects sensitive applications from attacks and ''zero-day'' threats coming from applications, the network or the device.

### THREAT INTELLIGENCE

Pradeo's RASP SDK acts as a threat intelligence module by collecting mobile security data to enrich SOC and SIEM databases and improve threats knowledge and management.

### FRAUD PROTECTION

By detecting threats on-device prior to executing any transaction, Pradeo Security in-app self-protection prevents mobile fraud.

### OPTIMAL USER EXPERIENCE

The Pradeo Security module performs transparent security checks and has no impact on the battery consumption, ensuring a seamless protection of users.

### PRIVACY LAW ENFORCEMENT

Pradeo helps organizations to comply with data protection regulations by protectings mobile applications from data leakage and breach.

### QUICK IMPLEMENTATION

Pradeo's SDK is ready-to-use and can be embedded within any app source code in a couple of hours, with no further update required and a fully remote management.

## Explore further

Datasheet - Pradeo Security RASP

# MOBILE APPLICATION SECURITY TESTING TO ELIMINATE INTERNAL FLAWS

Before publishing their mobile banking application on public stores, financial institutions must test their security levels and correct their flaws.

Pradeo Security Mobile Application Security Testing solution allows organizations to precisely audit their mobile applications security levels by identifying all their behaviors and vulnerabilities. Then, it offers to remediate unwanted behaviors and provides detailed advises to eliminate vulnerabilities.

Furthermore, integrating a security testing phase to the application development cycle mitigates risks, as required by data privacy laws.

## Benefits of Pradeo Security Mobile Application Security Testing

### READY-TO-USE

Pradeo Security is available in SaaS, On Premise or as an API to integrate within the development environment. It only requires applications binary code to run an analysis, no source code is required.

### BEHAVIORS DETECTION

Pradeo Moble Application Security testing automatically performs the most trustworthy static and dynamic analysis to identify and qualify all malicious and unwanted behaviors.

### VULNERABILITIES DETECTION

Pradeo identifies all the vulnerabilities referenced by the US National Vulnerability Database, the OWASP mobile security project, US-CERT, etc. as well as many internal ones. Then, it provides clear corrective actions.

### REMEDIATION

Pradeo Security automatically remedies applications unwanted behaviors. In one click, it repackages applications according to the security policy.

### UNIVERSALITY

Pradeo is compatible with Android, iOS and Windows UI to allow organizations to carry out all their tests within one unified tool.

### CUSTOMIZATION

A good security policy must suit organizations requirements. Pradeo allows its administrators to personalize their security policy so it entirely fits their context.

## Explore further

Datasheet - Pradeo Security MAST

# PRADEO SECURITY SECURES THE MOBILE CHAIN

Pradeo developed Pradeo Security, a patented mobile security technology that uses artificial intelligence and machine learning to automatically ward off known, unknown and advanced mobile threats. Pradeo Security has been recognized by major research firms such as Gartner, IDC, etc.

Pradeo's solutions suite offers a complete and automatic protection of the data manipulated by mobile devices and applications, aligned with organizations' security policy, while preserving business agility.

## One Technology to Master Application & Endpoint Security

The technology

**PRADEO SECURITY**

### Unknown & advanced threat detection

Our behavioral engine detects brand new and advanced threats to ensure 0-day protection.

### Customizable security

Pradeo's solutions are highly customizable to allow each company to implement its own security levels.

### Limitless coverage

Our technology is entirely flexible and is compatible with Android, iOS, Windows and BYOD workforce.

### MOBILE APP SECURITY

**Mobile App Security Testing**

**Runtime App Self-Protection**

### MOBILE ENDPOINT SECURITY

**Mobile Threat Defense**

# PRADEO STRATEGIC TECHNICAL ALLIANCES

Pradeo is partnering with mobility key players:

airwatch by vmware

BlackBerry

IBM MaaS360

MobileIron

Microsoft

SAMSUNG

SOTI

## For more information

**www.pradeo.com**

**contact@pradeo.com**