The State of Mobile Finance App Security

2021

ZIMPERIUM®

Introduction

Dramatic changes last year drove organizations and consumers to change the way they conduct all types of financial business. With offline interactions curtailed by the COVID-19 pandemic, use of finance mobile apps and other digital channels skyrocketed across the globe.

According to Fidelity National Information Services, new mobile banking registrations jumped by 200% in April 2020 alone.[1] During the past year, time spent in finance apps increased by 45%,[2] activity in investment apps increased by 88%,[3] and mobile wallet point-of-sale transactions picked up by 19.5%, helped by higher limits for contactless payments.[4]

As organizations scrambled to meet the surge in demand, cybercriminals took advantage. In June, the FBI issued an alert about an increase in attacks on mobile finance applications including banking trojans and fake/cloned banking apps.

The rapidly evolving threat landscape makes it critical for financial institutions to prioritize their mobile application security. Fintech firms realize this on some level. A Verizon survey found that 92% of financial services companies say organizations need to take mobile security more seriously. Yet 43% knowingly sacrificed mobile security to meet a deadline or productivity target—despite a slew of new or updated security regulations set to hit in 2021.[5]

How well-equipped are today's mobile finance apps to tackle these ongoing challenges? To understand the greatest threats to financial application security globally, Zimperium looked at a cross-section of mobile apps, including contactless payment apps, across multiple geographies. This report presents the results of that analysis, along with strategies to help finance app developers and organizations mitigate vulnerabilities and risk.

Key Findings

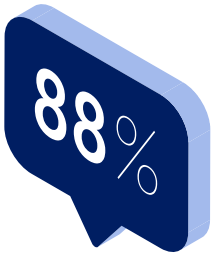
The assessment uncovered serious security gaps in mobile finance apps across the board and in every region.

1

of apps have at least one critical or high severity vulnerability

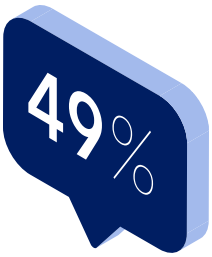
2

of finance apps leak data



3

of apps fail cryptographic tests



4

of payment apps are vulnerable to encryption key extraction

5

UK finance apps contain the fewest critical vulnerabilities

6

Banking apps contain more vulnerabilities than any other type of finance app

7

Nearly 3/4 of high severity threats could have been mitigated using in-app protection

The State of Financial App Security

The global pandemic greatly accelerated the pace of mobile finance app adoption. Mobile payments, in particular, have been propelled years ahead of projections.[6]

In the charge toward a mobile-first strategy, however, many financial organizations defer application security until the final lap. At best, this can derail progress. At worst, it leaves security gaps that bring serious consequences. Cybercriminals exploit vulnerable apps to steal user credentials and personal information, access customer financial assets, or even insert backdoors into an organization's enterprise systems.

This not only opens organizations to risk of theft of funds and regulatory fines, it can impact customer acquisition and retention too. While the pandemic drove customers to digital channels, 41% of mobile banking users still express a high degree of concern over illegal use of personal and account information and 38% over fraudulent fund transfers. App security breaches may push these customers to other providers or to abandon these channels altogether once health safety no longer shapes their behavior.

Mobile Device Risks

Many mobile devices contain hardware-based security mechanisms such as embedded cryptographic processors or trusted execution environments (TEE). However, they are not always available and a lack of standardization across TEEs means that security levels vary from device to device. Hardware-backed also doesn't mean impenetrable. Attackers can use differential power analysis (DPA) or other side channel attack methods to extract keys.

Moreover, serious mobile OS security flaws constantly come to light. In the first quarter of 2021 alone, Google patched 121 critical and high severity vulnerabilities in its Android operating system.[7] During the same time period, Apple fixed 54 iOS security issues.[8] And in July 2020, a hacking group discovered a permanent vulnerability in the Apple Secure Enclave chip, which could put encryption keys at risk.[9]

Jailbroken or rooted devices pose another significant threat. Finance app providers have no control over the device their application is installed on and once a device is jailbroken or rooted, OS-level security controls are compromised and things like crypto keys can be read in the clear if a zero-trust model was not anticipated and implemented as part of your security posture.

Financial App Threat Landscape

Malware targeting mobile finance applications remains one of the fastest growing and rapidly-evolving cyber threats. In 2020, 156,710 new mobile banking trojans were detected, more than doubling over the previous year.[10]

Many of these played off pandemic fears. Multiple fake COVID contact-tracing apps delivered SpyNote and Anubis banking trojans. Once installed, Anubis injects an overlay that sits on top of the banking app and captures banking credentials, PIN data,[11] and other valuable personal data. Cryptocurrency-themed attacks were also popular, some targeting crypto wallets, others installing general banking malware, such as a Google Play store-sanctioned cryptocurrency converter that distributed the Cerberus trojan.[12]

Mobile finance threats also continue to grow more sophisticated, incorporating new techniques to steal data while avoiding detection by security tools. For example, the new Ghimob banking trojan identifies and monitors the installed finance apps on a device, captures device and account info by exploiting accessibility features, and, when ready, performs the fraudulent transaction in the background while the user looks at an overlay screen. By hijacking the device, it evades machine identification and anti-fraud security measures implemented by financial institutions.[13]

Emulators that spoof devices to access apps pose another threat. In late 2020, a cybercrime gang stole millions of dollars from financial institutions in the U.S. and Europe by using stolen data and emulating account holders' mobile devices to complete fraudulent transactions.[14]

Fake or cloned banking apps also remain in play as an attack vector. Genuine applications are reverse-engineered to get the source code, tampered with to create a malicious version, repackaged, and distributed through counterfeit websites or posted in app stores. Once installed, they open with a form to capture login credentials or bank card details, and ultimately steal funds.

Financial App Security Risks

Finance organizations may not be able to control the environments their apps run in or the threats cybercriminals churn out but they are in charge of their application code. The Open Web Application Security Project (OWASP) maintains a list of the top ten mobile app vulnerability types that pose the greatest security risks for organizations and users.[15] Insecure coding and app security practices can lead to data leakage, insecure communications, authentication and authorization issues, weak cryptography, and susceptibility to code tampering and reverse engineering. These create openings for attackers to steal personal and financial information, exfiltrate crypto keys, inject malware into the app, and hijack app processes. The vulnerabilities tested in our analysis all fall under one or more of these OWASP risk categories.

OWASP Mobile Top 10 Risks

Many mobile devices contain hardware-based security mechanisms such as embedded cryptographic processors or trusted execution environments (TEE). However, they are not always available and a lack of standardization across TEEs means that security levels vary from device to device. Hardware-backed also doesn't mean impenetrable. Attackers can use differential power analysis (DPA) or other side channel attack methods to extract keys.

Moreover, serious mobile OS security flaws constantly come to light. In the first quarter of 2021 alone, Google patched 121 critical and high severity vulnerabilities in its Android operating system. During the same time period, Apple fixed 54 iOS security issues. And in July 2020, a hacking group discovered a permanent vulnerability in the Apple Secure Enclave chip, which could put encryption keys at risk.

Jailbroken or rooted devices pose another significant threat. Finance app providers have no control over the device their application is installed on and once a device is jailbroken or rooted, OS-level security controls are compromised and things like crypto keys can be read in the clear if a zero-trust model was not anticipated and implemented as part of your security posture.

M1	**Improper platform usage**
M2	**Insecure data storage**
M3	**Insecure communication**
M4	**Insecure authentication**
M5	**Insufficient cryptography**
M6	**Insecure authorization**
M7	**Client code quality**
M8	**Code tampering**
M9	**Reverse engineering**
M10	**Extraneous functionality**

How Secure are Today's Financial Apps?

With the pandemic accelerating the use of mobile financial applications globally, and the accompanying rise in attacks on these apps, mobile app security should be a top priority for organizations.

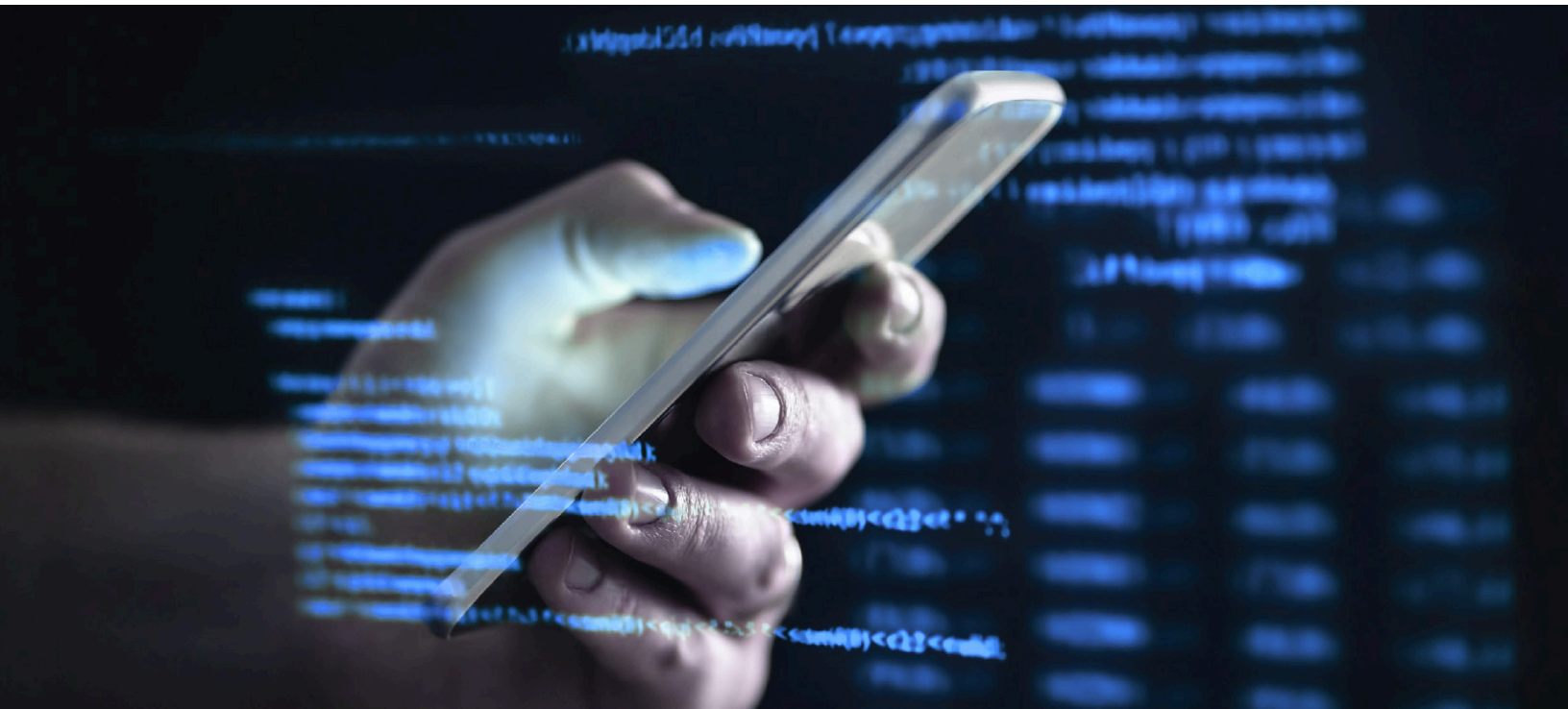
This study evaluated applications from 5 countries or regions—the United States, India, the United Kingdom, the European Union, and Southeast Asia—to determine the security level of financial apps worldwide and their resilience to cyberthreats.

What was Tested

Security assessments were conducted on 160 publicly available mobile financial services apps from four major categories: banking, mobile payment, investment/trading, and lending. All apps were downloaded directly from their respective stores (Apple Inc.'s App Store® and Google Play™) and selected based on the number of downloads and size of the organization.

Apps were analyzed using both static application security testing (SAST) and dynamic application security testing (DAST), based on OWASP guidelines.

Threats were classified as Low, Medium, High, and Critical according to the Common Vulnerability Scoring System (CVSS). See the Appendix for classification details and a complete list of tested vulnerabilities.



Top Significant Threats Detected

Although nearly every type of vulnerability was detected in multiple apps, some threats stood out in terms of severity, prevalence, or both.

Vulnerability	Why it matters	OWASP category	Potential PCI-DSS violation	Percent of tested apps affected
Storing unencrypted information in Shared Preferences	Shared Preferences are a set of APIs in Android that allow apps to store and retrieve data from the device. Unencrypted sensitive information should never be stored in Shared Preferences as the data is readily readable and editable by attackers and malicious apps.	M2: Insecure Data Storage	Sections 3.2, 3.3, 3.4 regarding protection of stored cardholder data	73% of Android apps
Weak derived crypto keys	The predominant Android Java Security API defaults to using ECB block cipher mode for AES encryption, which is considered less secure than other methods as it results in the same ciphertext for identical blocks of plain text. Developers that rely on the default OS-provided encryption process run the risk of information and code theft.	M5: Insufficient Cryptography	Sections 3.5, 3.6 regarding protection of stored cardholder data	61% of Android apps
Disabled SSL CA validation and certificate pinning	Pinning associates a host with their expected X.509 certificate or public key. The most secure certificate pinning method adds the certificate or public key to the application at development time. If certificate pinning is poorly implemented, attackers can use false credentials to access traffic between the application and the web server and steal confidential data.	M3: Insecure Communication	Section 4.1 requiring strong encryption for authentication and transmission of cardholder data across public networks	60% of Android apps
Misconfigured App Transport Security (ATS)	ATS is an iOS networking security feature that ensures network connections employ the most secure protocols and ciphers. When used incorrectly, data can be intercepted and exploited.	M3: Insecure Communication	Section 4.1 requiring strong encryption for authentication and transmission of cardholder data across public networks	65% of iOS apps
Insecure data storage in iOS apps	This is actually a combination of several vulnerabilities. We found multiple instances of iOS apps storing sensitive data in places that do not have built-in support for encryption. This means sensitive information is being stored in plain-text unless custom encryption mechanisms, such as white-box cryptography, are being used. If the local device is compromised then the stored data is easily compromised.	M2: Insecure Data Storage	Sections 3.2, 3.3, 3.4 regarding protection of stored cardholder data	iOS apps storing sensitive information in: NSUserDefaults-61% Property Lists-55% SQLite3 databases-46%

Detailed Findings

Every app tested had at least one basic security issue. Diving in deeper, 88% had cryptographic issues, 81% can leak data, and 77% contained flaws that present high-level risks to finance organizations and their customers. These findings suggest that increased attention on cybersecurity risks and tightened regulations have not translated into secure mobile finance apps. Applications in all four finance categories displayed widespread insecure coding practices along with a general lack of application security controls and in-app technology protections, such as application shielding, runtime application self-protection (RASP), and white-box cryptographic key protection.

We found differences in security level of app types as well as significant disparities between regions. However, we should be cautious in making any firm conclusions regarding regional characteristics as there was not 100% parity in app types tested. For example, the testing samples from the EU included more payment apps than other regions, whereas the sample from India contained more apps that fell in the trading category. Nevertheless, these discrepancies cannot account for the quite dramatic regional differences.

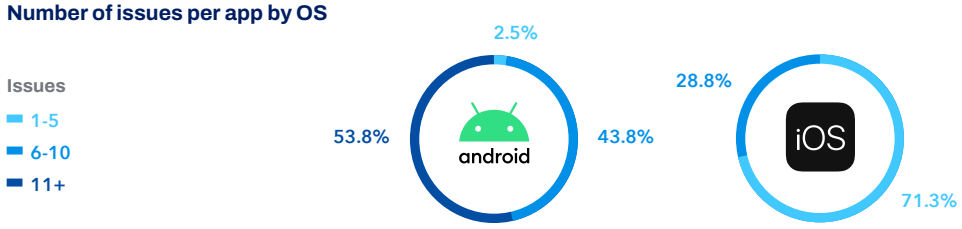
App security by OS

Many organizations assume iOS is an inherently more secure platform than Android but Android's greater popularity among users and attackers alike makes comparisons murky.

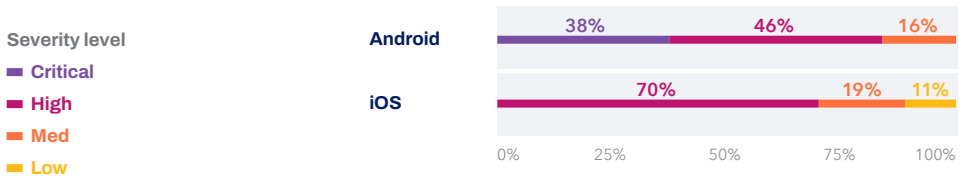
What's unquestioned is that both rank in the top ten most vulnerable operating systems for total number of distinct vulnerabilities. Developers cannot rely on OS protections to keep their apps secure on either platform, particularly as jailbreaking and rooting remain prevalent.[16]

In our testing, Android apps had far more issues than iOS apps. On a per app basis, nearly every Android finance app (97.5%) had more than five security flaws compared to around 30% of iOS apps. When looking at severity level, however, the gap narrows. Approximately 84% of Android finance apps contained at least one critical or high severity vulnerability versus 70% of iOS apps.

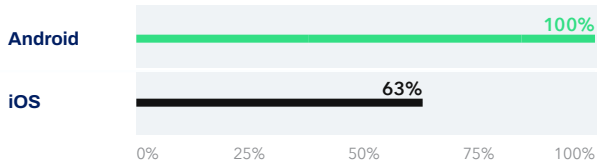
Number of issues per app by OS



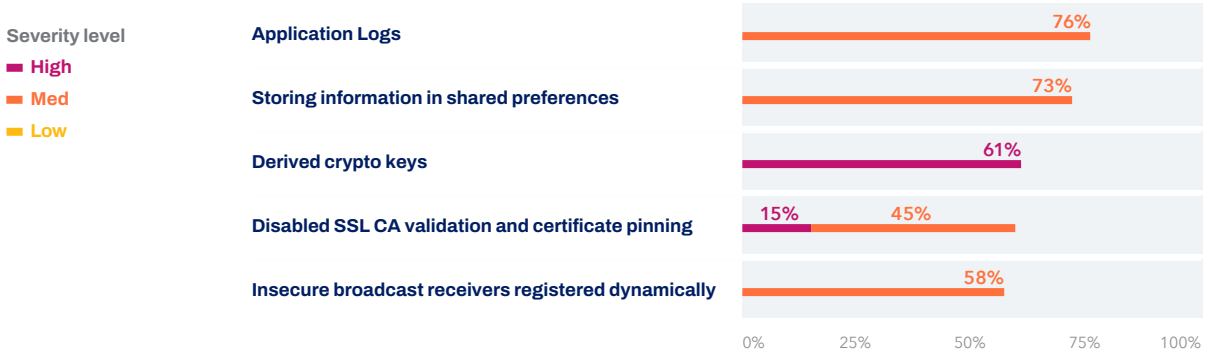
Breakdown of vulnerability by OS



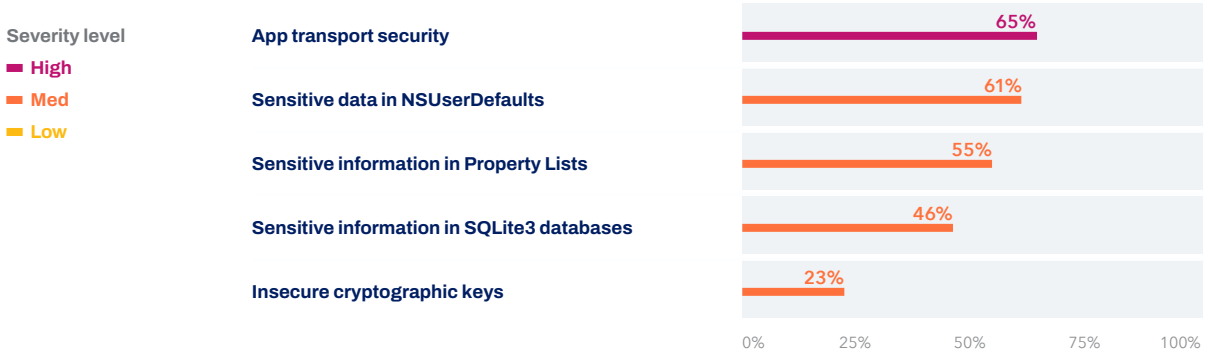
Apps with a data leak vulnerability by OS



Top five significant vulnerabilities found: Android apps



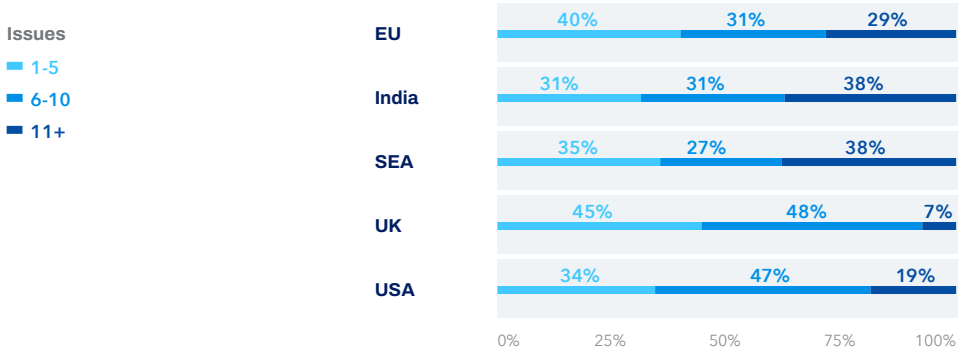
Top five significant vulnerabilities found: iOS apps



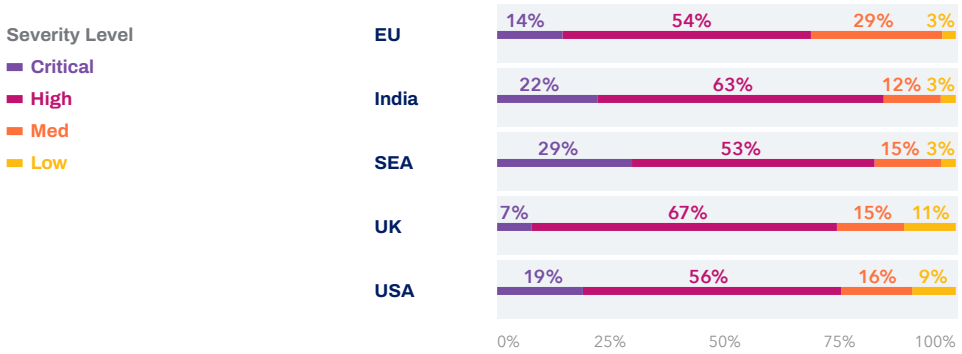
App Security by Country/ Region

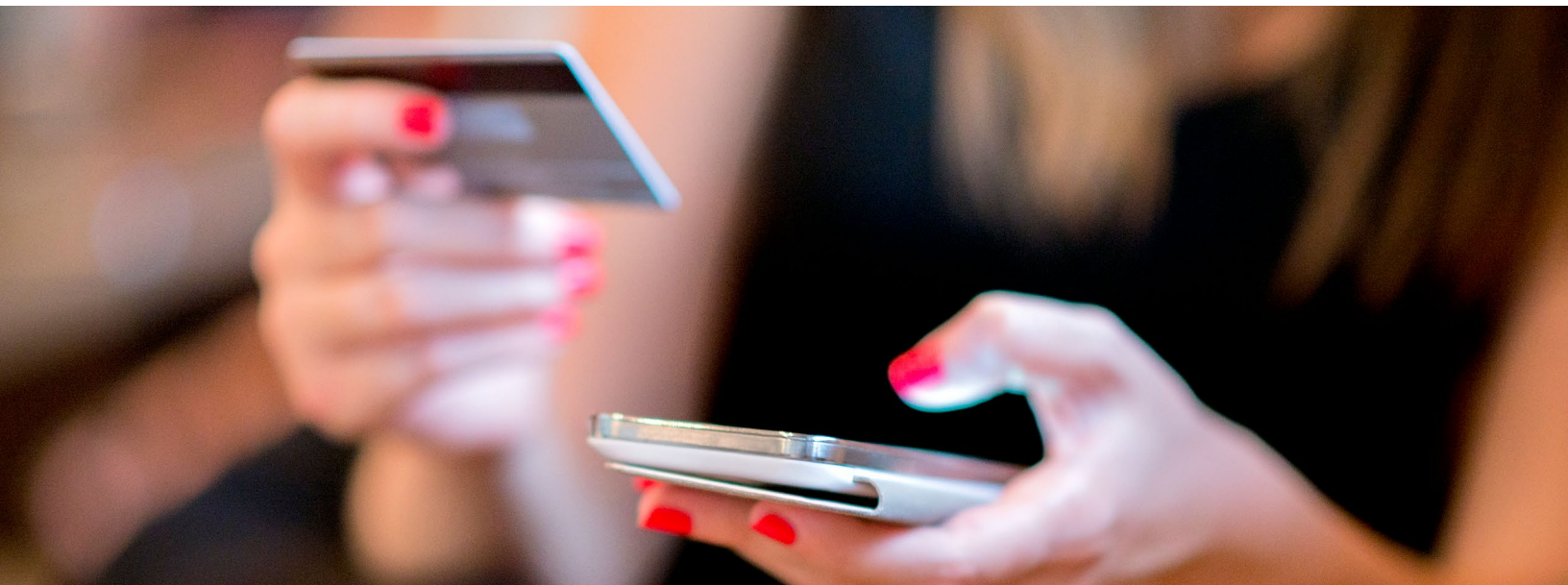
We found significant variations between geographies in app security levels. UK finance apps contained far fewer security issues than apps from other regions—only 7% had more than 10 vulnerabilities compared to 38% of apps in India and Southeast Asia, 29% of apps from the EU, and 19% of U.S. finance apps. Apps from the UK also contained the lowest number of critical vulnerabilities compared to other regions. Apps in Southeast Asia and India performed the weakest in terms of security. The results suggest that the strict financial services security and data privacy regulations in the UK and EU strongly impact financial app security. Beyond the requirements themselves, which generally provide a minimum baseline, such regulations encourage app developers to understand security considerations and take app defense more seriously.

Number of issues detected by country/region



Breakdown of vulnerability severity by country/region

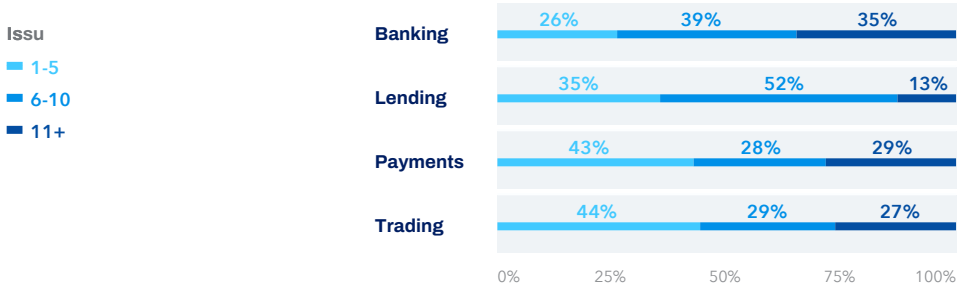




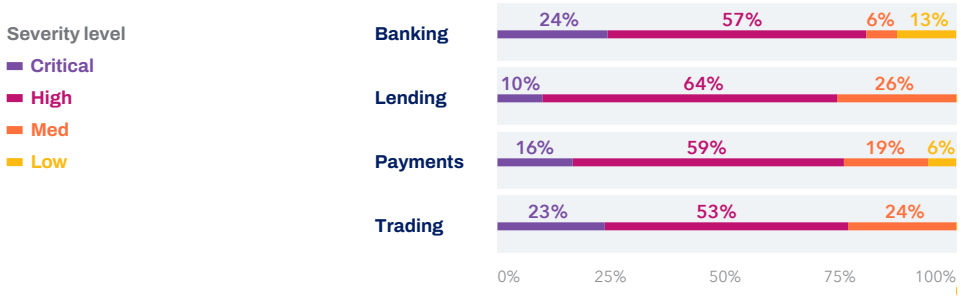
App security by Financial App Type

When looking at the different mobile finance app categories, we uncovered some startling results. Banking apps proved to be significantly more vulnerable both in terms of total number of issues and severity, 35% contained more than 10 vulnerabilities and 81% at least one critical or high severity issue. Payment apps fared only slightly better at 29% and 75%, respectively. Lending apps claimed the most secure spot, possibly because of their more limited functionality.

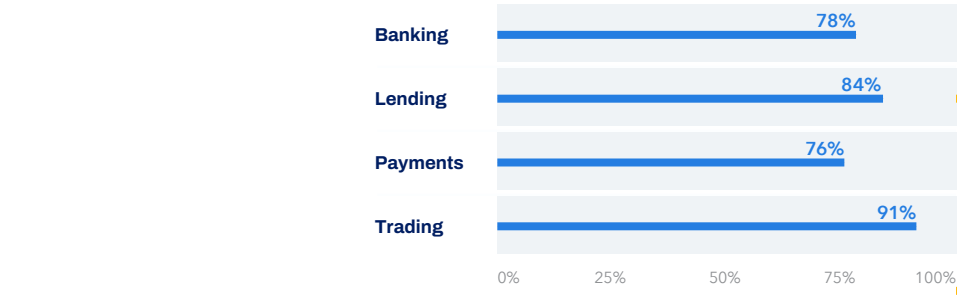
Number of issues detected by app type



Breakdown of vulnerability severity by app type



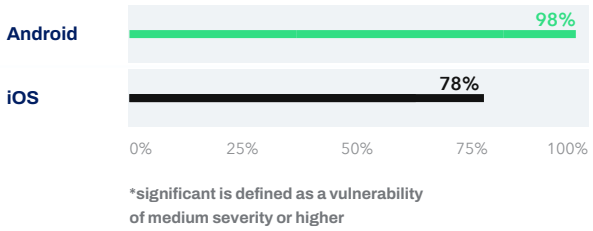
Breakdown of data leak vulnerability by app type



Cryptographic Issues

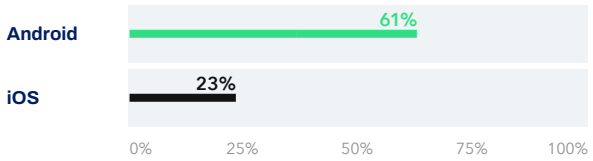
We break out cryptographic issues as a separate category as this continues to be an area of concern for financial applications across the board and in every region. 88% of tested apps had at least one significant (medium severity or higher) cryptographic issue including exposed encryption keys, poor implementation of cryptographic algorithms, insufficient key size, and failure to securely encrypt the communication of sensitive data. Within this class of vulnerabilities, susceptibility to cryptographic key extraction deserves particular attention as it exposes organizations to fraud and financial risks as well as regulatory liability. The analysis found that 61% of Android apps and 23% of iOS apps are vulnerable to crypto key extraction. When breaking down the numbers for geography and app type, the trends we saw in the previous sections hold. UK apps fared far better than their counterparts in other regions, while banking and payment apps proved to be the weakest in crypto key security of the app categories.

Number of apps with a significant* cryptographic issue

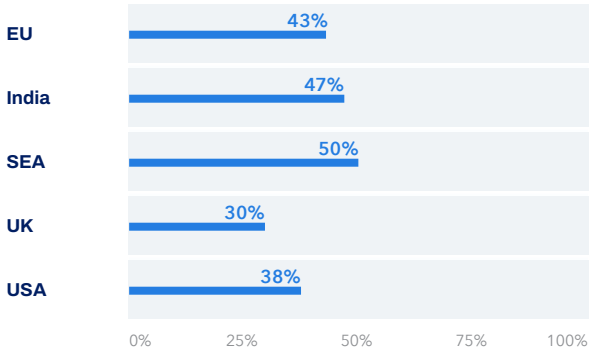


*significant is defined as a vulnerability of medium severity or higher

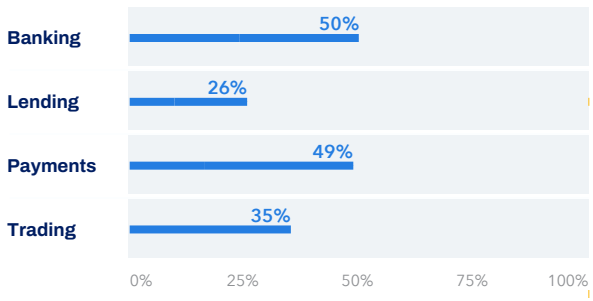
Number of apps vulnerable to crypto key extraction



Breakdown of crypto key extraction vulnerability by country/region



Breakdown of crypto key extraction vulnerability by app type



Improving Finance App Security

This study reveals a disconnect between the level of mobile threat concern expressed by financial services organizations—85% rated the risk as moderate to significant—and the level of security in the apps they and their customers use.[17]

The surge in adoption of mobile financial apps, the increasing scope of mobile financial services and the evolving threat landscape, all indicate that developers need to prioritize reducing the number of vulnerabilities in their apps, regardless of which sector or country they operate in.

Get the Basics Right

Financial services mobile software developers should follow, at the very least, basic secure app design practices. The OWASP Mobile App Security Verification Standard is a great resource. Test regularly and follow a DevSecOps framework so that security is part of the development lifecycle.

Don't neglect to stay on top of the latest regulatory changes and security compliance requirements such as GDPR and PCI-DSS. Proper risk-assessment requires that you be aware of your user's security status as well as your own.

Specific Recommended Improvements and Mitigations

- Do not store sensitive data in insecure locations where it can be easily extracted and exploited. This information should be protected using secure encryption technologies like white-box cryptography or by using strong data obfuscation techniques.
- The vast majority of financial services apps (88%) have mishandled and/or weak encryption that puts them at risk for data theft. Key protection technologies such as white-box cryptography should be used to secure the encryption process.
- Nearly every financial services application tested lacked safeguards to detect and stop analysis and reverse engineering by hackers. Anti-tampering and runtime protections are critical here.

Boost Security with In-App Protection

The rapid expansion of finance apps and their value as a lucrative target means that threats have grown more frequent, more complex, and more difficult to prevent using basic security measures.

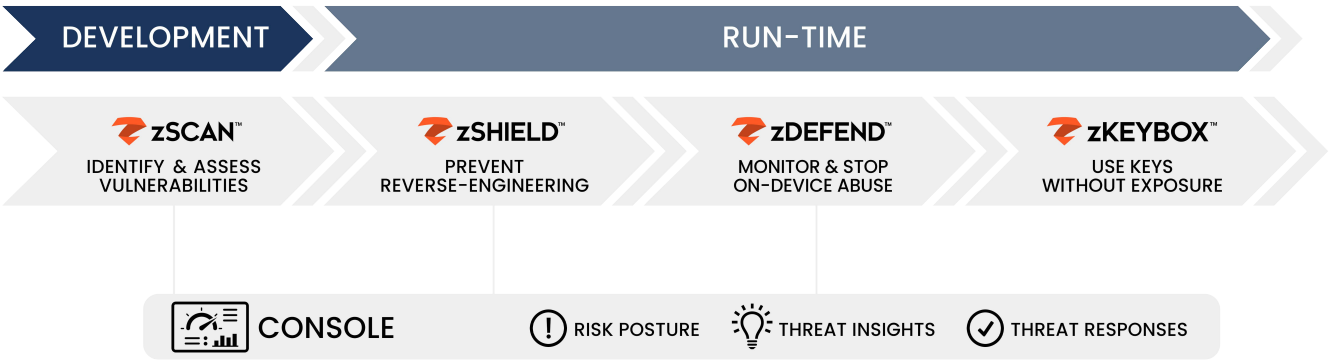
It's impossible to eliminate every application vulnerability. In-app protection technologies add security mechanisms into your app so that it becomes much more difficult to penetrate, modify, or reverse engineer. It involves a number of protective techniques including advanced code obfuscation, anti-debugging, iOS jailbreak and Android rooting detection, integrity protection, and tampering detection and response. The most robust tools shield applications from both static and dynamic threats as well as side-channel attacks like Differential Fault Analysis and Differential Power Analysis.

Protect Cryptographic Keys

The strongest encryption ciphers can't protect data or communications if the encryption keys are compromised. Skilled attackers lift them from code or from memory as they are being used in cryptographic operations. While OS provided Keystores provide some protection, their security can't be guaranteed for every device your app runs on and when rooted, provides no protection at all. Use white-box cryptography to build key protection directly into your apps.

Zimperium can Help

Zimperium provides powerful in-app protection and white-box cryptography solutions that protect apps with sensitive information, thwart attacks, and help you comply with industry regulations. Our team brings vast experience in the financial app security space.



Zimperium zScan
helps mobile app developers identify reputation and financial risks by automatically identifying privacy, security and compliance risks in the development process before apps are released to the public.

Zimperium zShield
injects self-defending capabilities into applications, enabling them to run securely in zero-trust environments. It uses multiple methods including code obfuscation and real-time intrusion detection to prevent tampering, reverse engineering, and other techniques used by cybercriminals to discover vulnerabilities and gain access to sensitive information and resources contained in financial services applications.

Zimperium zKeyBox
uses state-of-the-art white-box cryptography to keep secret cryptographic keys well hidden within the app code, even during runtime. Straightforward to integrate and use, it provides an extensive set of high-level classes and methods for operating with the most popular cryptographic algorithms on any platform.

Zimperium zDefend
is an SDK that enables mobile apps to immediately determine when a user's device is compromised, any network attacks are occurring and even if malicious apps are installed. App developers can configure appropriate remedial actions when a given threat is detected, reducing potential fraud and protecting users.

Appendix

Zimperium provides powerful in-app protection and white-box cryptography solutions that protect apps with sensitive information, thwart attacks, and help you comply with industry regulations. Our team brings vast experience in the financial app security space.

Vulnerability scoring

Vulnerabilities were rated according to the CVSS[18] which is based on exploitability, scope, impact, and other qualitative metrics.

CVSS Qualitative Rating Scale

Rating	CVSS score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

The collateral damage implication for each threat category can be broken down as follows:

Threat classification	Impact
None (N)	No potential for loss of assets, revenue or productivity
Low - Medium (L)	Limited damage to assets, or minor loss of revenue productivity
Medium - High (M)	Serious damage or loss
High (H)	Catastrophic damage or loss

Vulnerabilities Tested and Occurence

Vulnerability	Severity level	Total
Network Security Misconfiguration: Android	Critical	27
Weak Derived Crypto Keys: Android	High	49
JavaScript CORS enabled in Webview: Android	High	39
Insufficient Transport Layer Protection: Android	High	30
Content Provider File Traversal Vulnerability: Android	High	4
PhoneGap HTTPS Whitelist Bypass: Android	High	0
Application Debugging: Android	High	0
Remote URL Redirection Vulnerability: Android	High	0
Cordova Remote Start Page Manipulation Vulnerability: Android	High	0
Insecure SSLSocketFactories: Android	High	0
PhoneGap Error URL Redirection Vulnerability: Android	High	0
PhoneGap HTTPS Bypass Vulnerability: Android	High	0
JavaScript Interface Remote Code Execution: Android	High	0
Connection to External Redis Server: Android	High	0
Disabled SSL CA Validation and Certificate Pinning: Android	Medium-High	48
Application Logs: Android	Medium	61
Storing Information in Shared Preferences: Android	Medium	58
Insecure Broadcast Receivers registered dynamically: Android	Medium	46
Sensitive information in SQLite database: Android	Medium	44
Broken SSL Trust Manager: Android	Medium	29
MediaProjection: AndroidService allows recording of audio, screen activity: Android	Medium	28
AndroidComponent Hijacking via Intent: Android	Medium	27
Broken HostnameVerifier for SSL: Android	Medium	25
App Extending WebViewClient: Android	Medium	24
External data in raw SQL queries: Android	Medium	13
WebView Exploits: Android	Medium	12
PhoneGap Debug Logging: Android	Medium	9
HostnameVerifier Allowing All Hostnames: Android	Medium	7
PhoneGap Whitelisted URLs: Android	Medium	6
Java Object Deserialization Vulnerability: Android	Medium	1
Insecure Hashing Algorithms: Android	Medium	0
Sending address book data over unencrypted insecure transport layer: Android	Medium	0
AndroidFragment Injection: Android	Medium	0
Unused Permissions: Android	Low	79
Unprotected Exported Activities: Android	Low	58
Unprotected Exported Receivers: Android	Low	56
Bytecode Obfuscation missing: Android	Low	41

Vulnerability	Severity level	Total
Unprotected Exported Service: Android	Low	31
Deprecated setPluginState in WebView: Android	Low	24
Enabled AndroidApplication Backup: Android	Low	12
PhoneGap JavaScript Injection: Android	Low	9
Unprotected Exported Provider: Android	Low	8
Surreptitious Sharing on Android: Android	Low	4
Improper Custom Permissions: Android	Low	0
Non-signature Protected Exported Activities: Android	Low	0
Non-signature Protected Exported Services: Android	Low	0
Non-signature Protected Exported Providers: Android	Low	0
Non-signature Protected Exported Receivers: Android	Low	0
Do not allow WebView to access sensitive local resource through file scheme: Android	Low	0
Improper Content Provider Permissions: Android	Low	0
Unprotected Services: Android	Low	0
App Transport Security: iOS	Low	52
PhoneGap Whitelist Open Access: iOS	High	6
Insufficient Transport Layer Protection: iOS	High	4
PhoneGap Whitelist RegEx Bypass: iOS	High	2
Short HMAC Keys: iOS	High	2
UIWebView Exploits: iOS	High	1
Sensitive Data in NSUserDefaults: iOS	High	49
Sensitive Information in Property Lists: iOS	Medium	44
Sensitive Information in SQLite3 Databases: iOS	Medium	37
Insecure Cryptographic Keys: iOS	Medium	18
Unsecured Data in CoreData: iOS	Medium	10
Debug Logging with NSLog: iOS	Medium	6
Unsecured Data in RealmDB: iOS	Medium	1
iOSSecKeyEncrypt implementation: iOS	Medium	1
PhoneGap Debug Logging: iOS	Medium	0
Unsecured Data in YapDB: iOS	Medium	0
Vulnerable Hash Algorithms: iOS	Medium	0
Unsecured Data in CouchDB: iOS	Medium	0
Insecure Peer Connections: iOS	Medium	0
Zipperdown vulnerability leading to remote code execution attack: iOS	Low	77
Deprecated NSURLConnection: iOS	Low	11
iOSBinary having ASLR Protection: iOS	Low	0

Sources

1 https://www.cnbc.com/2020/05/27/coronavirus-crisis-mobile-banking-surge-is-a-shift-likely-to-stick.html

2 State of Mobile 2021, App Annie, January 2021

3 The Mobile Finance Report 2020, Adjust and Apptopia, October 2020

4 The 2021 Global Payments Report, Worldpay from FIS, March 2021

5 Verizon Mobile Security Index 2020 Report, Verizon, February 2020

6 The 2021 Global Payments Report, Worldpay from FIS, March 2021

7 https://source.android.com/security/bulletin

8 https://support.apple.com/en-us/HT201222

9 https://9to5mac.com/2020/08/01/new-unpatchable-exploit-allegedly-found-on-apples-secure-enclave-chip-heres-what-it-could-mean/

10 https://threatpost.com/mobile-adware-booms-attacks/164386/

11 https://www.anomali.com/blog/anomali-threat-research-identifies-fake-covid-19-contact-tracing-apps-used-to-monitor-devices-steal-personal-data

12 https://latesthackingnews.com/2020/07/12/cerberus-malware-emerged-on-play-store-impersonating-cryptocurrency-converter-app/

13 https://thehackernews.com/2020/11/watch-out-new-android-banking-trojan.html

14 https://securityintelligence.com/posts/massive-fraud-operation-evil-mobile-emulator-farms/

15 https://owasp.org/www-project-mobile-top-10/

16 https://www.cvedetails.com/top-50-products.php?year=2021

17 Mobile Security Index 2020 Financial services spotlight, Verizon

18 https://www.first.org/cvss/

About Zimperium

Zimperium, the global leader in mobile security, provides the only on-device, machine learning-based protection against Android, iOS, and Chromebook threats. Zimperium defends mobile endpoints and apps against device, network, phishing and malicious app attacks. Headquartered in Dallas, Texas, Zimperium is backed by Warburg Pincus, SoftBank, Samsung, Sierra Ventures, and Telstra Ventures.

Start protecting your applications today. For a free analysis of your mobile app, visit:
https://www.zimperium.com/contact-us

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com
Zimperium, Inc
4055 Valley View, Dallas, TX 75244