

## App Security and Risk Findings - Finance -

Europe and Middle East

#### Executive Summary

The top banks and mobile payment providers in the European and Middle Eastern regions may be accepting too much risk for security and privacy by failing to adhere to coding best practices, continuing to utilize excessive privileges, and sharing sensitive customer data with advertisers. According to our latest research of over 450 iOS and Android mobile banking and payment applications distributed in the European and Middle Eastern regions, most failed the Open Web Application Security Project Mobile Top 10 and contain unnecessary risks and vulnerabilities.



# UK and EU suffer high average per transaction fraud cost







#### Bank Impersonations



These attacks leverage malicious mobile apps designed in such a way as to trick users into thinking they are from a legitimate financial institution.

Criminals seek to gain account credentials and/or credit card numbers. Once an account is breached, criminals can execute transfers or payments after logging into the account or can sell the credentials to another party.



Specially crafted apps for graphically and behaviorally mitating legitimate banking apps

rojans running services and lisplaying overlays on top of egitimate banking apps mimicking. egitimate banking applications





# Nearly 3 of every 4 fraudulent transactions (72%) are via the mobile channel.



# The average value of a fraudulent mobile payment transaction is \$767.







#### Lack of Obfuscation Leads to Reverse Engineering



#### Gain insight into critical processes

Exploit vulnerabilities

Extract sensitive information such as personal, financial information from the application's code



Uncover algorithms to replicate or abuse Discover embedded credentials Bypass security checks



Frida, Xposed, Substrate, QBDI, scriptable debuggers, CaptainHook, MobileSubstrate, Cycript, Cynject, IDA, Ghidra, BinaryNinja, Hopper, Radare2, JEB, jadx, apktool; dextra, jtool,joker





#### Methodology

This research provides findings for security, data leakage, privacy abuse, and compliance for over 450 mobile banking and payment apps (193 iOS and 267Android) distributed in the European and Middle Eastern regions.

Findings result from testing each public mobile app using Zimperium's application analysis engine, <u>zScan</u>. zScan is an application reputation scanning service providing deep intelligence about app behavior, including content (the app code itself), intent (the app's behavior), context (the domains, certificates, shared code, network communications, and other data), and compliance.



The OWASP summary contains testing results performed on the applications against the OWASP Top 10 Mobile categories.

The security summary focuses on application risks. These risks include functionality and code use, application capabilities, and critical vulnerabilities.

The privacy information focuses on the application's access to private user data, unique device identifiers, SMS, communications, and data storage.



#### OWASP Mobile Top 10 Results

Part of our research into the mobile banking applications includes providing a passing or failing mark for each of the <u>OWASP Mobile Top 10</u>. The tables below summarize passing and failing marks collectively for all the apps on each platform. Some highlights include:

Nine of 10 apps (93%) fail for M2: Insecure Data Storage. These vulnerabilities can result in data loss of one user or many. Data loss typically leads to identity theft, fraud, material loss, and reputation damage for the organization that owns the app's risk.

97 59

99

88

Most apps fail (97% of iOS and 59% of Android) for M3: Insecure Communication. Insecure communication vulnerabilities are common and easy to exploit. Mobile applications often do not protect network traffic and therefore are easy to exploit.



Ninety-seven percent of iOS apps (97%) and twenty-two percent of Android apps (22%) fail M8: Code Tampering. An attacker will typically exploit code modification by manipulating binaries to create malicious forms of the app.



Almost all of the apps in our sample (99%) fail for M9: Reverse Engineering. Generally, most applications are susceptible to reverse engineering due to the inherent nature of code.



### OWASP Mobile Top 10

M1 - Improper Platform Usage M2 - Insecure Data Storage M3 - Insecure Communications M4 - Insecure Authentication M5 - Insufficient Cryptography M6 - Insecure Authorization M7 - Client Code Quality M8 - Code Tampering M9 - Reverse Engineering M10 - Extraneous Functionality





Pass



#### OWASP Mobile Top 10



M1 - Improper Platform Usage M2 - Insecure Data Storage M3 - Insecure Communications M4 - Insecure Authentication M5 - Insufficient Cryptography M6 - Insecure Authorization M7 - Client Code Quality M8 - Code Tampering M9 - Reverse Engineering M10 - Extraneous Functionality







#### Privacy and Security Risk Rankings -EMEA

Privacy Risk



Needs Improvement Security Risk



#### Critical Security Findings





#### Critical Security Findings





Finance App Security and Risk Findings - EMEA – Zimperium, Inc

🗢 💎 ZIMPERIUM

#### Dangerous Security Findings

Contain Facebook Access Token Vulnerability

Facebook SDK tracking opens, sharing







7 Source: Zimperium







### Dangerous Privacy / Leakage Findings





### Dangerous Privacy / Leakage Findings 📹





#### Privacy and Security Risk Rankings -EMEA





Privacy Risk





#### Critical Security Findings



Uses WebKit to download a file from the Internet Uses insecure data storage mode Uses method to blindly load all apps and JAR files Can retrieve remote apps, Java code and DEX files Vulnerable Facebook SDK version Does validate CN(Common Name) of the SSL certificate This app contains unsafe cryptographic encryption patterns Has the functionality to install additional apps App refers to SSL/TLS hosts with self-signed certificate This app accepts all security certificates Vulnerable to CVE-2015-8320 Bundling Additional Android applications Contains commands to Stop and Start a proxy server The application has been packed with Jiagu Packer Uses an SSL connection with disabled security checks This app can perform a Traceroute network function.





0%

#### Critical Security Findings



Uses WebKit to download a file from the Internet Uses insecure data storage mode Uses method to blindly load all apps and JAR files Can retrieve remote apps, Java code and DEX files Vulnerable Facebook SDK version Does validate CN(Common Name) of the SSL certificate This app contains unsafe cryptographic encryption patterns Has the functionality to install additional apps App refers to SSL/TLS hosts with self-signed certificate This app accepts all security certificates Vulnerable to CVE-2015-8320 Bundling Additional Android applications Contains commands to Stop and Start a proxy server The application has been packed with Jiagu Packer Uses an SSL connection with disabled security checks This app can perform a Traceroute network function.







#### Dangerous Security Findings

Stores inline API keys/values Using 'proceed()' method during SSL error handling This app can create and share an RSS Feed App implements a custom keyboard extension API can publish/receive messages from nearby devices Gives PendingIntent to another application Additional app links discovered in communications App is accessing Google Drive 0% 10%



#### Dangerous Security Findings



Stores inline API keys/values Using 'proceed()' method during SSL error handling Uses insecure data storage mode This app can create and share an RSS Feed App implements a custom keyboard extension API can publish/receive messages from nearby devices Gives PendingIntent to another application Additional app links discovered in communications App is accessing Google Drive







App sets data content as Android Package (APK) MIME Content Providers are implicitly insecure and could leak... Accesses the phone call log A URL contains a GET parameter named 'password' App is reading complete address book This app uses IBM's MQTT library to send push notifications Grants permission to one or more content provider's data Access credentials (username/password) have been... Can capture screenshots Using Beacon to send / receive information to nearby... Bundled with the Chinese ad platform Igexin



0%





App sets data content as Android Package (APK) MIME Content Providers are implicitly insecure and could leak.. Accesses the phone call log A URL contains a GET parameter named 'password' App is reading complete address book This app uses IBM's MQTT library to send push notifications Grants permission to one or more content provider's data Access credentials (username/password) have been... Can capture screenshots Using Beacon to send / receive information to nearby... Bundled with the Chinese ad platform Igexin



# Dangerous Privacy / Leakage Findings





# Dangerous Privacy / Leakage Findings

Uses getLastKnownLocation() method to retrieve GPS. Accesses address book and obtains all contacts Capturing the SPN (Service Provider Name) Can access and read global clipboard Some PII data can be collected via Crashlytics Facebook SDK tracking opens, sharing Has access to the device microphone Can capture inbound SMS message Returns current device position when a change is detected Has functionality to record video Exposing passwords in clear text in the user interface Can access the SMS Inbox Can share video through the Facebook SDK Gains access to storage service without using any credentials





#### **Best Practices and Recommendations**



Scan and test for app vulnerabilities and risks in the build pipeline to reduce attack surface



Shield and harden app to increase reverse engineering difficulty



Defend from fraud by measuring vulnerabilities and realtime attacks to customers' devices



#### About the authors





Scott has over 20 years experience providing customized software solutions to enterprise customers in mobile, supply chain and DevOps. Scott invests his time researching mobile app security and worldwide mobile threat events.

king@zimperium.com



Ken Lloyd VP of Risk

Ken Lloyd is a highly accomplished Senior Global Tech Executive and Board Member with more than 20 years of success in cyber security sector focusing in on the areas of Anti-Malware/Virus technologies and Mobile Security product solutions.

