ZIMPERIUM

App Security and Risk Findings - Finance -

Latin and South America

Executive Summary

The top banks and mobile payment providers in the Latin and South American 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 280 iOS and Android mobile banking and payment applications distributed in the Latin and South American regions, most failed the Open Web Application Security Project Mobile Top 10 and contain unnecessary risks and vulnerabilities.

Send query parameters containing PII over insecure communication channels.

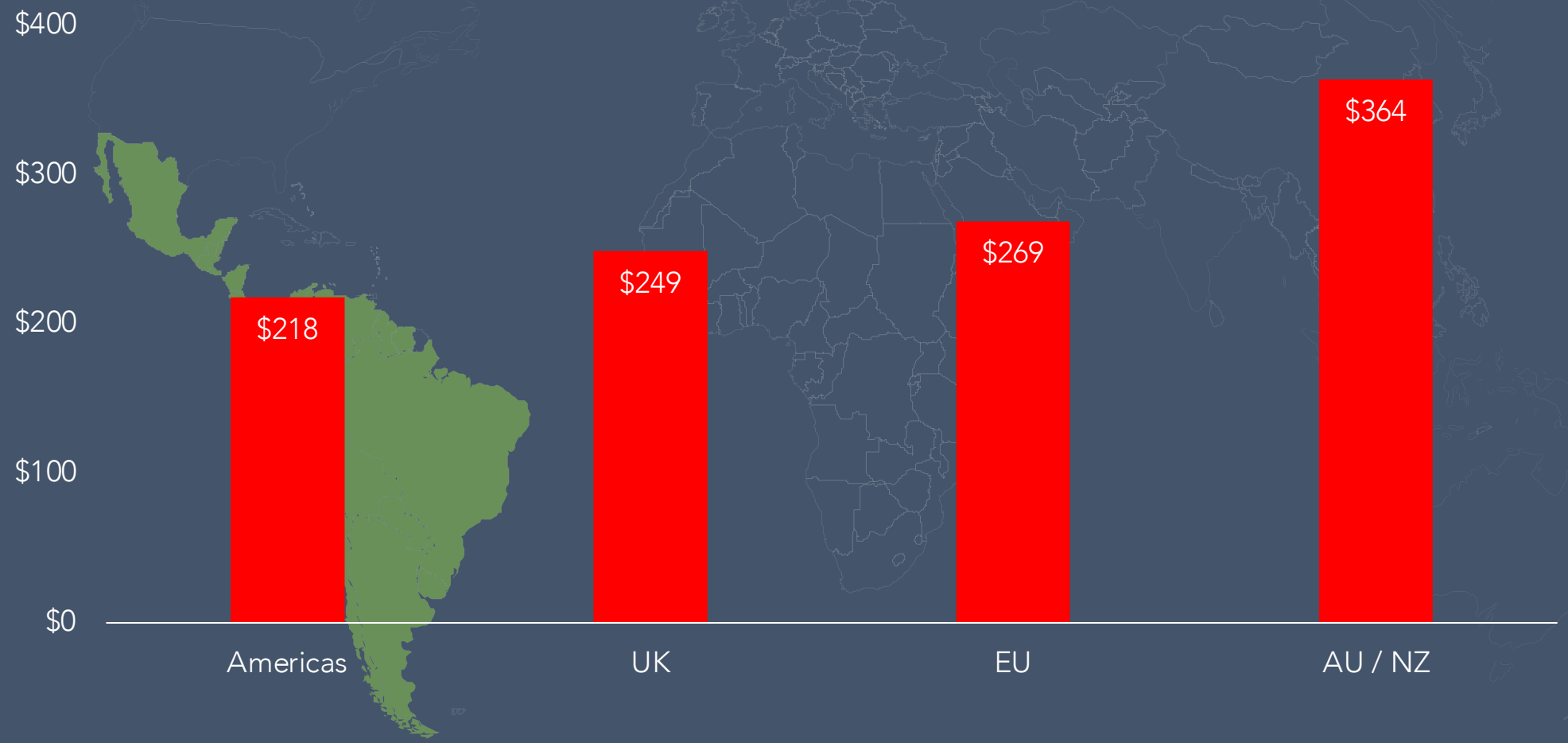
Most apps 56% do not utilize any obfuscation or application shielding software to prevent reverse engineering.

Banks and payment app providers use excessive and unnecessary permissions on customers devices. This increases the risk of data leakage and privacy abuse.

Most finance mobile applications fail OWASP Mobile Top-10 checks for reverse engineering, secure storage, and secure communications.

Fraudulent mobile transactions have increased to an average of $767 and make up 72% of fraudulent transactions.

Average value per fraudulent transaction



Source: RSA Quarterly Fraud Report, Q1 2020

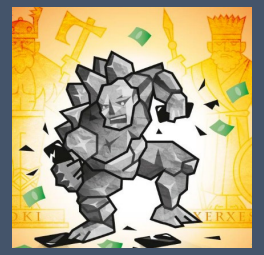
Bank Impersonations

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 imitating legitimate banking apps

Trojans running services and displaying overlays on top of legitimate banking apps mimicking legitimate banking applications



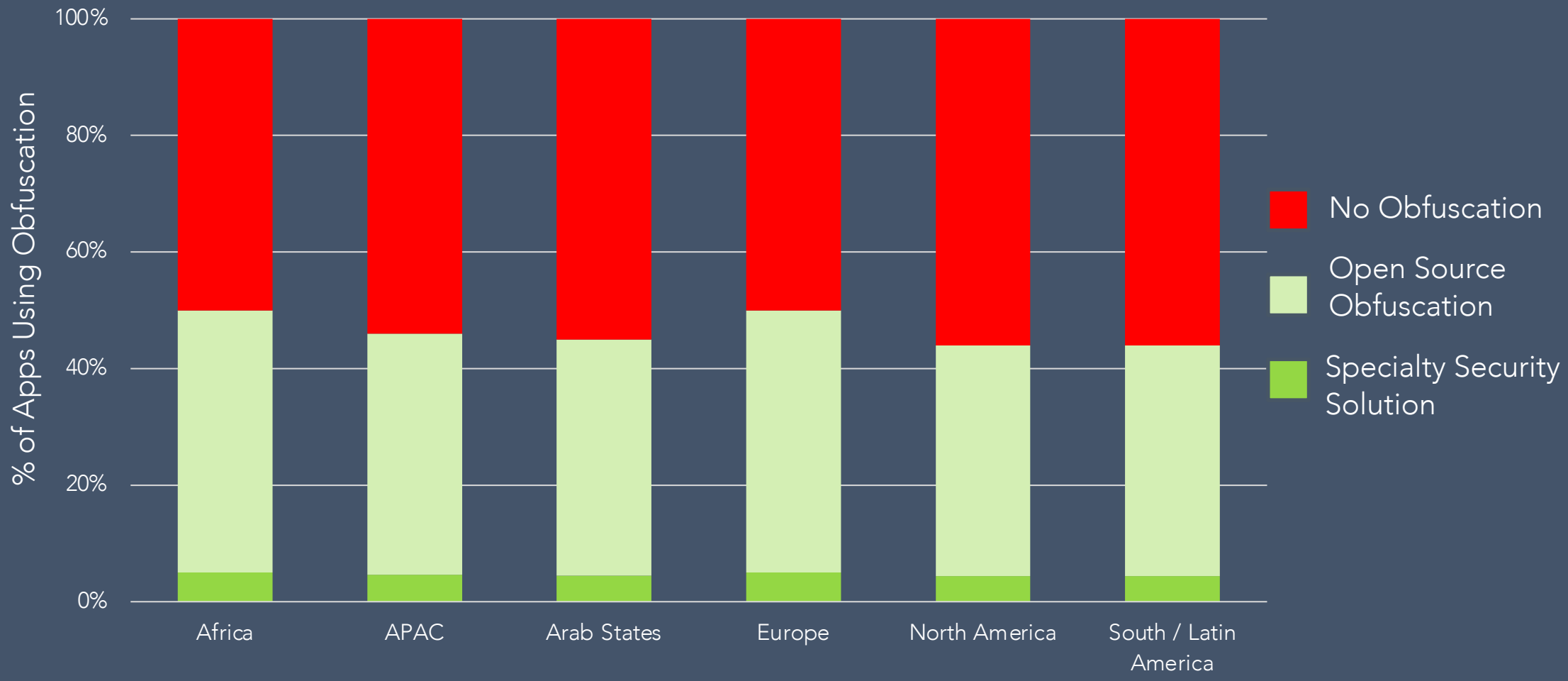
Nearly 3 of every 4 fraudulent transactions (72%) are via the mobile channel.

Source: RSA Quarterly Fraud Report, Q1 2020

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

Source: RSA Quarterly Fraud Report, Q1 2020

3,000+ Android Mobile Finance Apps



Source: Most Mobile Financial Apps Fall Short of Security Best Practices

ZIMPERIUM

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

ZIMPERIUM

Methodology

This research provides findings for security, data leakage, privacy abuse, and compliance for over 288 mobile banking and payment apps (114 iOS and 174 Android) distributed in the Latin and South American regions.

Findings result from testing each public mobile app using Zimperium's application analysis engine, zScan. 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 OWASP Mobile Top 10. The tables below summarize passing and failing marks collectively for all the apps on each platform. Some highlights include:

Nine of 10 apps (92%) 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.

Most apps fail (96% of iOS and 53% 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-nine percent of iOS apps (99%) and eighteen percent of Android apps (18%) fail M8: Code Tampering. An attacker will typically exploit code modification by manipulating binaries to create malicious forms of the app.

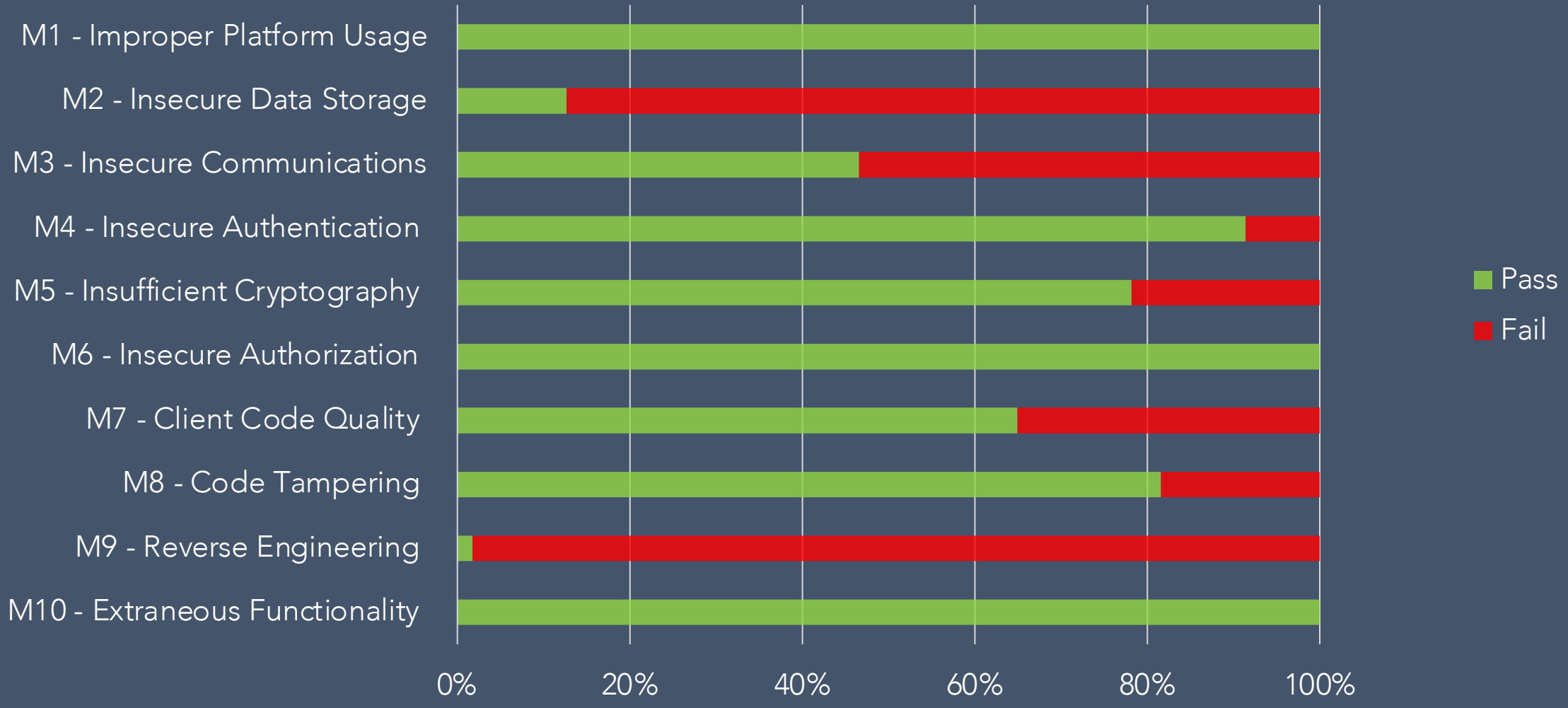
Almost all of the apps in our sample (99%) fail for M9: Reverse Engineering. Generally, most applications are susceptible to reverse engineering due to the inherent nature of code.

OWASP Mobile Top 10

Source: Zimperium

ZIMPERIUM

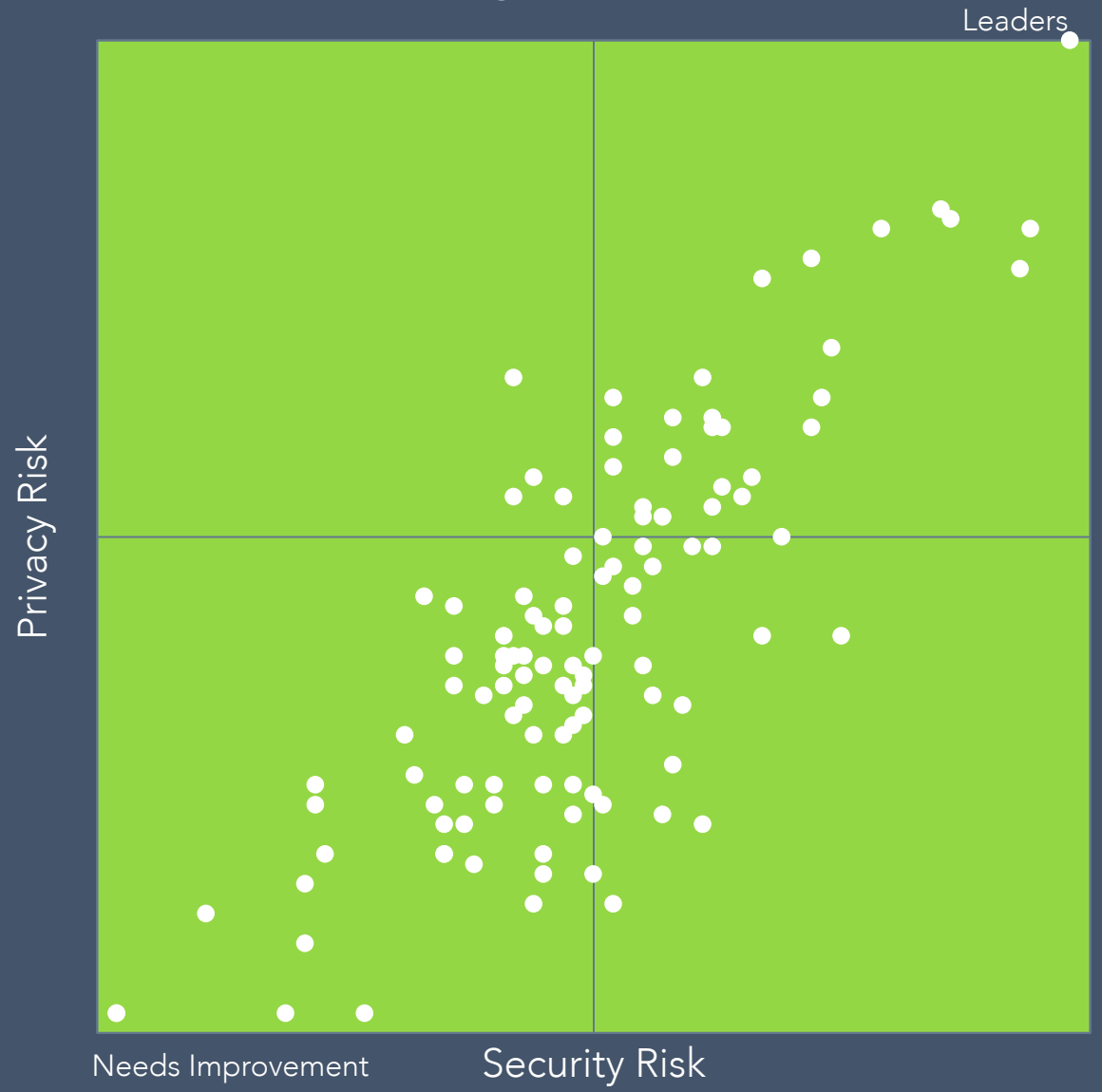
OWASP Mobile Top 10



Source: Zimperium

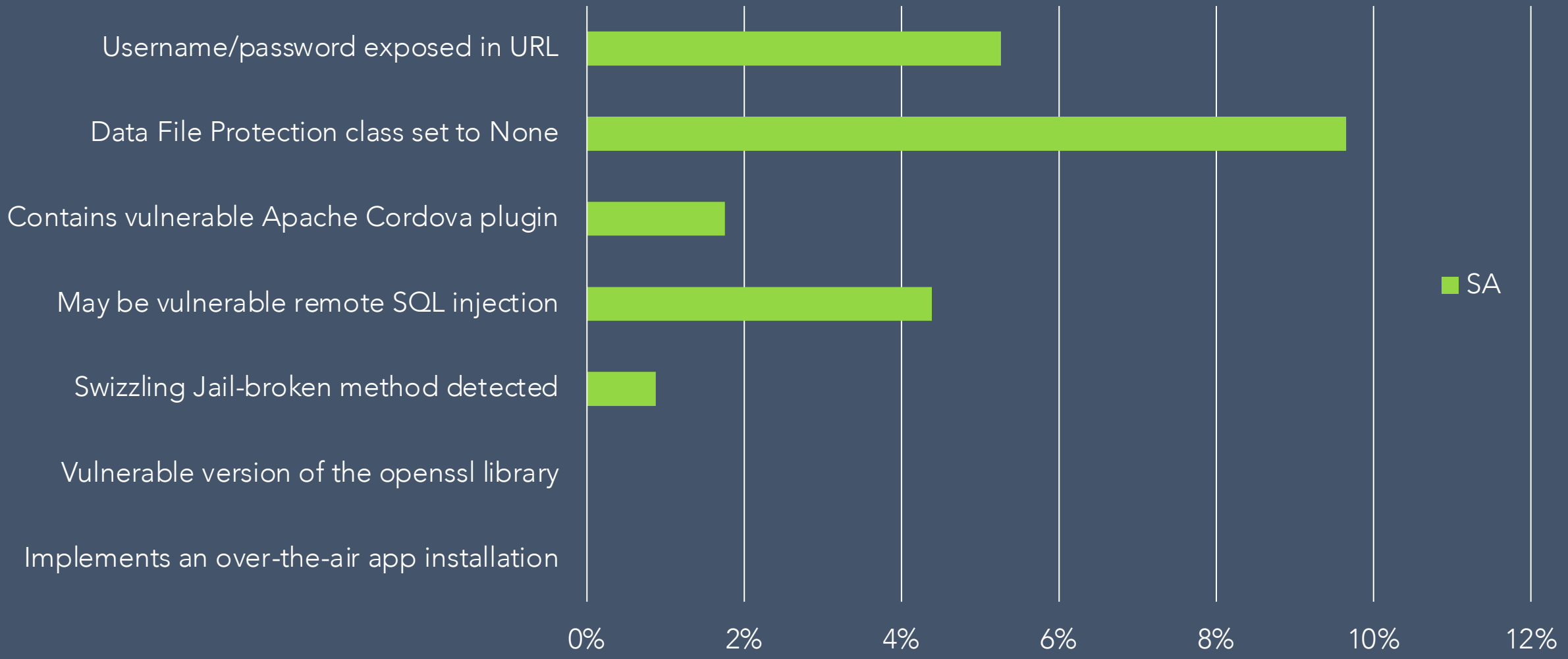
ZIMPERIUM

Privacy and Security Risk Distribution



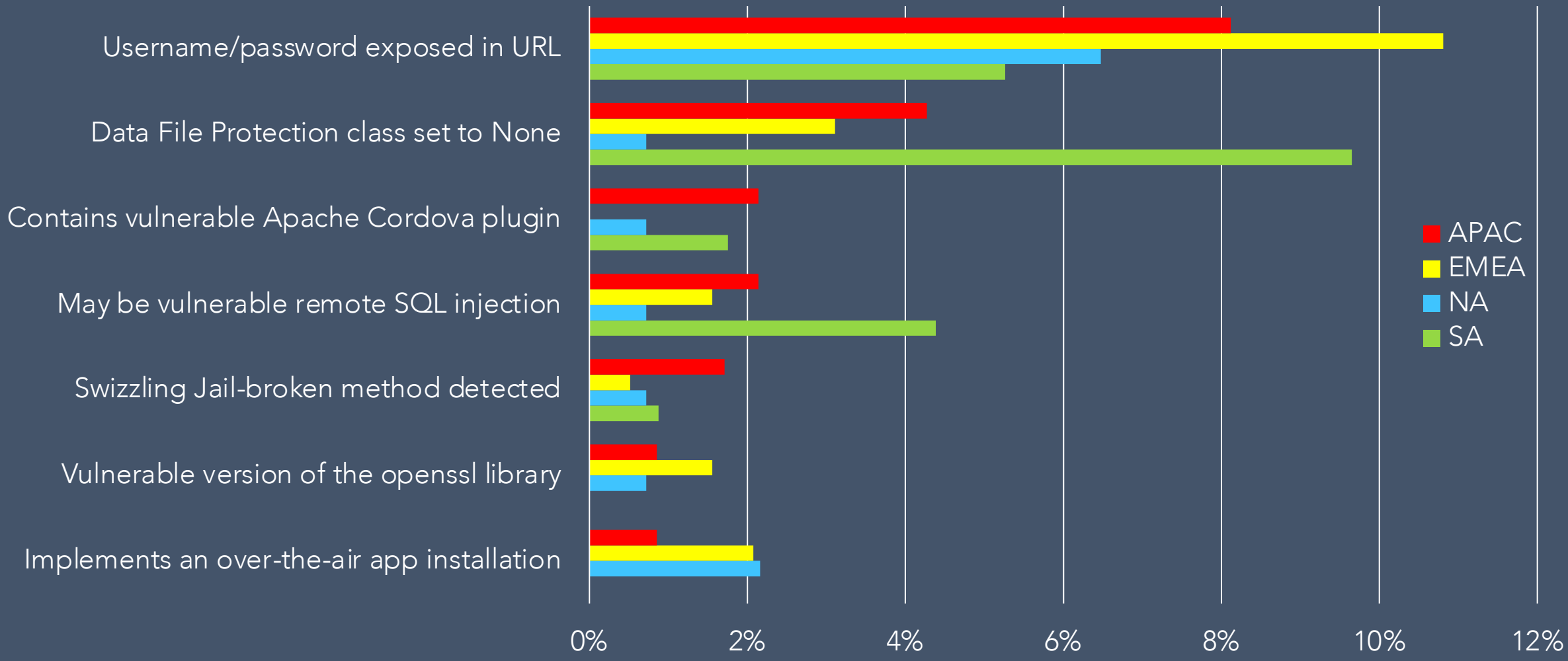
Source: Zimperium

Critical Security Findings



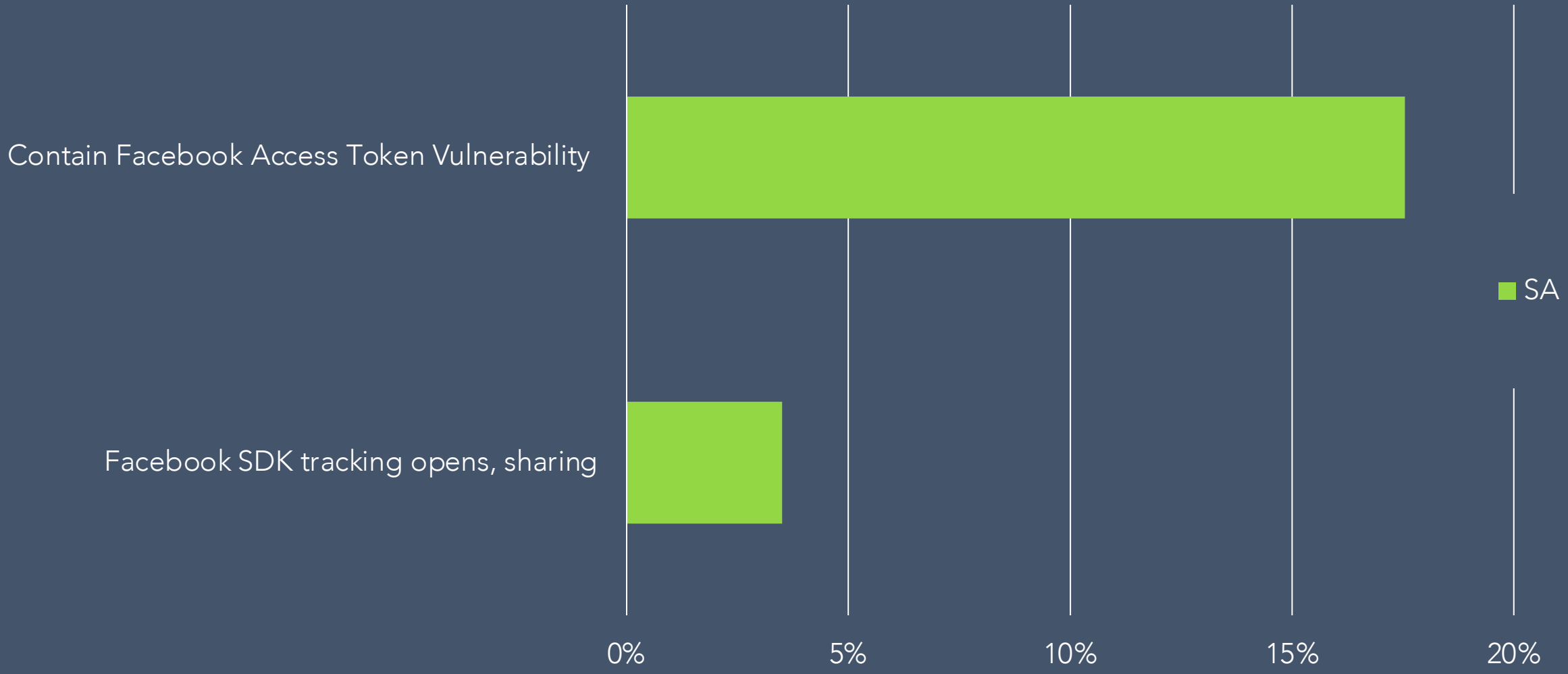
Source: Zimperium

Critical Security Findings



Source: Zimperium

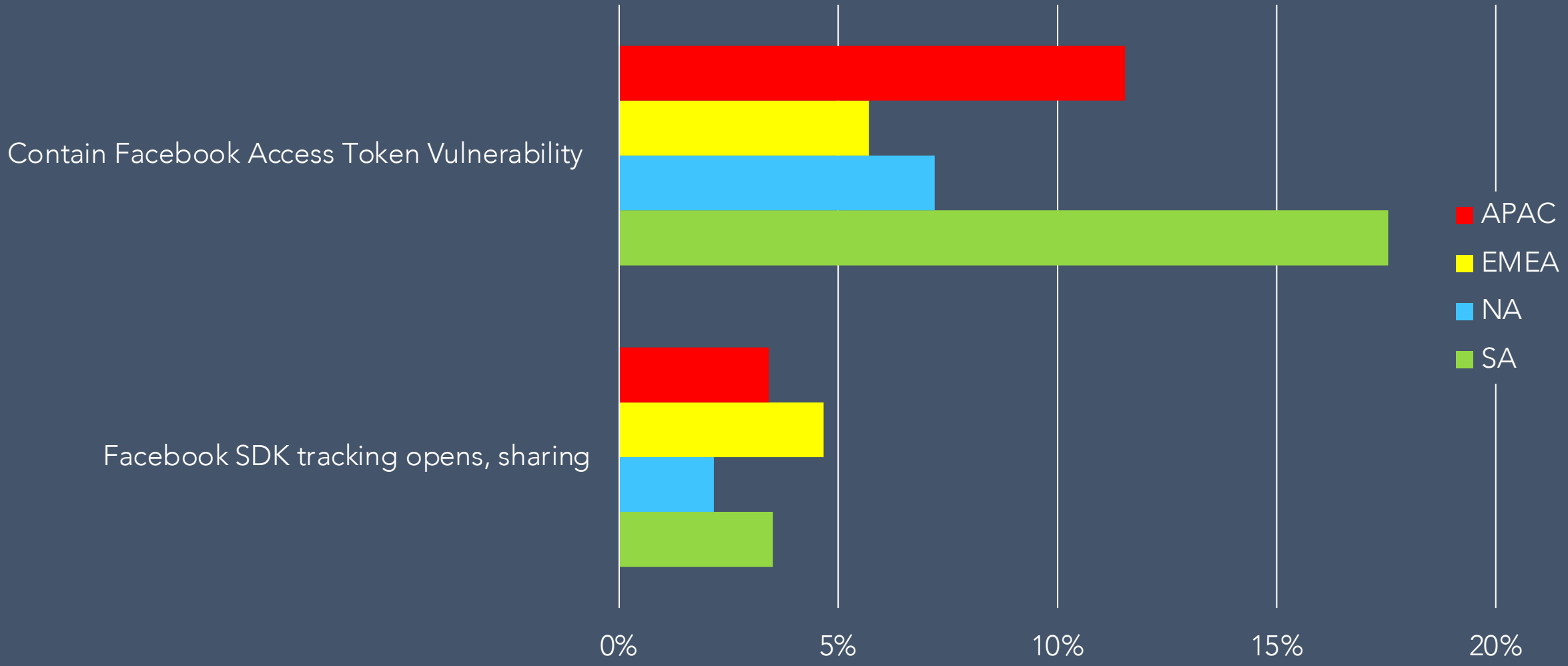
Dangerous Security Findings



Source: Zimperium

ZIMPERIUM

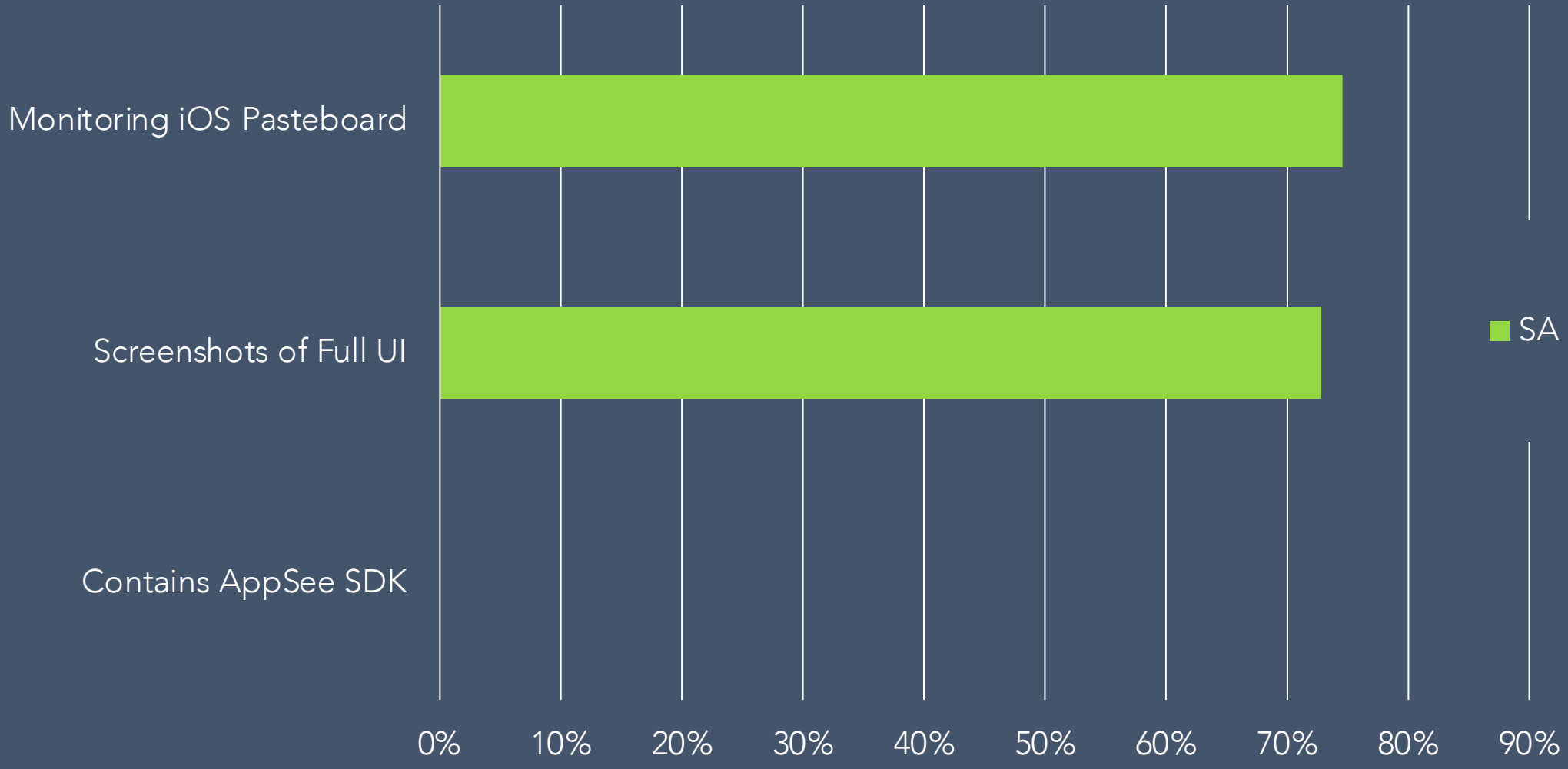
Dangerous Security Findings



Source: Zimperium

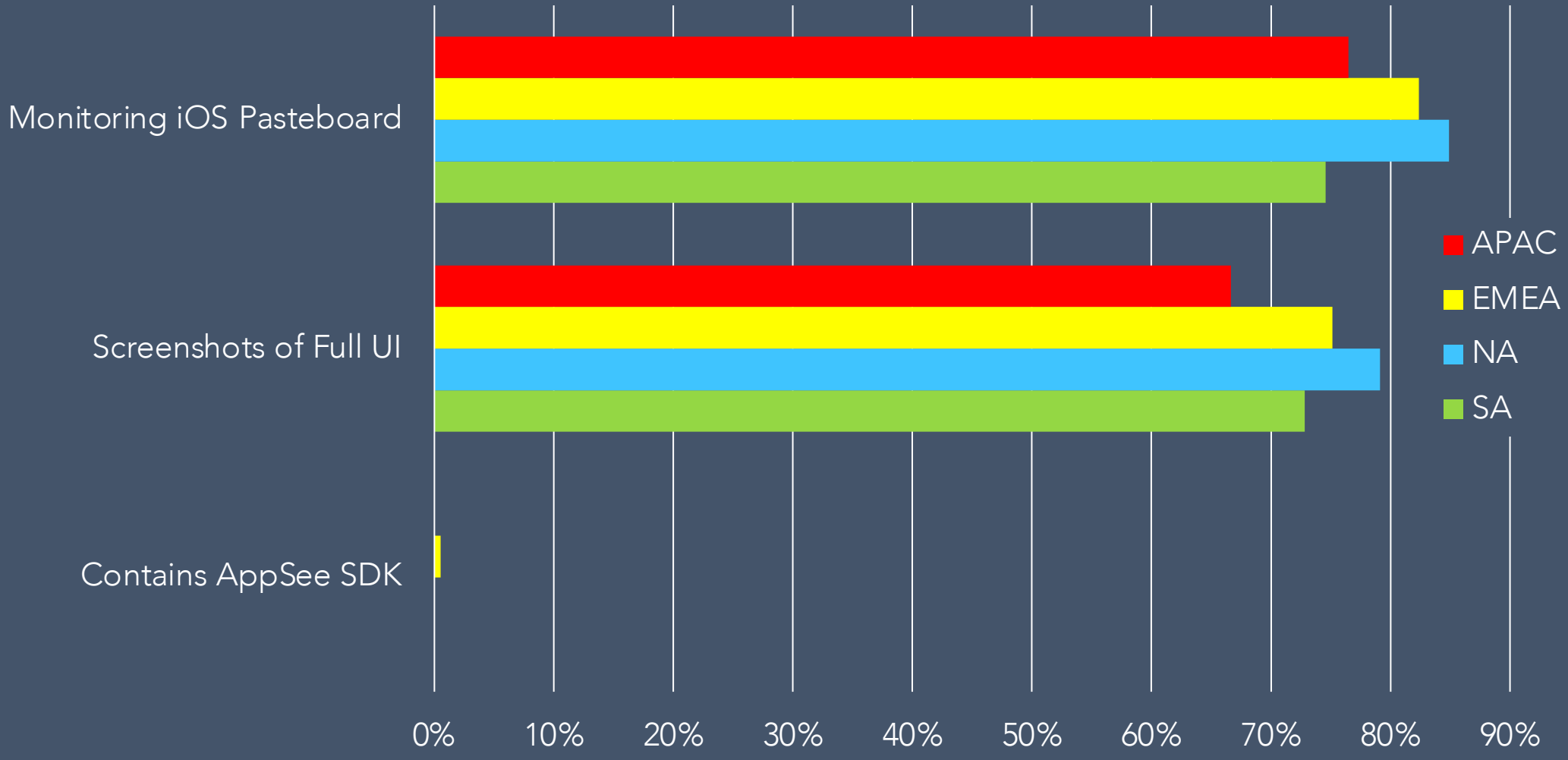
ZIMPERIUM

Critical Privacy / Leakage Findings



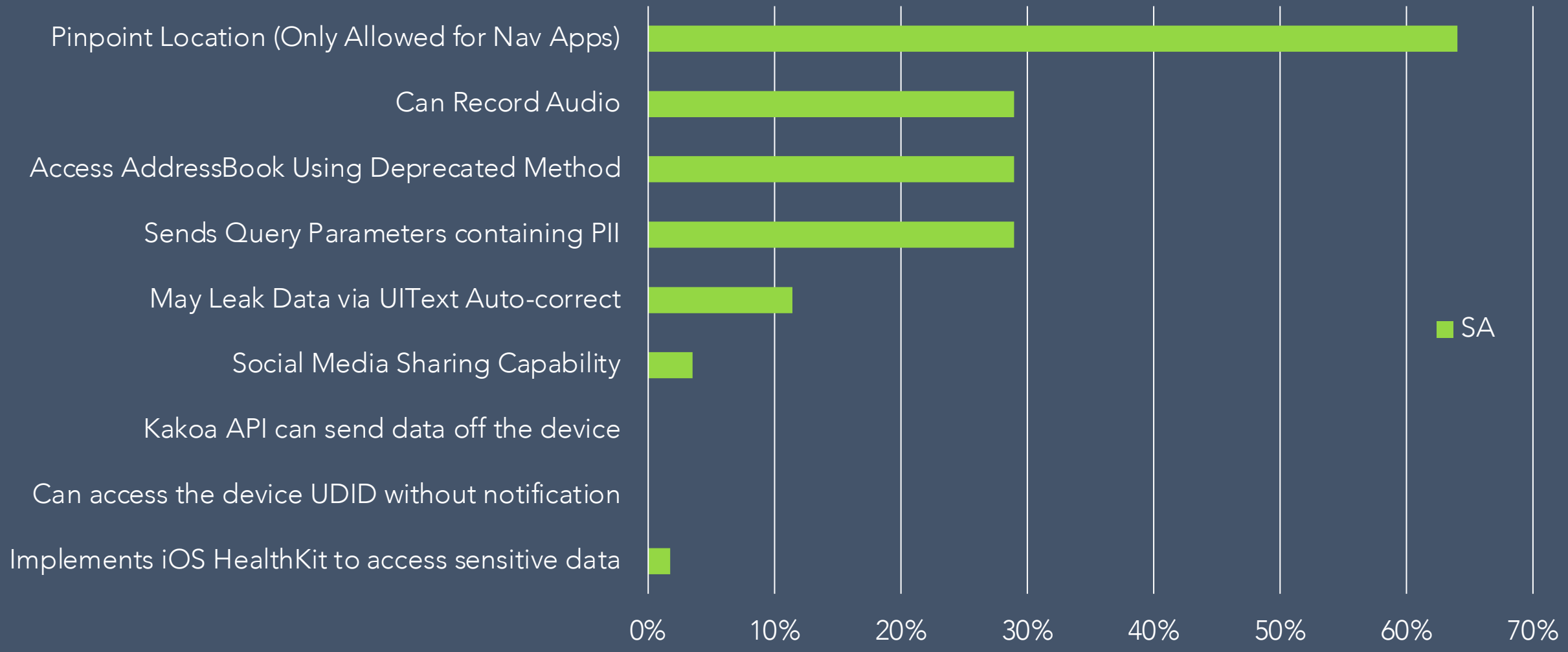
Source: Zimperium

Critical Privacy / Leakage Findings



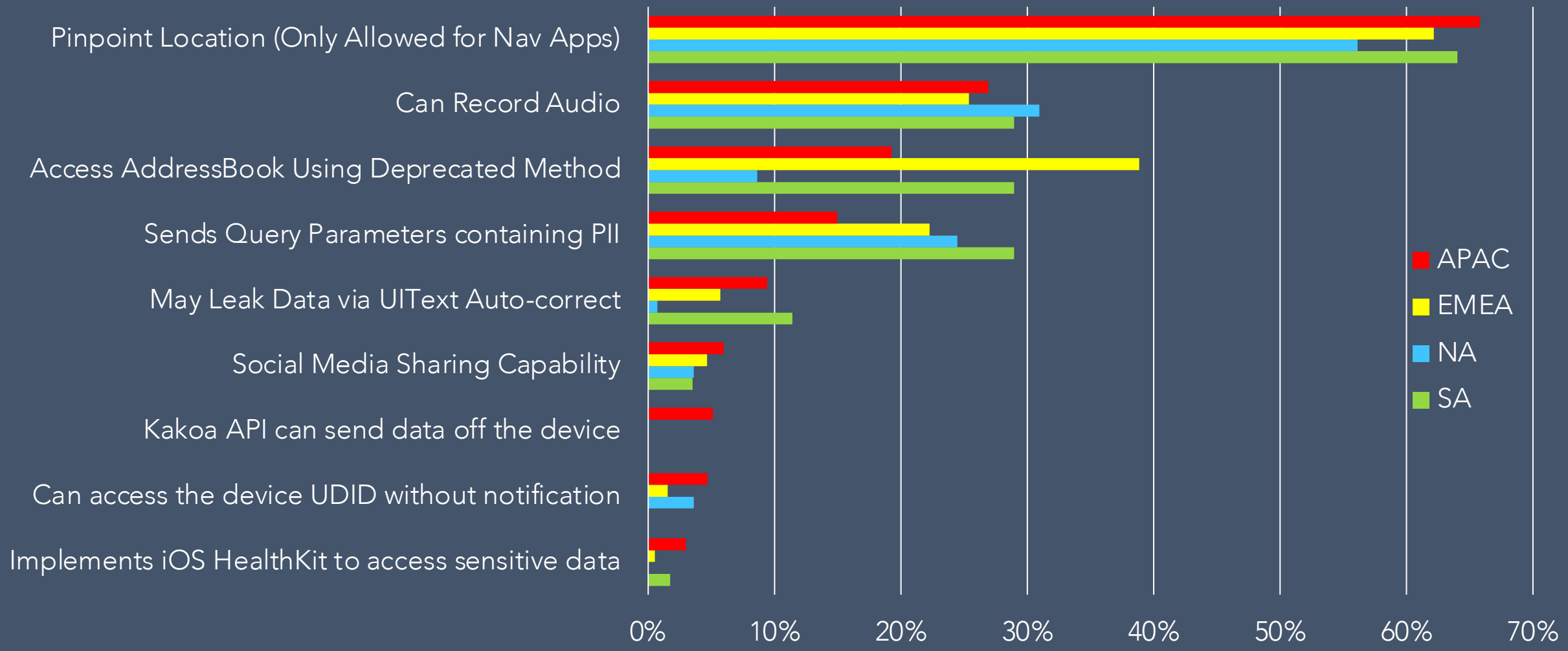
Source: Zimperium

Dangerous Privacy / Leakage Findings



Source: Zimperium

Dangerous Privacy / Leakage Findings

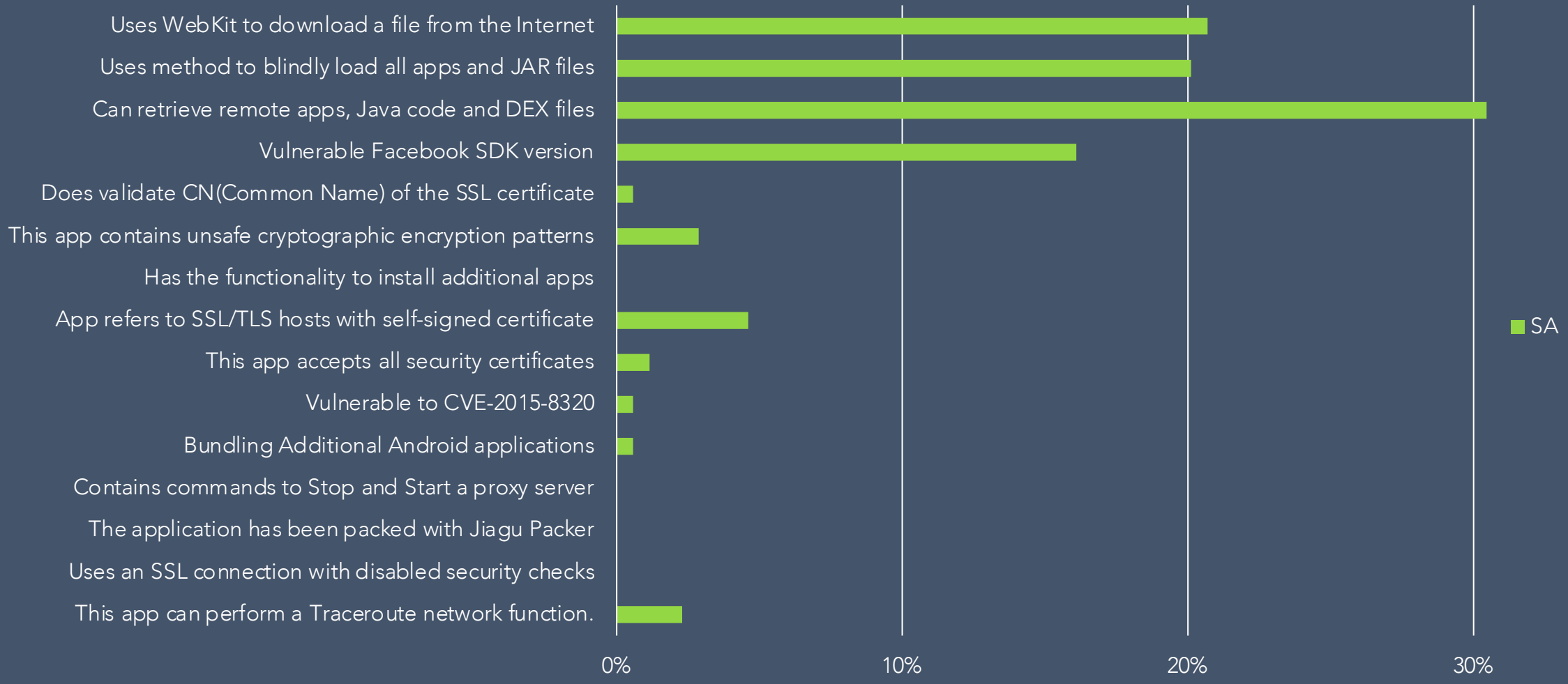


Source: Zimperium

Privacy and Security Risk Distribution

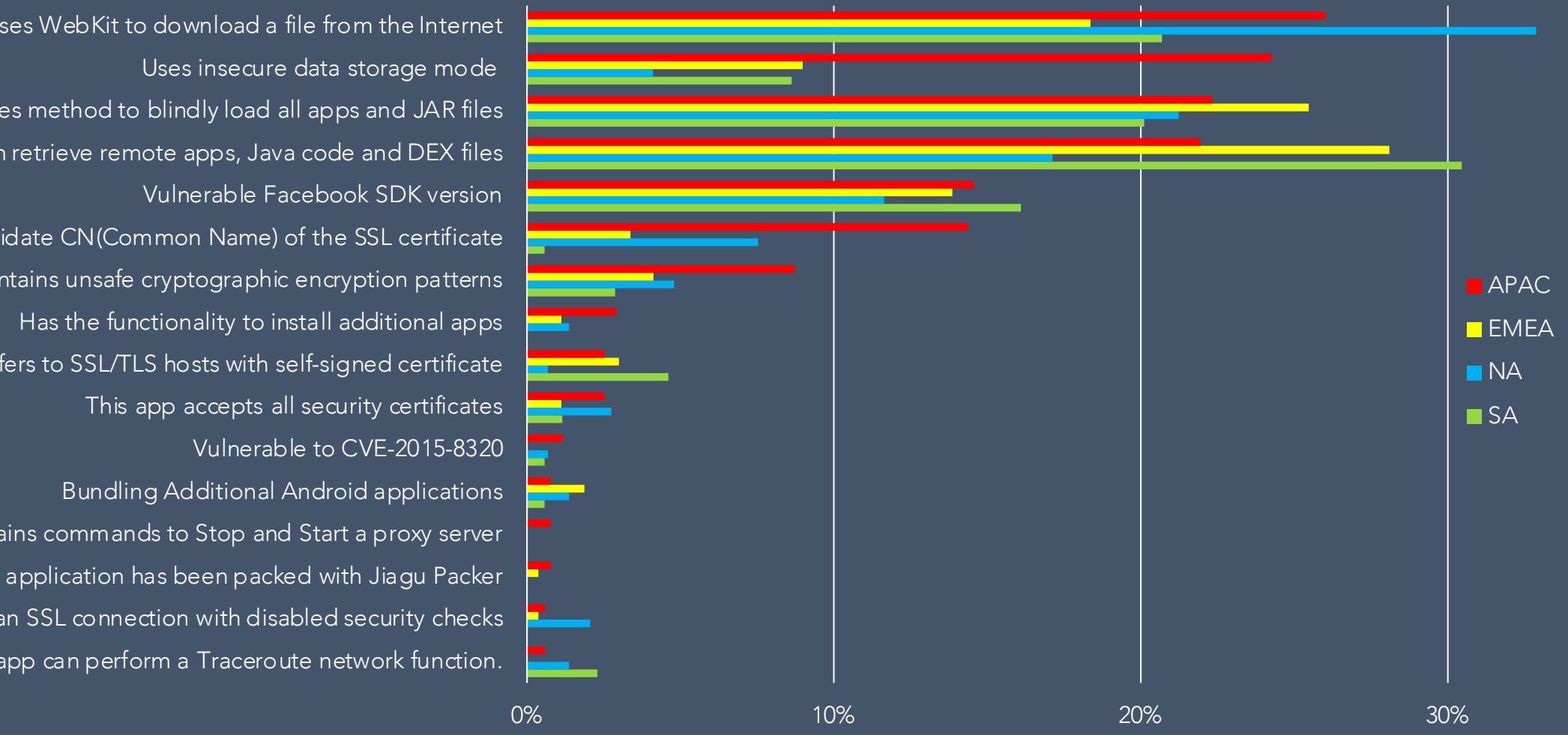
Source: Zimperium

Critical Security Findings



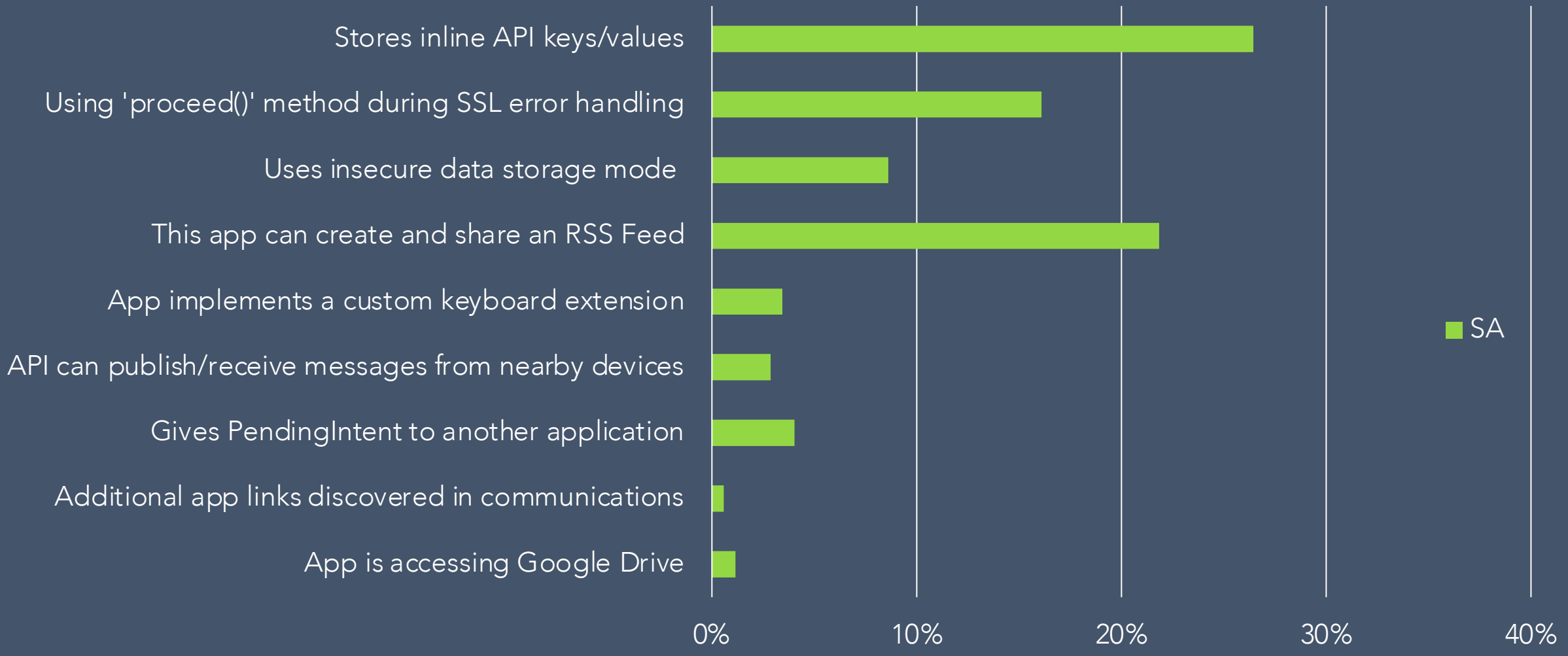
Source: Zimperium

Critical Security Findings



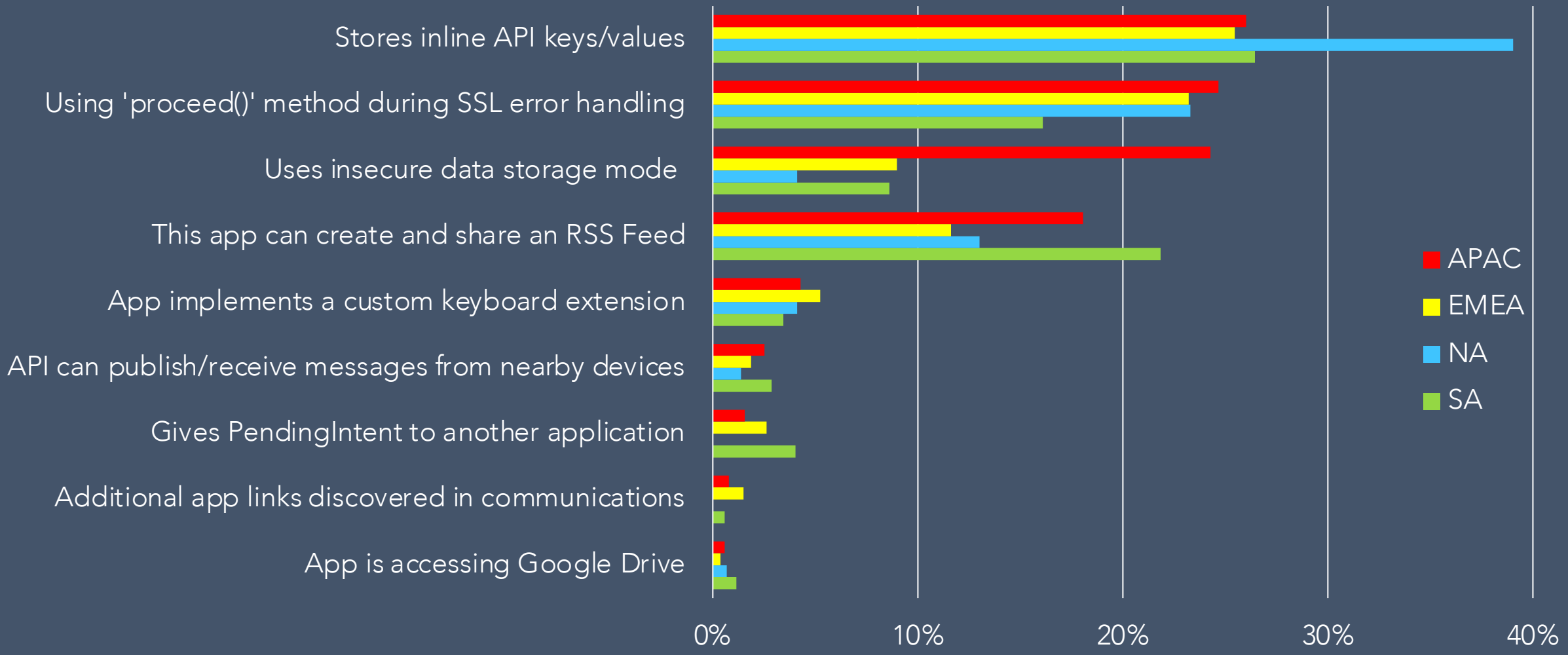
Source: Zimperium

Dangerous Security Findings



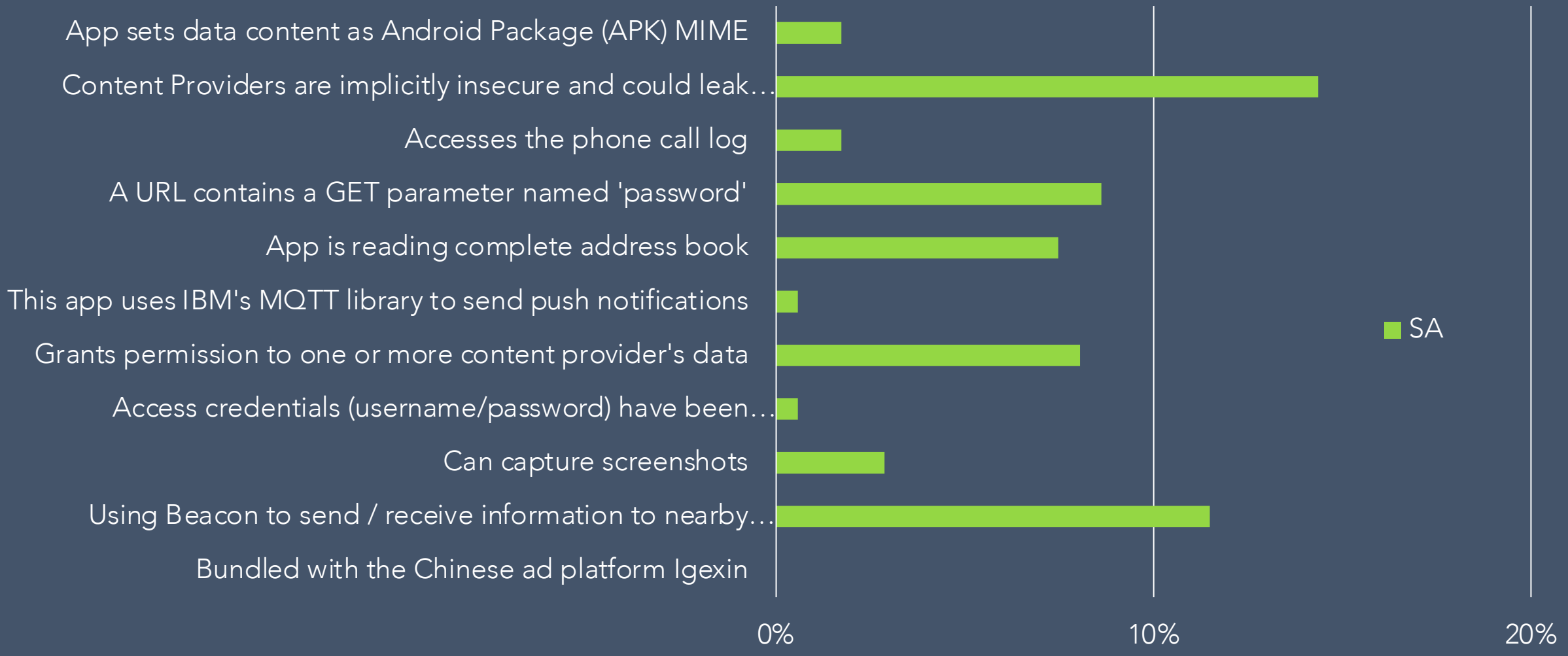
Source: Zimperium

Dangerous Security Findings



Source: Zimperium

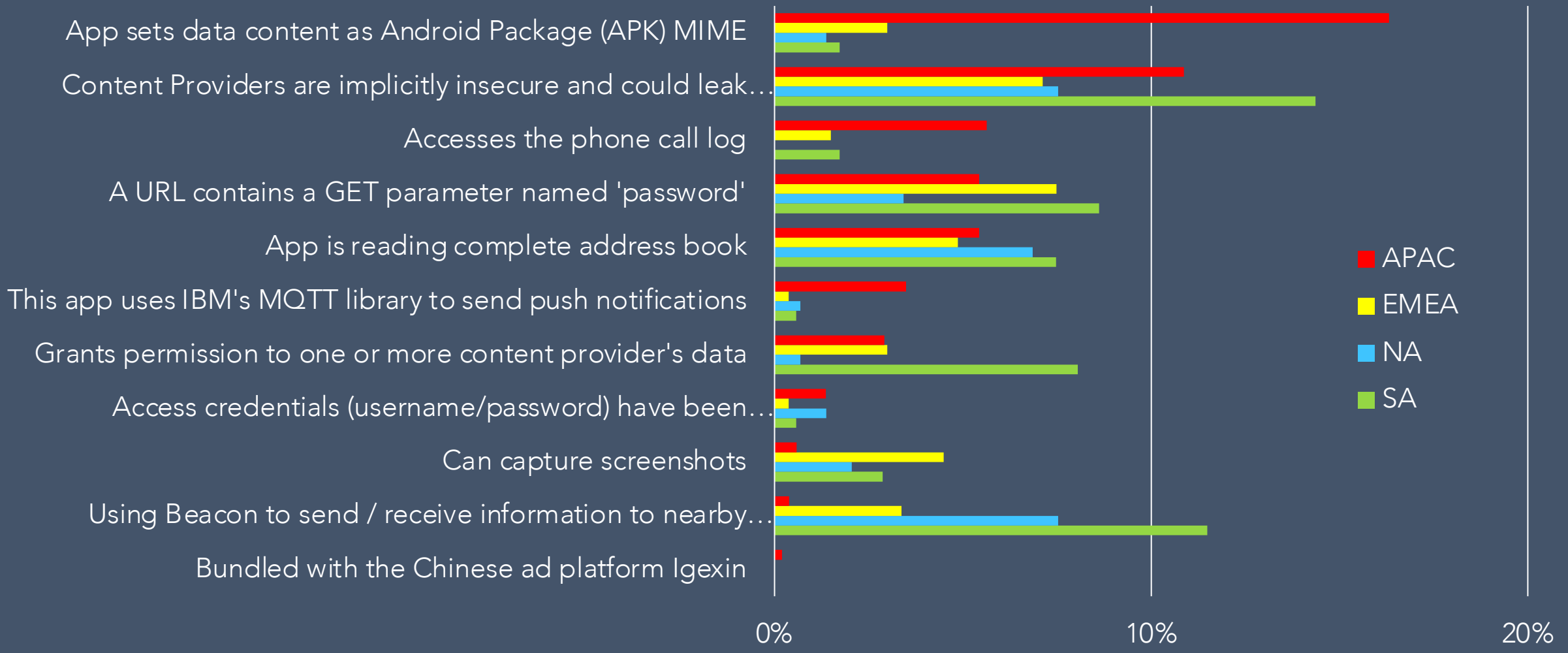
Critical Privacy/Data Leakage Findings



Source: Zimperium

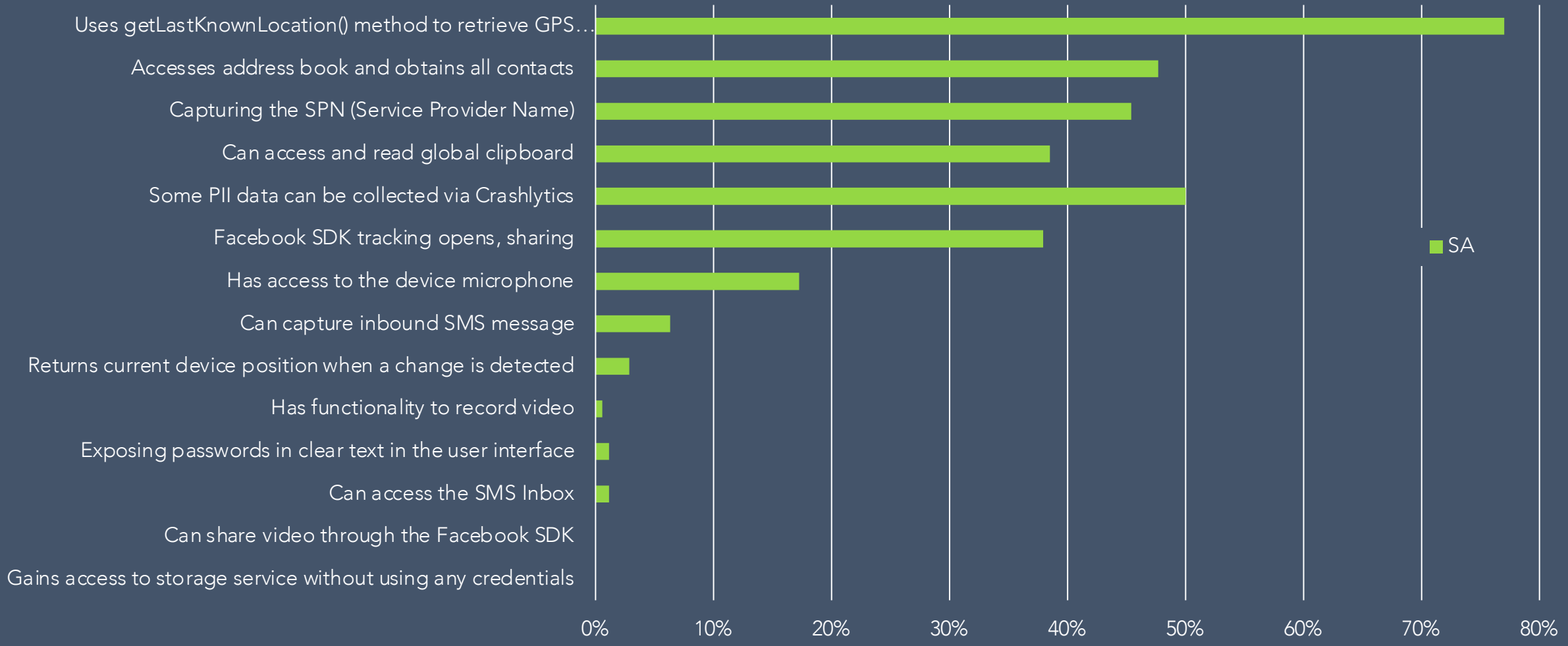
ZIMPERIUM

Critical Privacy/Data Leakage Findings



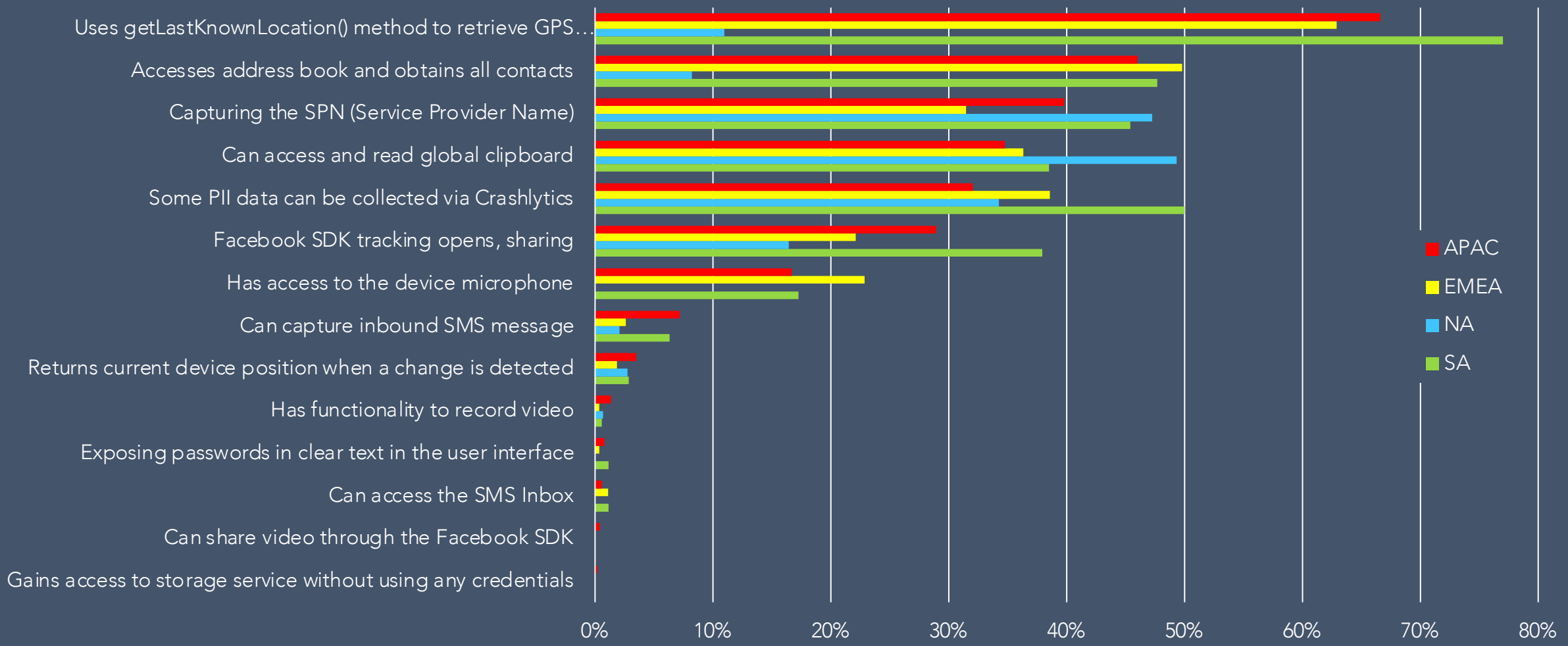
Source: Zimperium

Dangerous Privacy / Leakage Findings



Source: Zimperium

Dangerous Privacy / Leakage Findings



Source: Zimperium

Best Practices and Recommendations

1. Scan and test for app vulnerabilities and risks in the build pipeline to reduce attack surface
2. Shield and harden app to increase reverse engineering difficulty
3. Defend from fraud by measuring vulnerabilities and real-time attacks to customers' devices

About the authors

Scott King

Director Embedded Security

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.