Treat Your Mobile App Like You Treat Your Teenager

ZIMPERIUM®

Agenda

Scott King

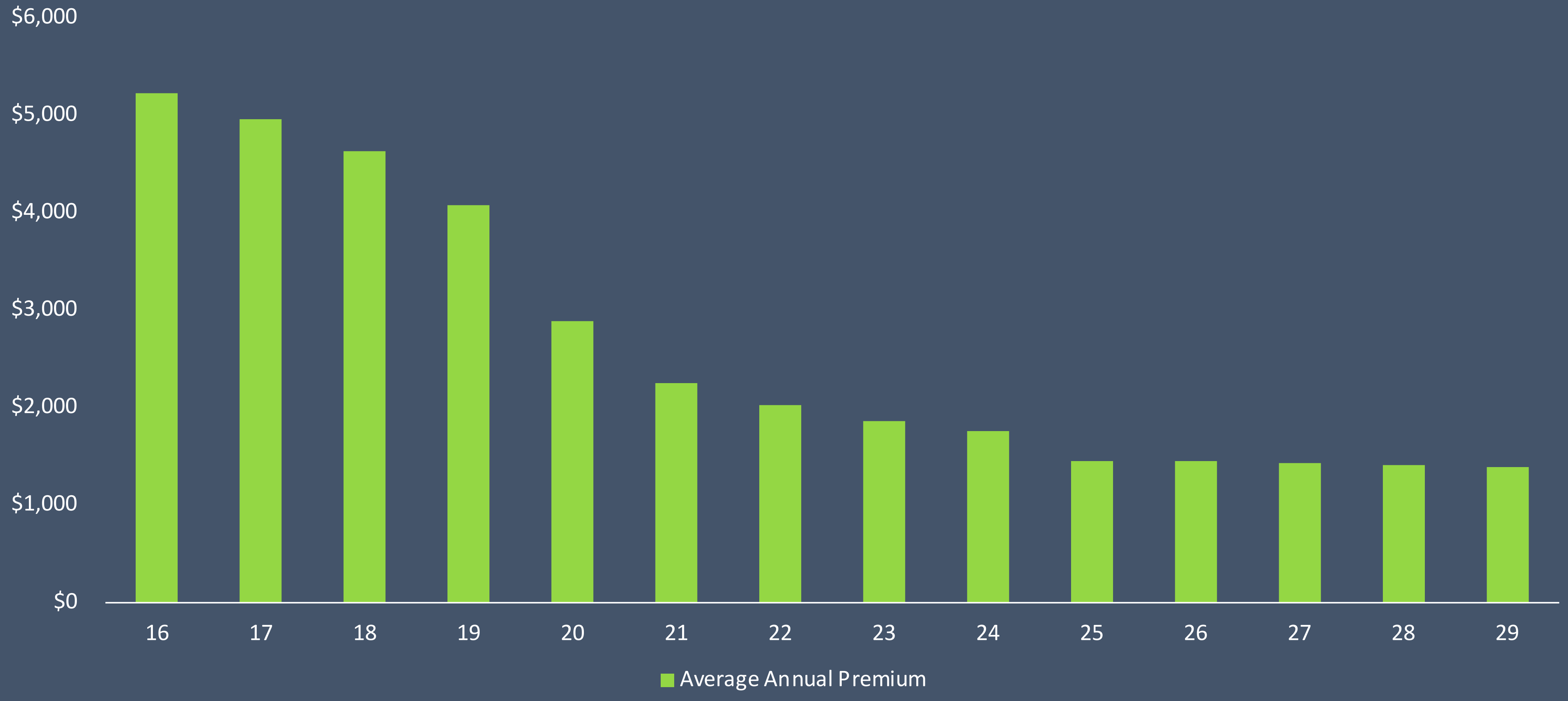
Director Embedded Security

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.

1. Teen decision making and driver statistics
2. Why are teens such bad drivers
3. Accident causes
4. Mobile app failures
5. Mobile app threats and causes
6. Decision making and remediation

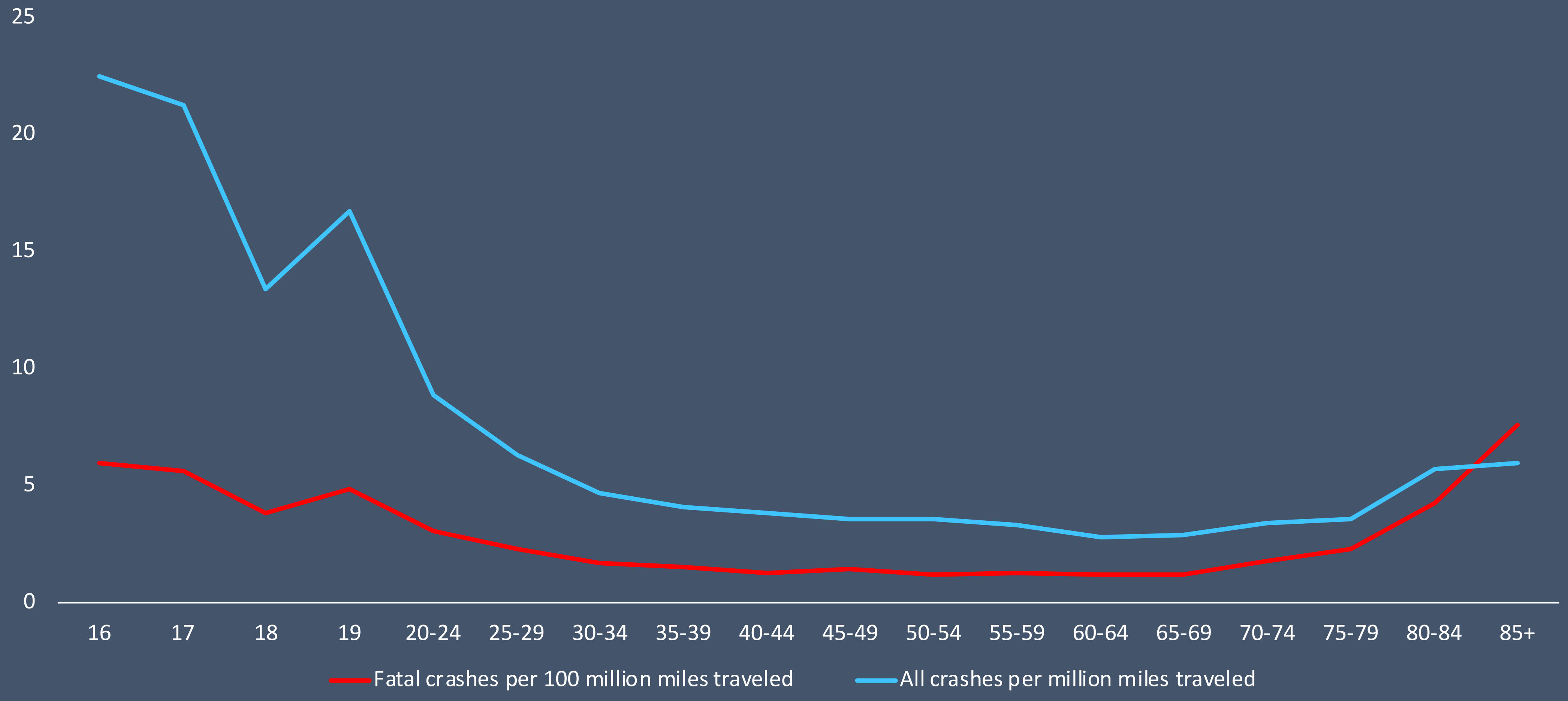
Photo: American Special Ops

Average Annual Car Insurance Premiums by Age



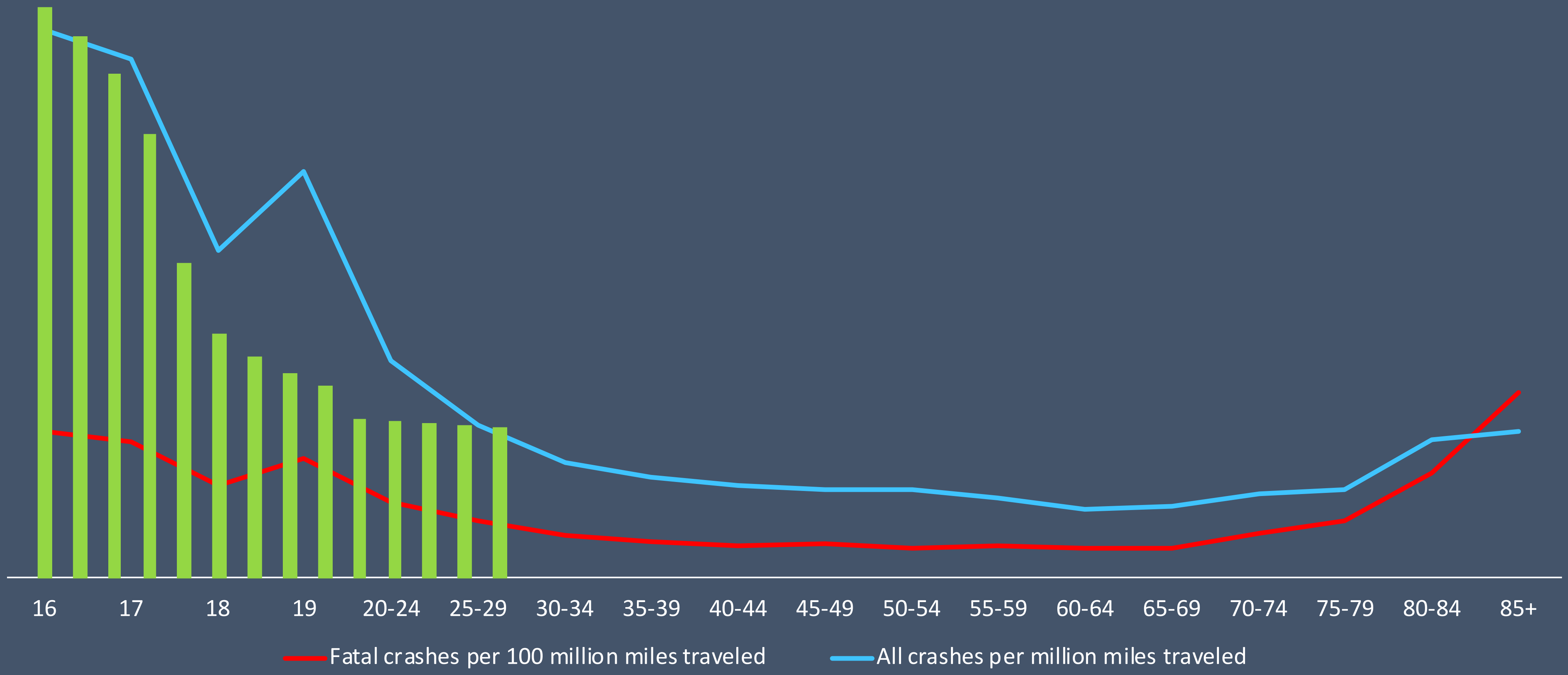
https://www.thezebra.com/car-insurance-age/

Passenger vehicle crash rates per mile traveled, by driver age, 2017



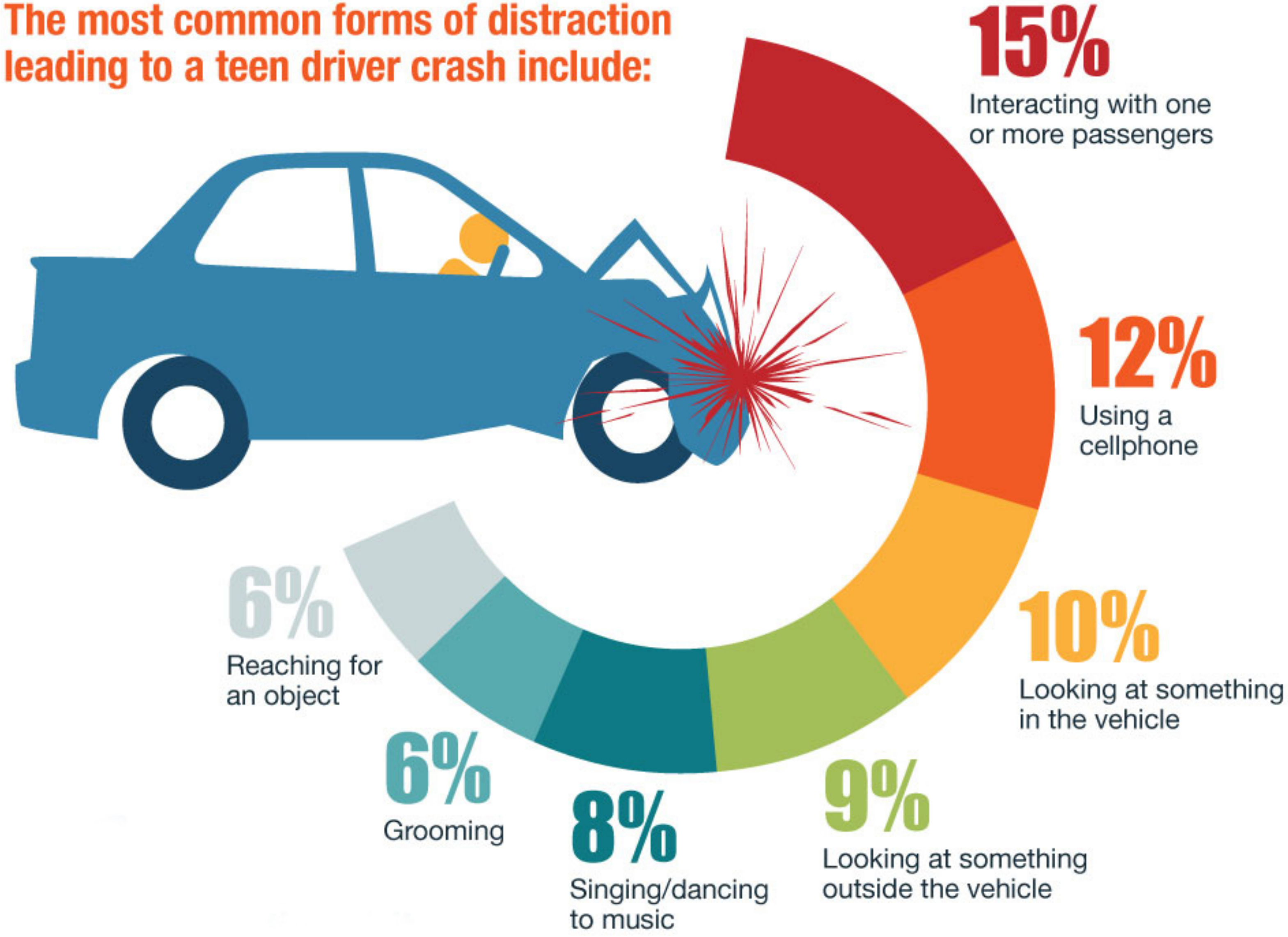
Source: Insurance Institute for Highway Safety

Premiums by Age vs Accident Rates



Source: https://www.thezebra.com/car-insurance-age/
Insurance Institute for Highway Safety

The most common forms of distraction leading to a teen driver crash include:



Source: AAA

Brain Development

Source: AAA

Physical Changes

Source: AAA

Emotion

Source: AAA

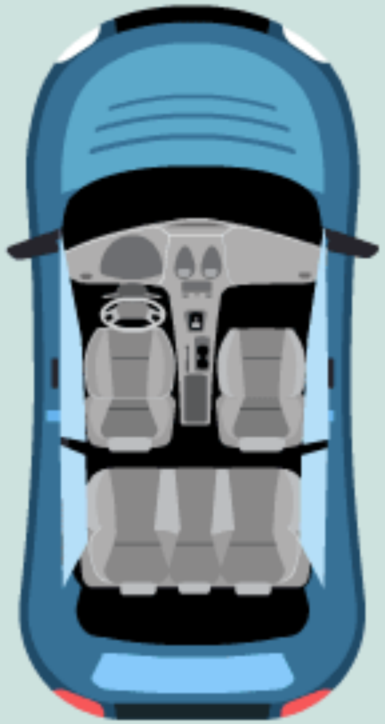
Impulse Control

Source: AAA

Judgement

Source: AAA

Detection



Source: AAA

Remediation

Source: AAA

How do you deploy a threat sensor in your mobile app?

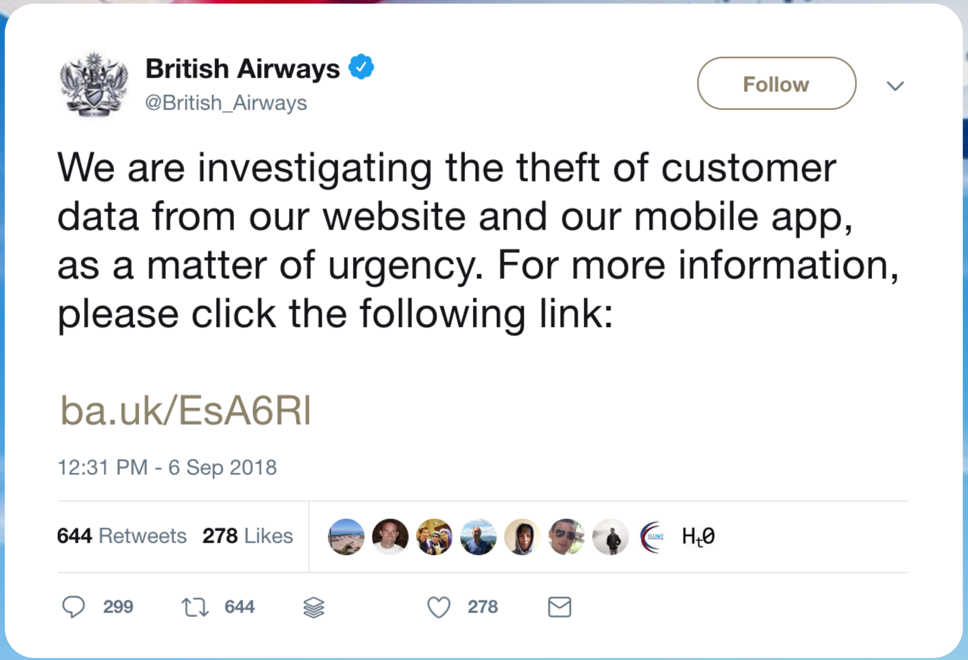
Source: AAA

Hackers Steal £2.5 Overnight from Tesco by Reverse Engineering Mobile App

“It has been revealed weaknesses in the bank’s mobile applications left the door open for cybercriminals to brute force their way in and take more than £2.5 million of customers’ money…”

The Financial Conduct Authority (FCA) later fined Tesco Bank £16.4m for “failing to exercise due skill, care and diligence in protecting” its current account holders.

Sources:
https://www.theguardian.com/business/2016/nov/08/tesco-bank-cyber-thieves-25m
https://www.fca.org.uk/news/press-releases/fca-fines-tesco-bank-failures-2016-cyber-attack



British Airways
@British_Airways

We are investigating the theft of customer data from our website and our mobile app, as a matter of urgency. For more information, please click the following link:

ba.uk/EsA6RI

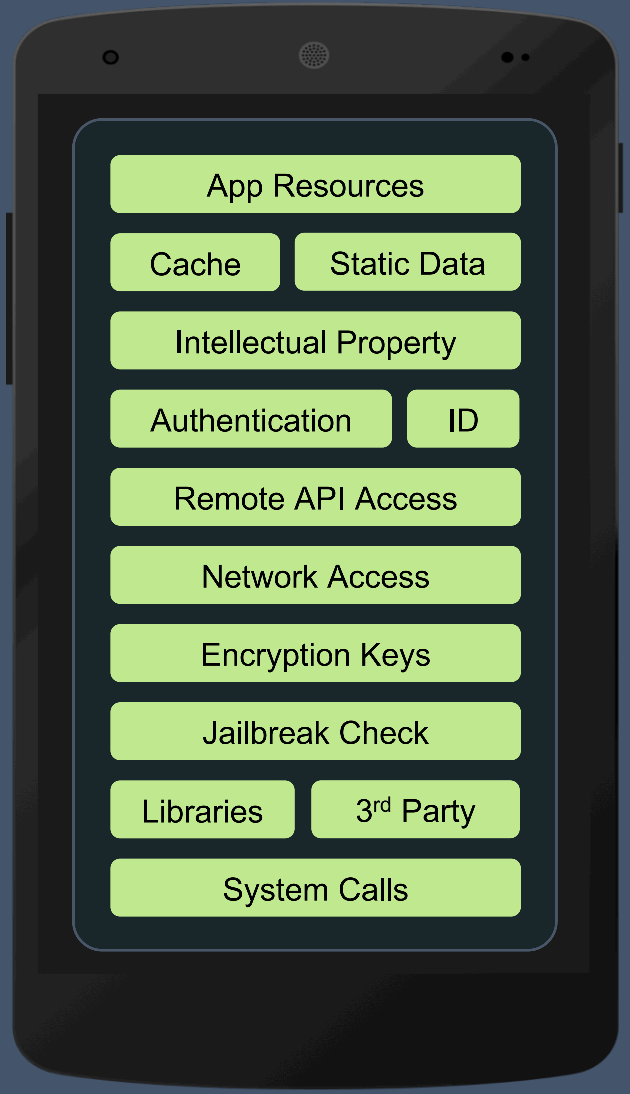
12:31 PM - 6 Sep 2018

644 Retweets 278 Likes

Britain’s data protection watchdog says it will fine British Airways £183.39 million ($229.2 million) under GDPR for security weaknesses that made it possible for hackers to steal information about 500,000 customers.

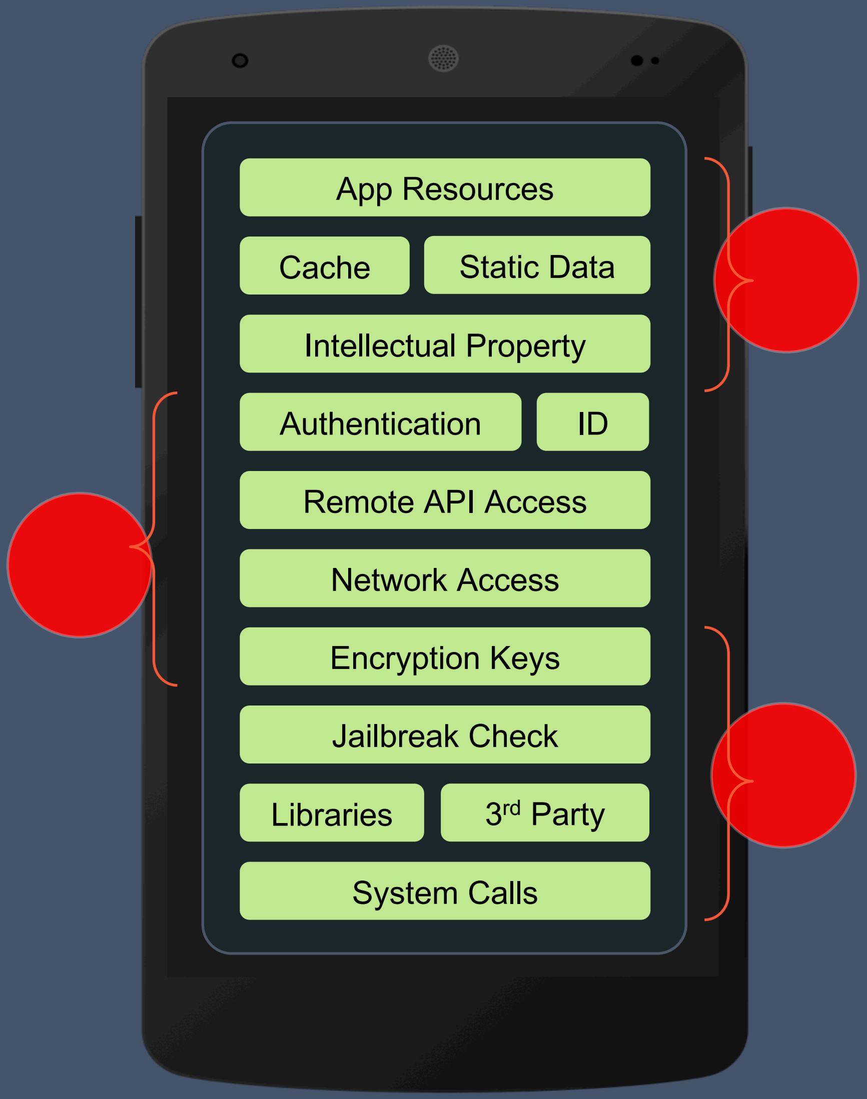
Hackers hijack 7pay mobile app to make illegal charges to customers.

Mobile Attack Surface



Source: NowSecure *Mobile Security Primer*, OWASP *Mobile AppSec Verification v1.1*

Mobile Attack Surface

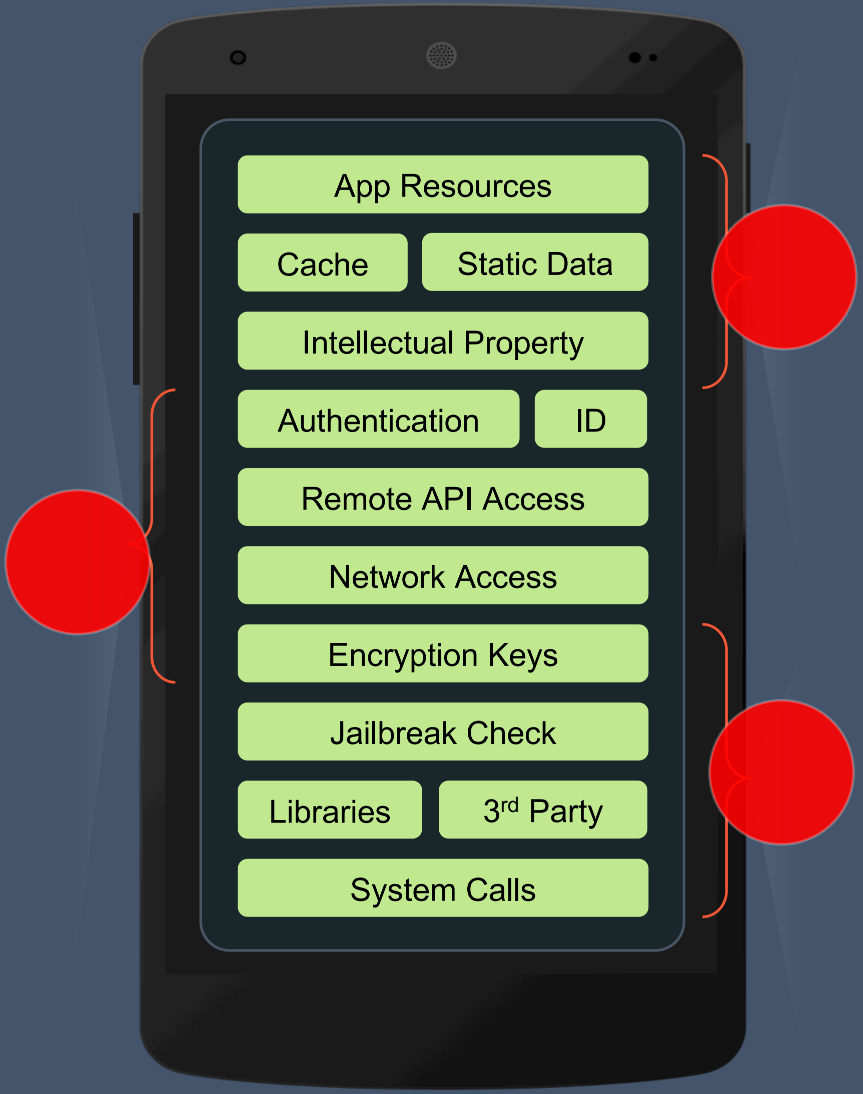


Source: NowSecure *Mobile Security Primer*, OWASP *Mobile AppSec Verification v1.1*

Mobile Attack Surface

SERVER

- Platform Vulnerabilities
- Server Misconfigurations
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Weak Input Validation
- Brute Force Attacks

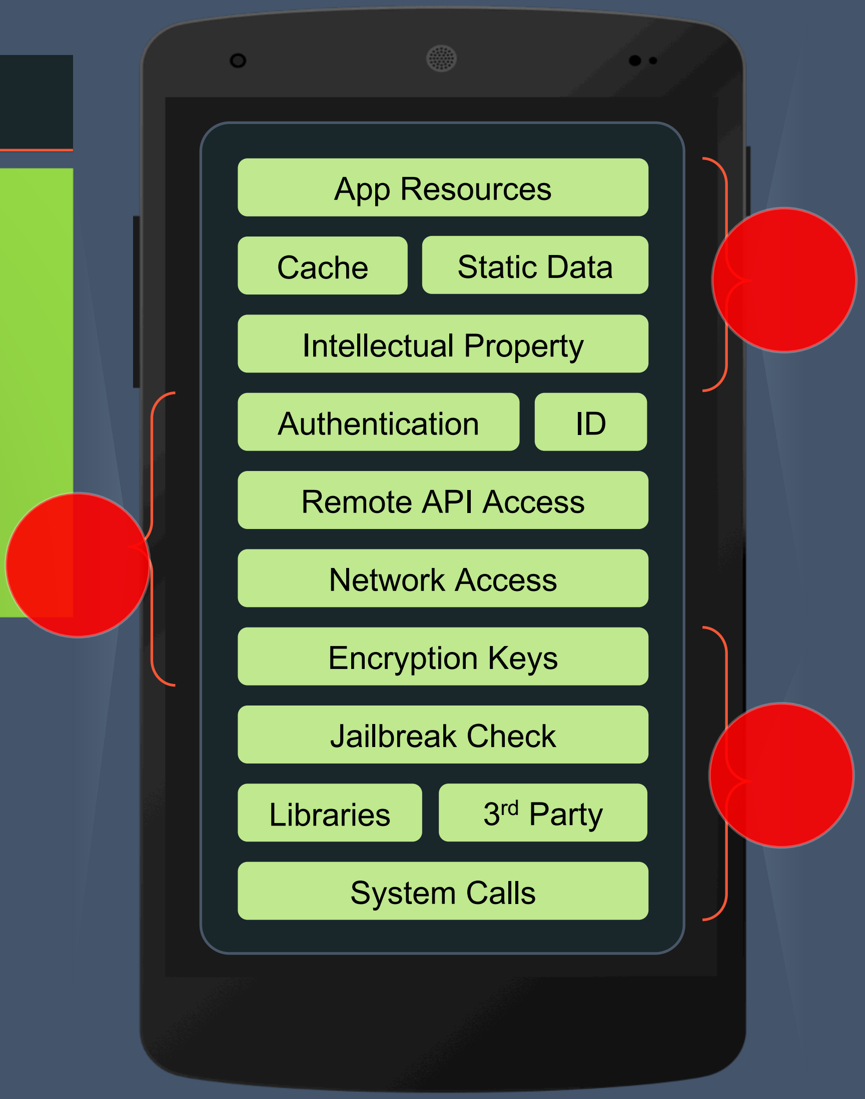


Source: NowSecure *Mobile Security Primer*, OWASP *Mobile AppSec Verification v1.1*

Mobile Attack Surface

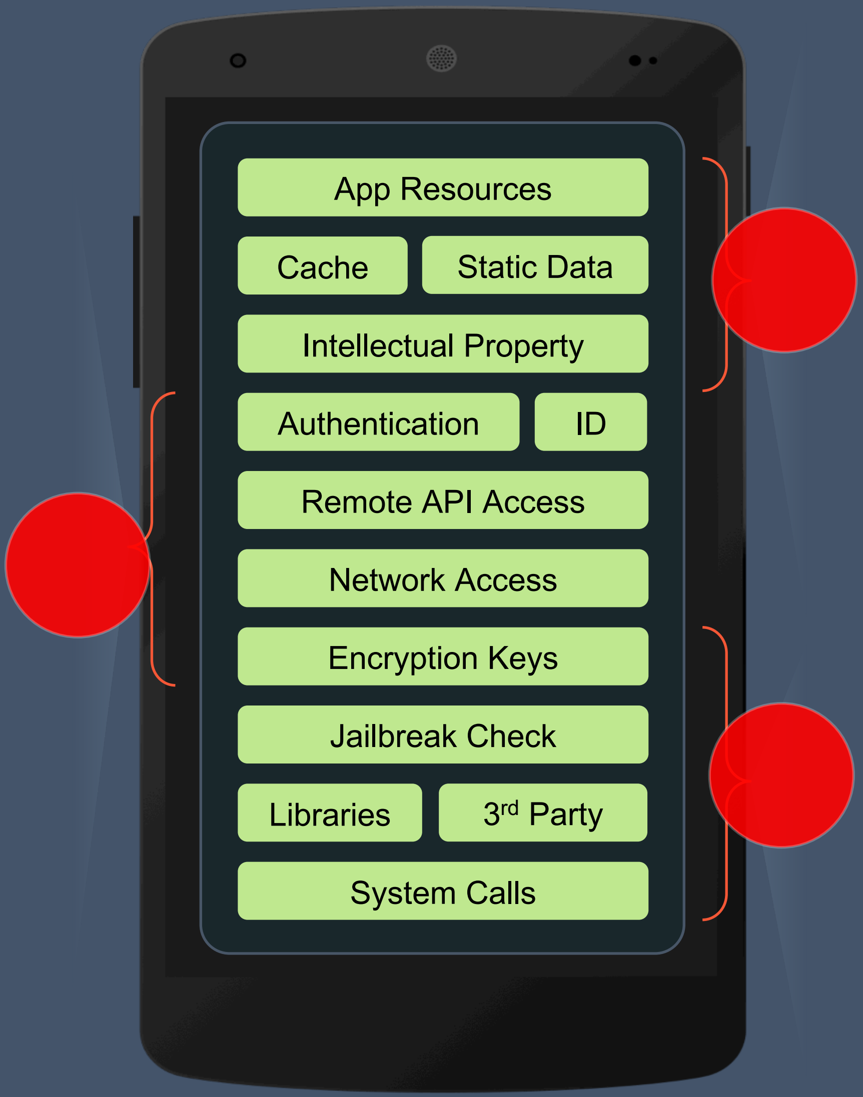
Network

- Rogue Access Point
- ARP MITM
- ICMP Redirect
- TLS Downgrade
- SSL Striping
- Session Hijacking
- Fake SSL Certificates
- DNS Poisoning



Source: NowSecure *Mobile Security Primer*, OWASP *Mobile AppSec Verification v1.1*

Mobile Attack Surface

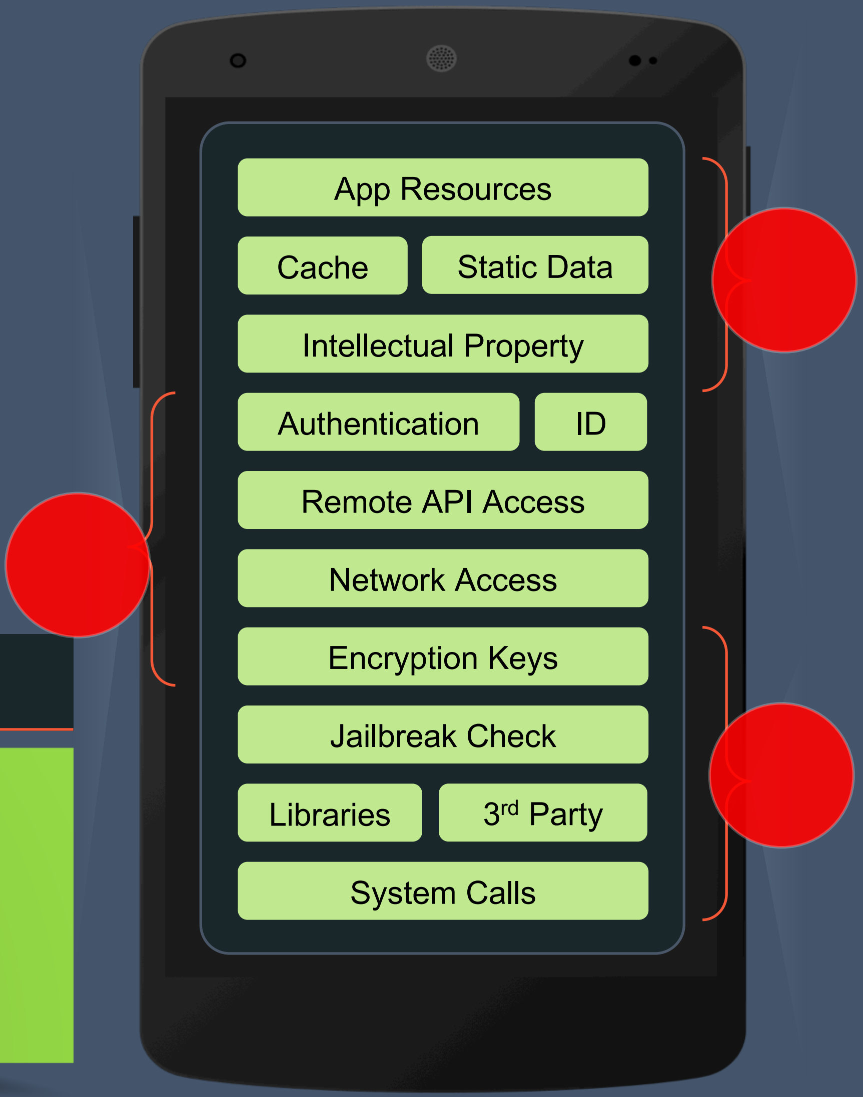


DATABASE

- SQL Injection
- Privilege Escalation
- Data Dumping
- OS Command Execution

Source: NowSecure *Mobile Security Primer*, OWASP *Mobile AppSec Verification v1.1*

Mobile Attack Surface



App Resources

Cache | Static Data

Intellectual Property

Authentication | ID

Remote API Access

Network Access

Encryption Keys

Jailbreak Check

Libraries | 3rd Party

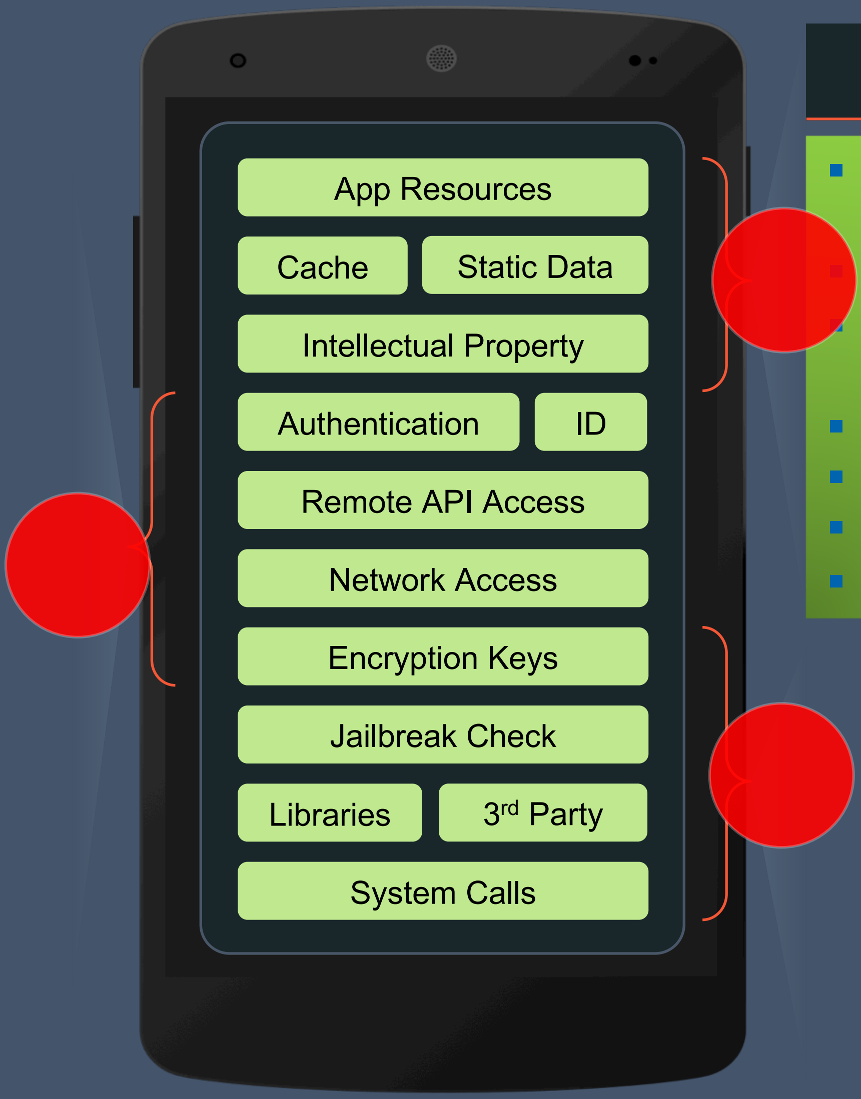
System Calls

Cellular / NFC / BT

- Rogue Cell tower (Femtocells)
- NFC Proxy
- Malicious Bluetooth

Source: NowSecure *Mobile Security Primer*, OWASP *Mobile AppSec Verification v1.1*

Mobile Attack Surface

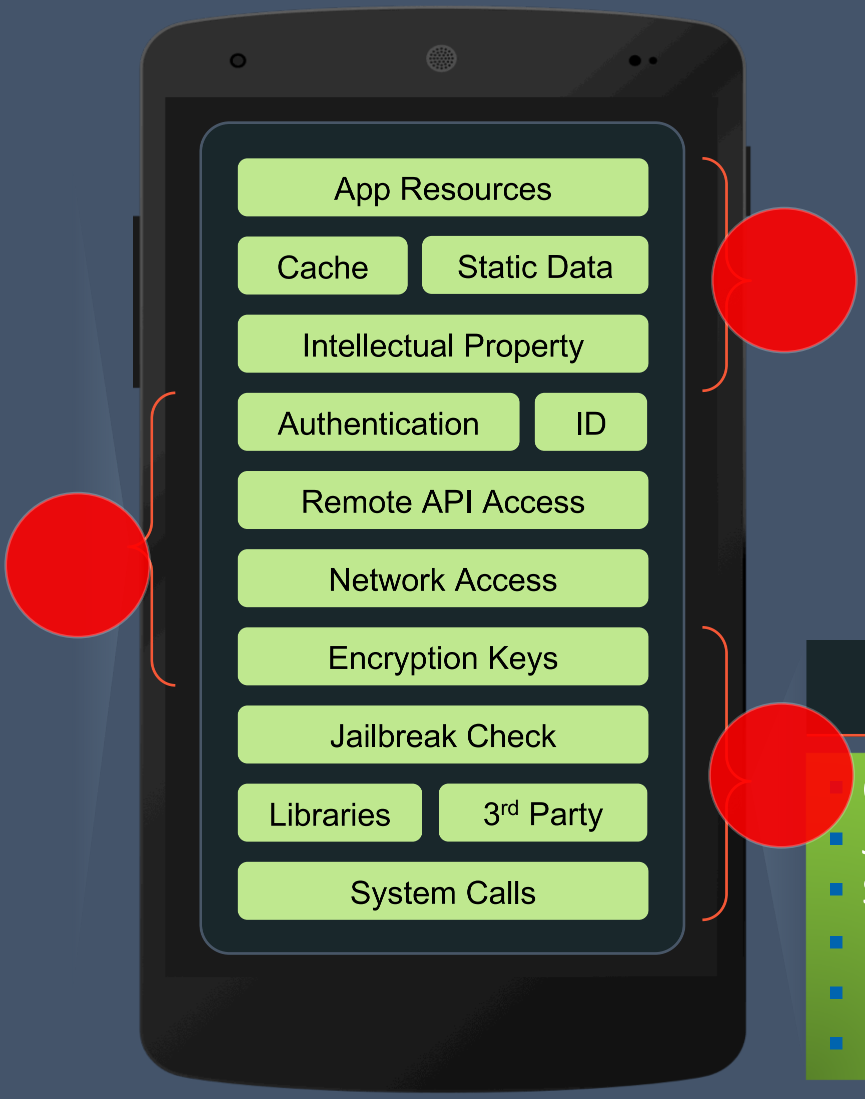


Apps

- **Malware** (Ransomware, Trojans, BankBots, Spyware)
- Repackaged Apps
- 3rd Party Libraries, Back Doors
- Dynamic Runtime Injection
- Swizzling / Hooking
- Key Loggers
- Config Manipulation

Source: NowSecure *Mobile Security Primer*, OWASP *Mobile AppSec Verification v1.1*

Mobile Attack Surface



Device

- OS Vulnerabilities, 0-Days
- Jailbreaking / Rooting
- System Tempering
- Privilege Escalation
- Malicious MMS (Stagefright)
- Download & Execute

Source: NowSecure *Mobile Security Primer*, OWASP *Mobile AppSec Verification v1.1*

Mobile Attack Surface

SERVER

- Platform Vulnerabilities
- Server Misconfigurations
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Weak Input Validation
- Brute Force Attacks

DATABASE

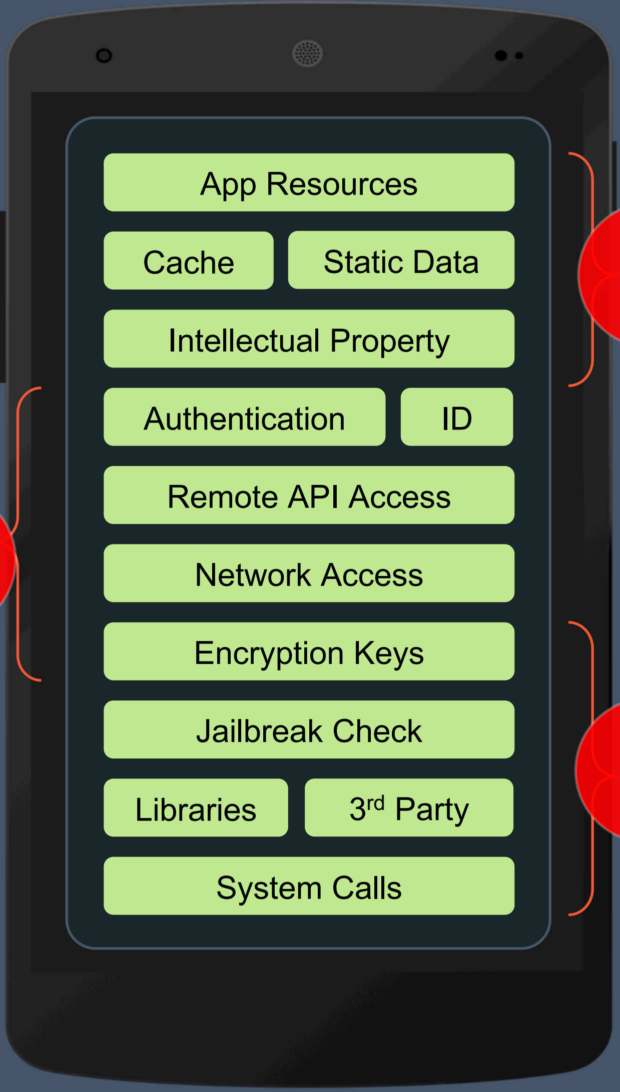
- SQL Injection
- Privilege Escalation
- Data Dumping
- OS Command Execution

Network

- Rogue Access Point
- ARP MITM
- ICMP Redirect
- TLS Downgrade
- SSL Striping
- Session Hijacking
- Fake SSL Certificates
- DNS Poisoning

Cellular / NFC / BT

- Rogue Cell tower (Femtocells)
- NFC Proxy
- Malicious Bluetooth



App Resources

Cache | Static Data

Intellectual Property

Authentication | ID

Remote API Access

Network Access

Encryption Keys

Jailbreak Check

Libraries | 3rd Party

System Calls

Apps

- **Malware** (Ransomware, Trojans, BankBots, Spyware)
- Repackaged Apps
- 3rd Party Libraries, Back Doors
- Dynamic Runtime Injection
- Swizzling / Hooking
- Key Loggers
- Config Manipulation

Device

- OS Vulnerabilities, 0-Days
- Jailbreaking / Rooting
- System Tempering
- Privilege Escalation
- Malicious MMS (Stagefright)
- Download & Execute

Source: NowSecure *Mobile Security Primer*, OWASP *Mobile AppSec Verification v1.1*

Mobile App Security Tooling

Static Code Analysis	App Shielding	App Tempering	Identity | 2FA | MFA
Locks	Locks	Locks	Keys

Fraud Detection (Server Side / Browser)	Cryptography	Pen Testing (Service Providers)	Runtime Application Self Protection (RASP)
Keys	Keys	Engine / Road Test	Airbags

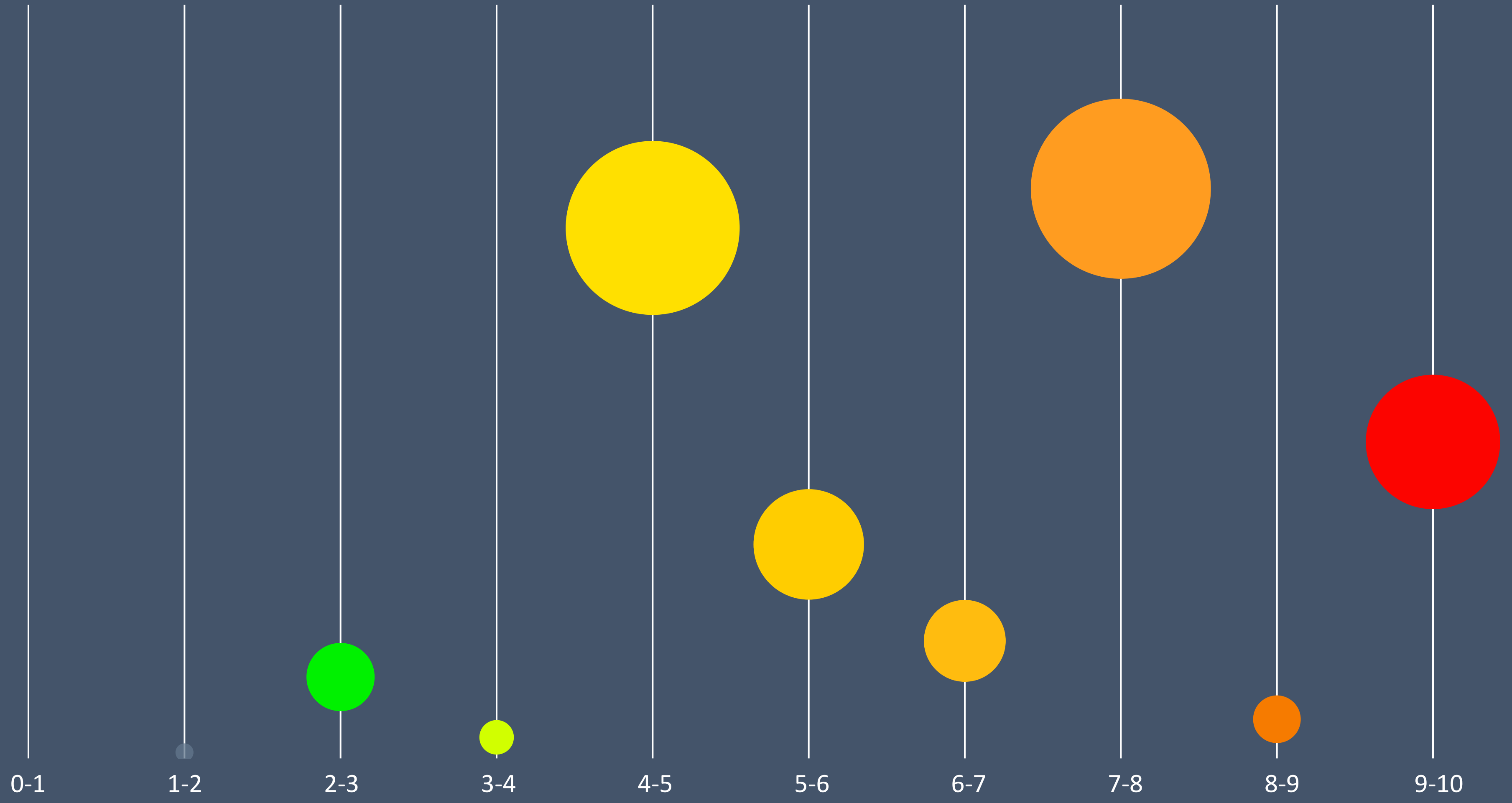
Mobile App Security Tooling

Static Code Analysis	Locks
App Shielding	Locks
App Tempering	Locks
Identity | 2FA | MFA	Keys
Fraud Detection (Server Side / Browser)	Keys
Cryptography	Keys
Pen Testing (Service Providers)	Engine / Road Test
Runtime Application Self Protection (RASP)	Airbags

No amount of app hardening can detect a cyberattack.

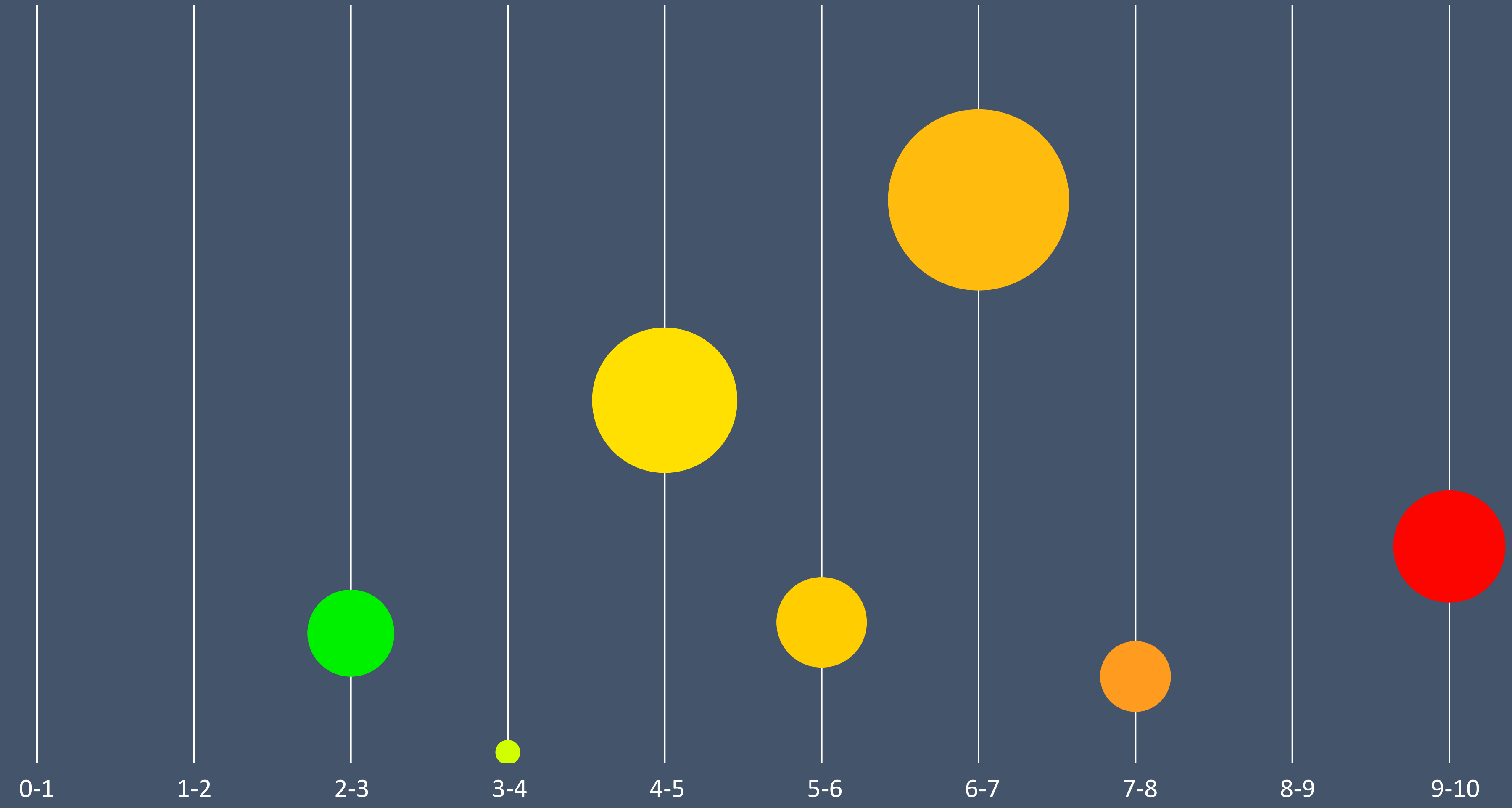
You cannot remediate an attack you cannot identify.

Android CVEs registered 2018 – April 2019



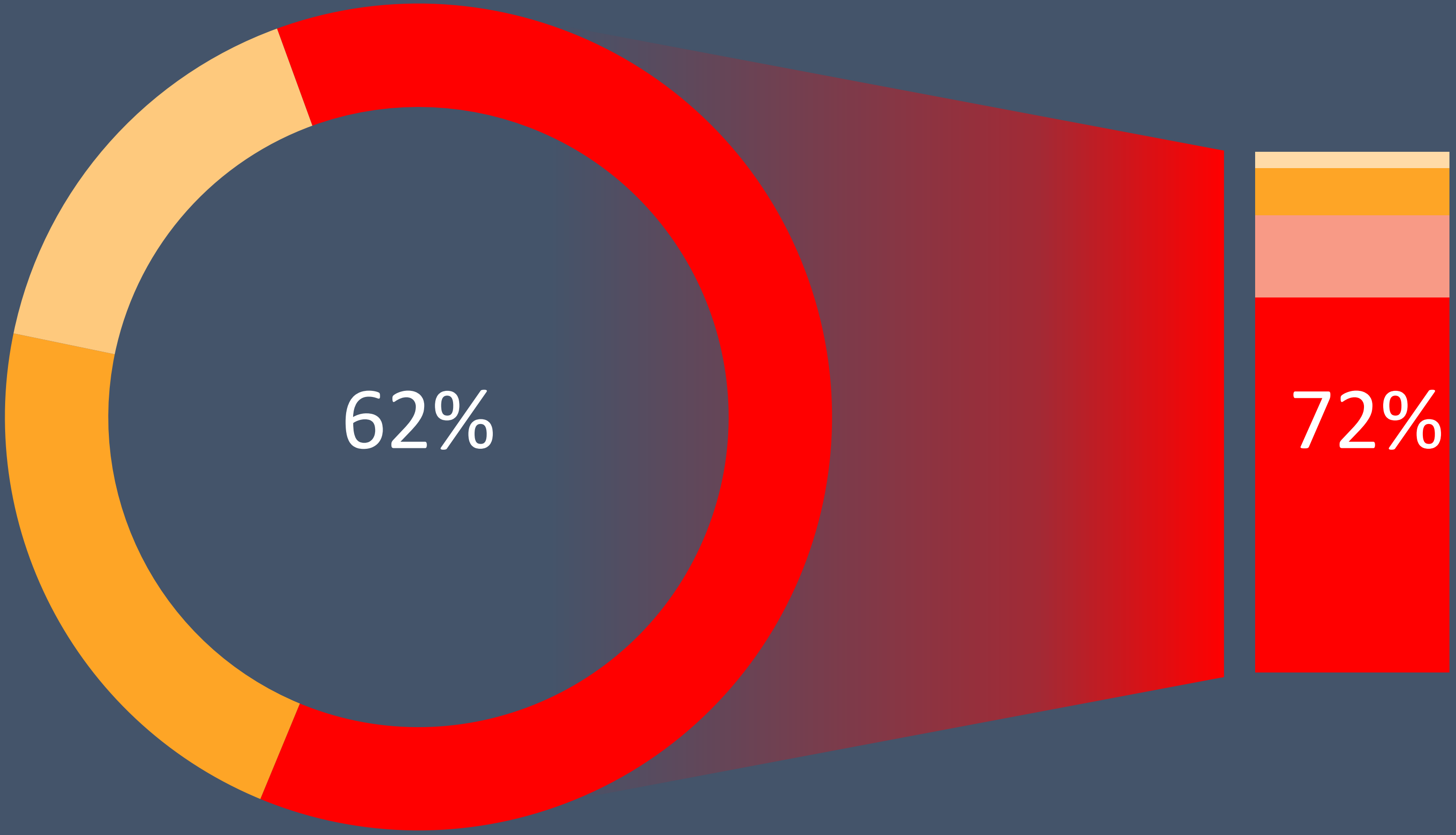
CVEs registered 2018 – April 2019
cve.mitre.org, Alphabet, Inc.

iOS CVEs registered 2018 – April 2019



CVEs registered 2018 – April 2019
cve.mitre.org, Apple, Inc.

72% of critical iOS CVEs allowed code injection

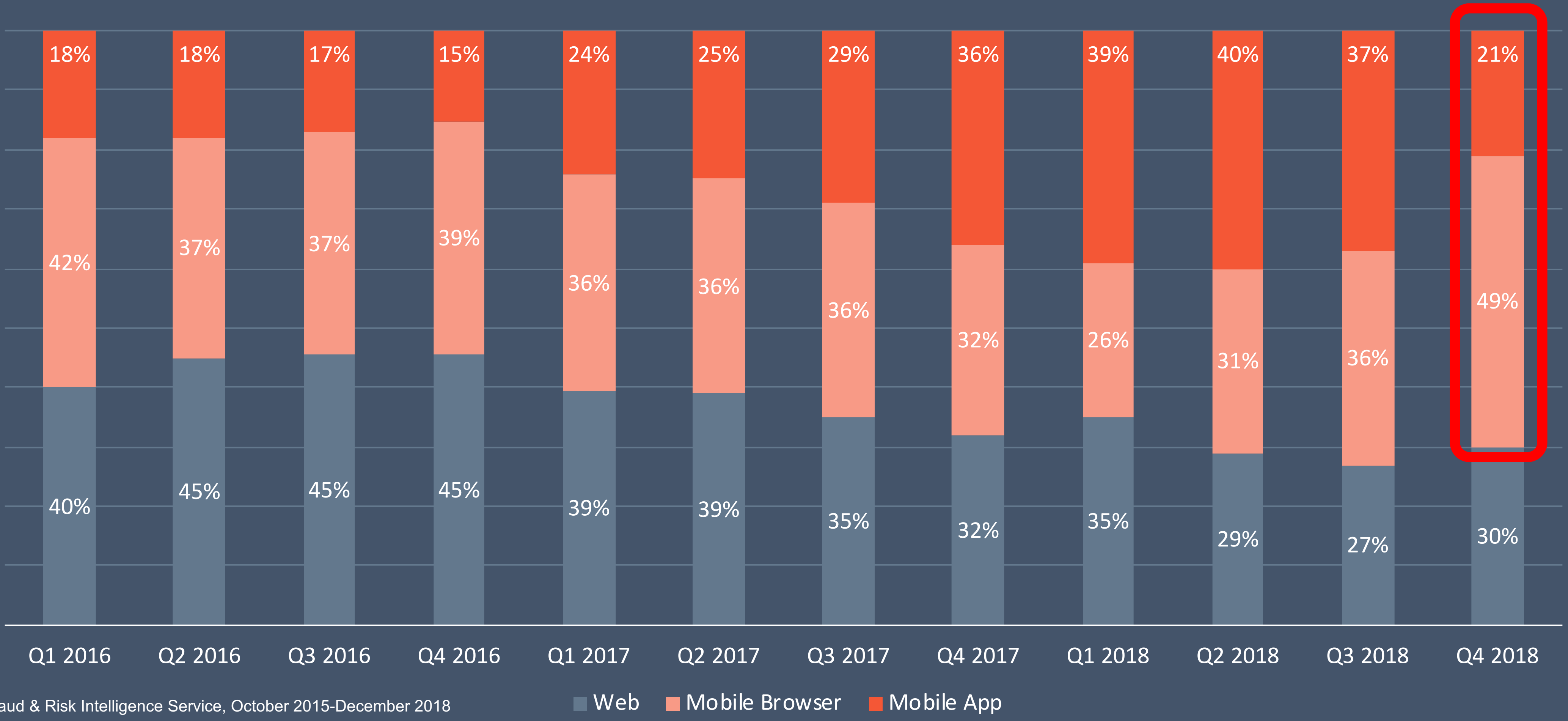


Critical Vulnerabilities

Code injection

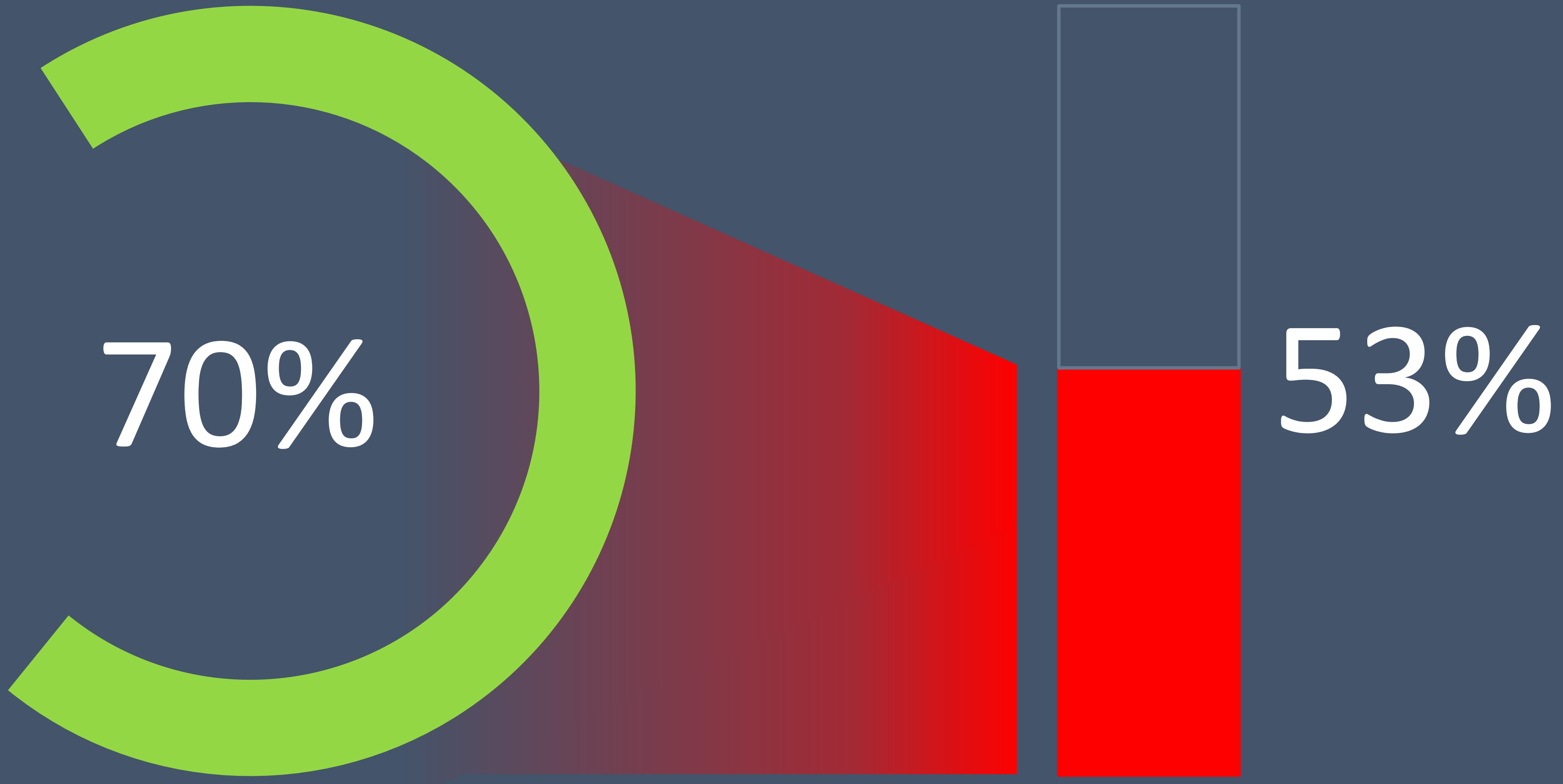
CVEs patched 2018 – March 2019
cve.mitre.org, Apple, Inc.

70% of Fraud Originated in a Mobile Browser/App



RSA Fraud & Risk Intelligence Service, October 2015-December 2018

Are the apps you build secure?

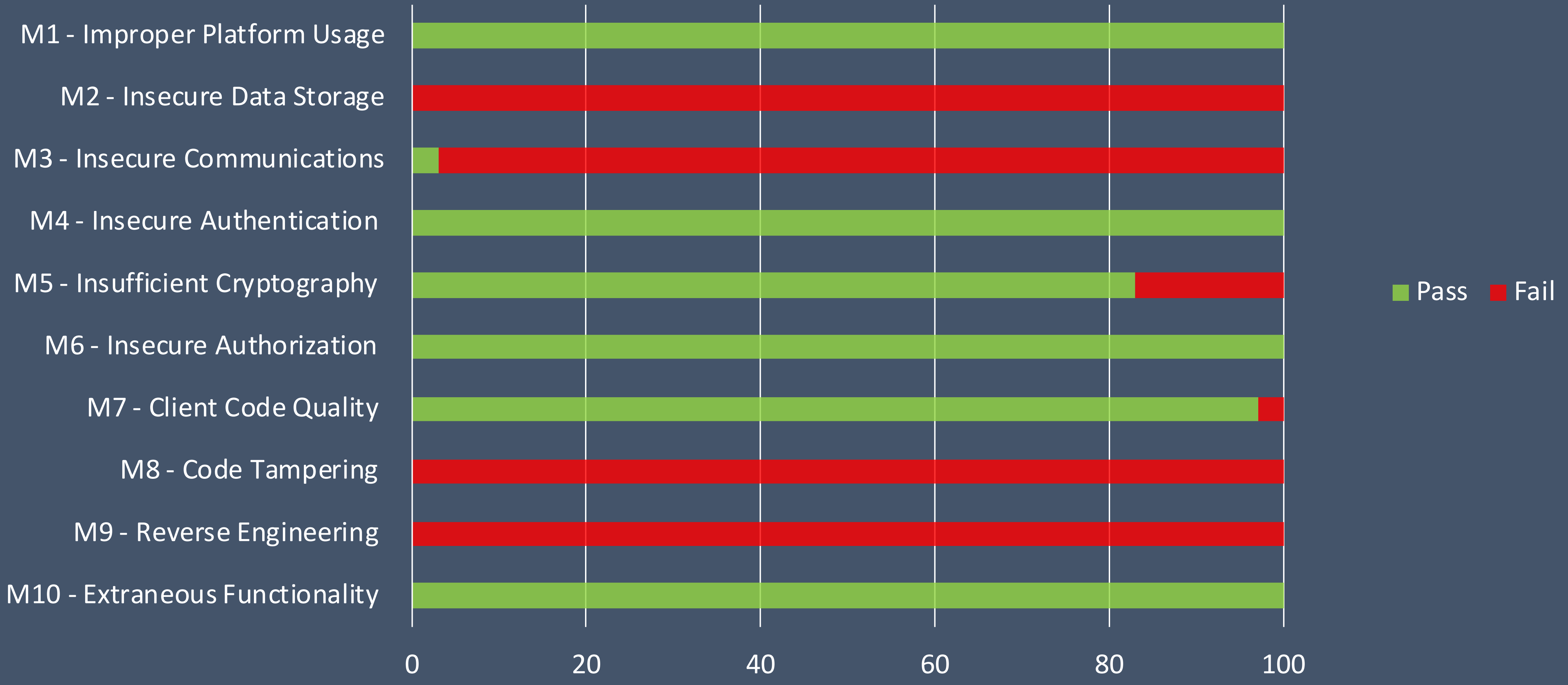


Do you build your own app?

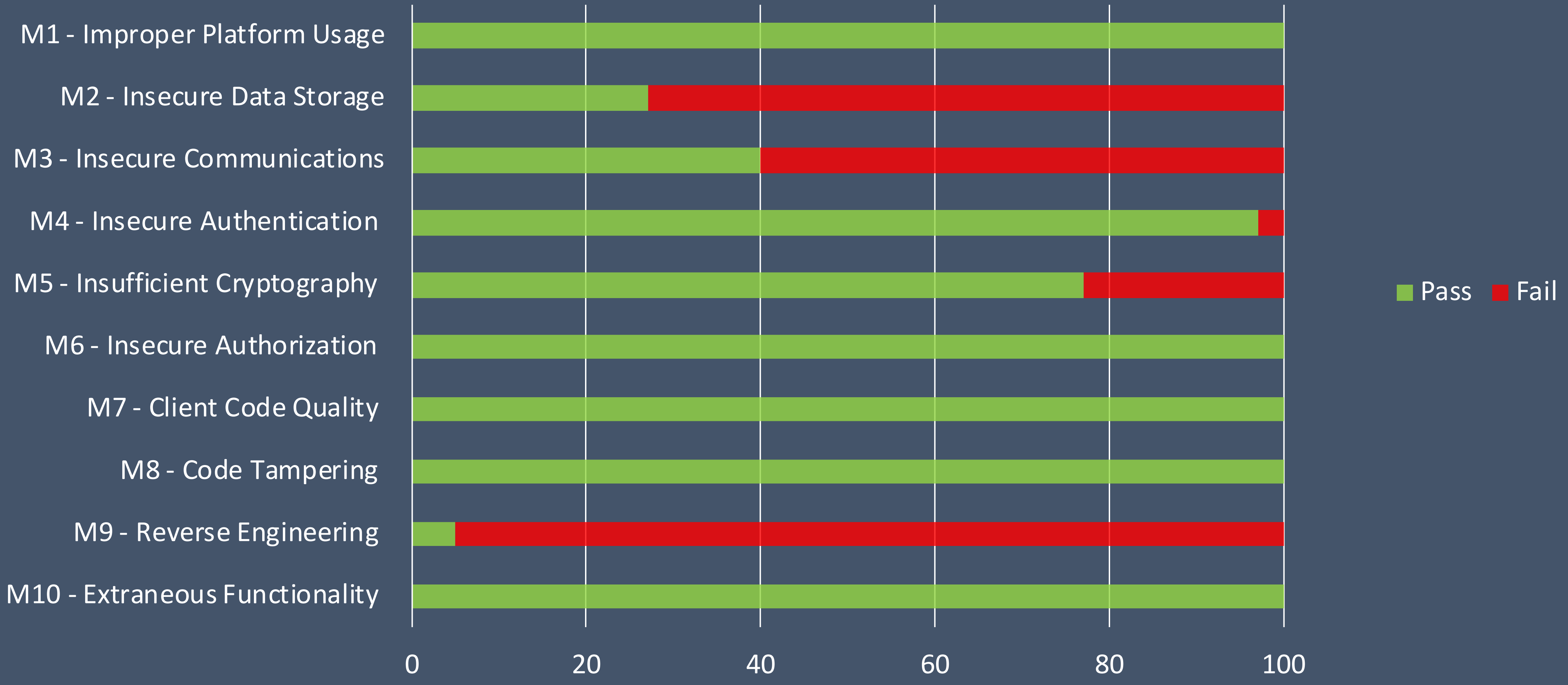
Are you concerned about insecure coding?

Verizon Mobile Security Index 2019

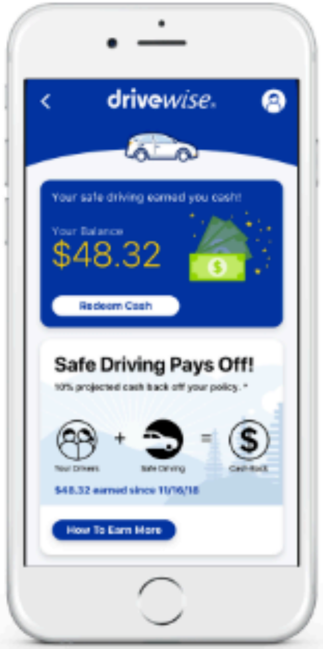
OWASP Mobile Top 10



OWASP Mobile Top 10



Insurance agencies want data on your driving



drivewise.

Your safe driving earned you cash!

Your Balance

$48.32

Redeem Cash

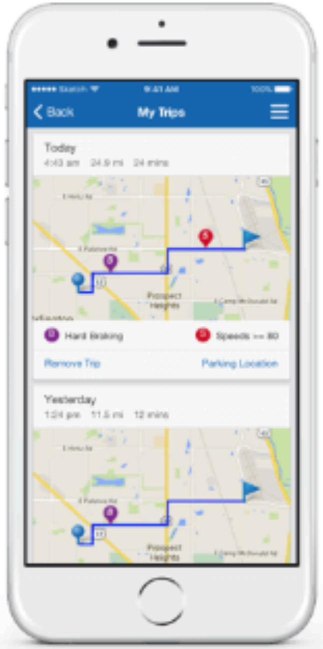
Safe Driving Pays Off!

10% projected cash back off your policy. *

Your Drivers + Safe Driving = Cash Back

$48.32 earned since 11/16/18

How To Earn More



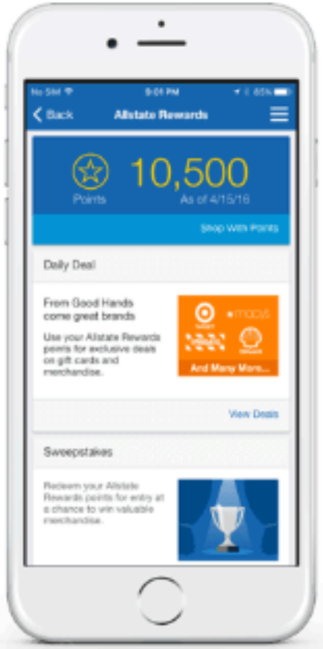
Back · My Trips

Today
4:43 am 24.9 mi 24 mins

Hard Braking · Speeds >= 80

Remove Trip · Parking Location

Yesterday
1:24 pm 11.5 mi 12 mins



No SIM · 9:01 PM · 85%

Back · Allstate Rewards

10,500
Points
As of 4/15/16

Shop With Points

Daily Deal

From Good Hands come great brands

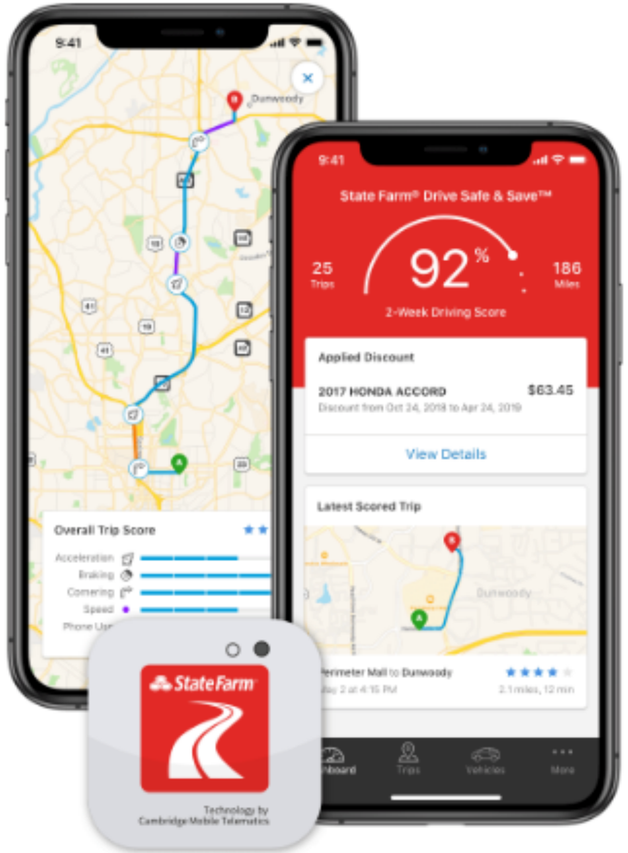
Use your Allstate Rewards points for exclusive deals on gift cards and merchandise.

And Many More...

View Deals

Sweepstakes

Redeem your Allstate Rewards points for entry at a chance to win valuable merchandise.



9:41

State Farm® Drive Safe & Save™

25 Trips · 92% · 186 Miles

2-Week Driving Score

Applied Discount

2017 HONDA ACCORD · $63.45
Discount from Oct 24, 2018 to Apr 24, 2019

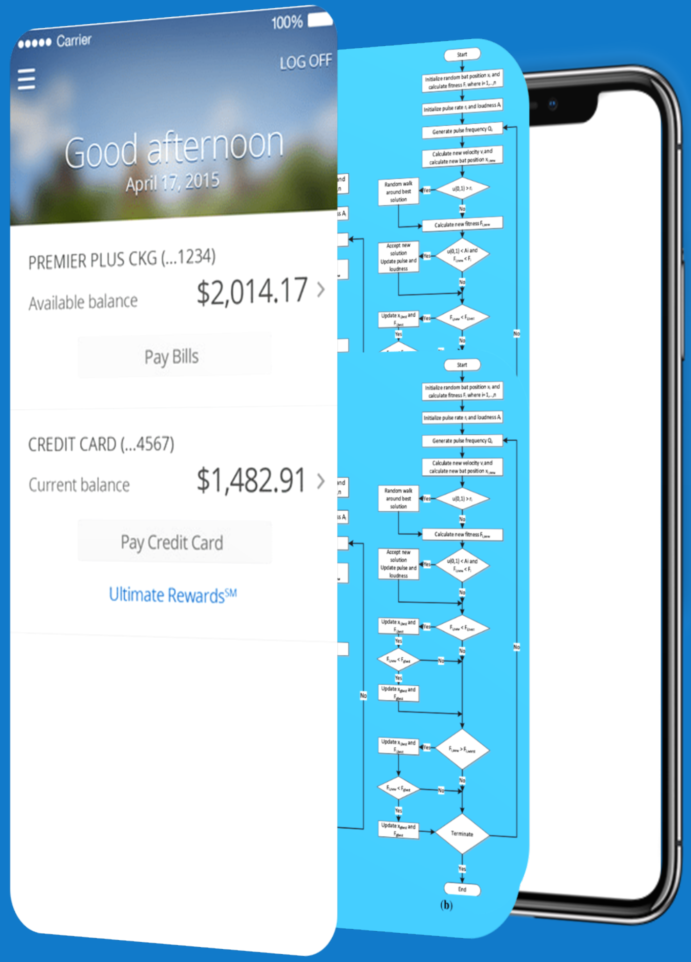
View Details

Latest Scored Trip

Perimeter Mall to Dunwoody ★★★★☆
May 2 at 4:15 PM · 2.1 miles, 12 min

Dashboard · Trips · Vehicles · More

Global Bank Detects Fraud via Mobile Channel



PREMIER PLUS CKG (...1234)
Available balance $2,014.17

CREDIT CARD (...4567)
Current balance $1,482.91

Mobile threat detection aids in reducing $1.1 Billion in fraud via the mobile channel.

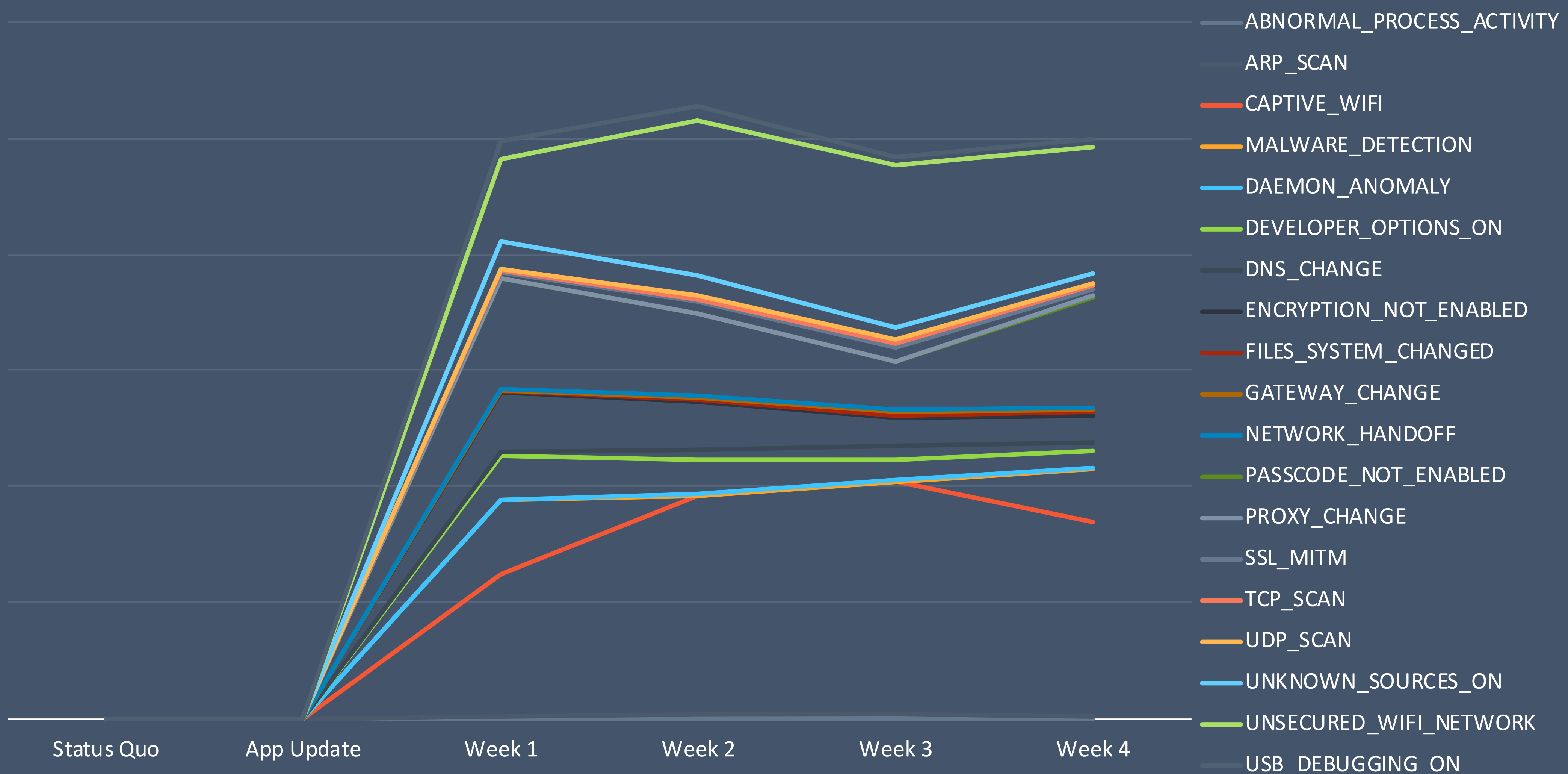
1,247 Compromised Devices

3,125 Compromised Networks

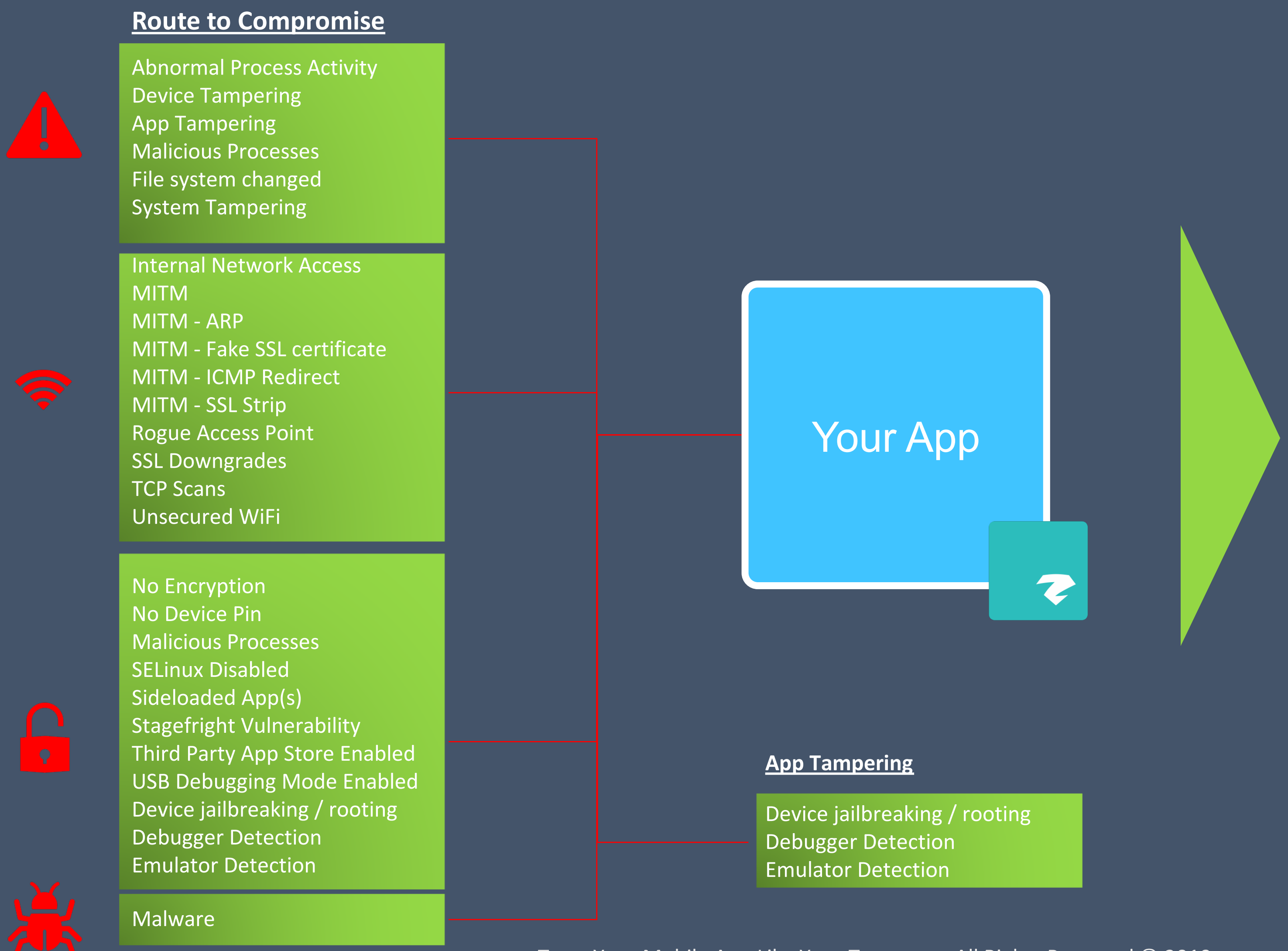
16,139 Rooted and Jailbroken Devices

2,231 Malicious Apps

Your app starts driving



Mobile threat detection and mitigation



Route to Compromise

Abnormal Process Activity
Device Tampering
App Tampering
Malicious Processes
File system changed
System Tampering

Internal Network Access
MITM
MITM - ARP
MITM - Fake SSL certificate
MITM - ICMP Redirect
MITM - SSL Strip
Rogue Access Point
SSL Downgrades
TCP Scans
Unsecured WiFi

No Encryption
No Device Pin
Malicious Processes
SELinux Disabled
Sideloaded App(s)
Stagefright Vulnerability
Third Party App Store Enabled
USB Debugging Mode Enabled
Device jailbreaking / rooting
Debugger Detection
Emulator Detection

Malware

Your App

App Tampering

Device jailbreaking / rooting
Debugger Detection
Emulator Detection

Mitigation (Examples)

Deny Authentication / Lock account

Delete Data / Clear Cache

Increase user risk score

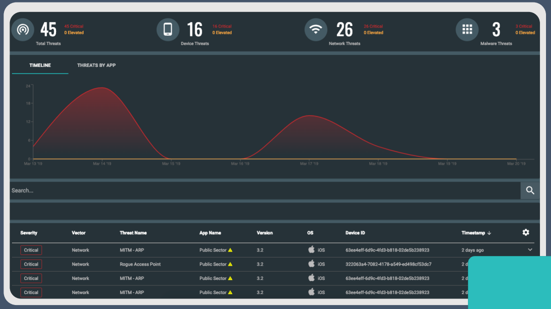
Restrict access until password reset

Establish VPN connection

Restrict or limit mobile transactions

Custom Rules and Remediations

Get the threat data (accidents) from your app



45 Total Threats — 45 Critical, 0 Elevated

16 Device Threats — 16 Critical, 0 Elevated

26 Network Threats — 26 Critical, 0 Elevated

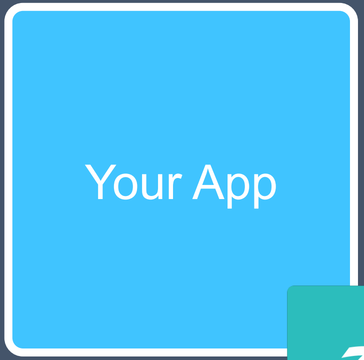
3 Malware Threats — 3 Critical, 0 Elevated

Severity	Vector	Threat Name	App Name	Version	OS	Device ID	Timestamp ↓
Critical	Network	MITM - ARP	Public Sector ⚠	3.2	iOS	63ee4eff-6d9c-4fd3-b818-02de5b238923	2 days ago
Critical	Network	Rogue Access Point	Public Sector ⚠	3.2	iOS	322063a4-7082-4178-a549-ed498cf53dc7	2 d
Critical	Network	MITM - ARP	Public Sector ⚠	3.2	iOS	63ee4eff-6d9c-4fd3-b818-02de5b238923	2 d
Critical	Network	MITM - ARP	Public Sector ⚠	3.2	iOS	63ee4eff-6d9c-4fd3-b818-02de5b238923	2 d

1

zIAP Administration Console

Create users, download documentation and SDK files.



2

Install Mobile Threat Detection SDK

Install zIAP mobile threat detection SDK and configure optional local remediation logic.

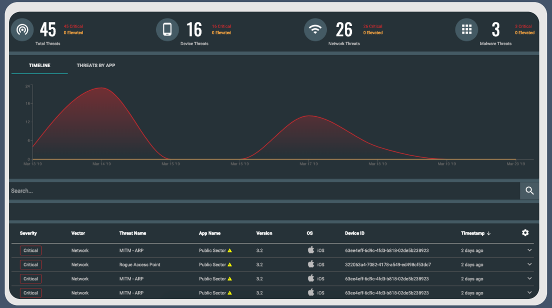
GET IT ON Google Play

Download on the App Store

3

Update App in Stores

Update app in App Store and Google Play. Users automatically receive new version and immediately are protected against malware and network attacks while using the app.



45 Total Threats — 45 Critical, 0 Elevated

16 Device Threats — 16 Critical, 0 Elevated

26 Network Threats — 26 Critical, 0 Elevated

3 Malware Threats — 3 Critical, 0 Elevated

TIMELINE THREATS BY APP

Search...

Severity	Vector	Threat Name	App Name	Version	OS	Device ID	Timestamp ↓
Critical	Network	MITM - ARP	Public Sector ⚠	3.2	iOS	63ee4eff-6d9c-4fd3-b818-02de5b238923	2 days ago
Critical	Network	Rogue Access Point	Public Sector ⚠	3.2	iOS	322063a4-7082-4178-a549-ed498cf53dc7	2 days ago
Critical	Network	MITM - ARP	Public Sector ⚠	3.2	iOS	63ee4eff-6d9c-4fd3-b818-02de5b238923	2 days ago
Critical	Network	MITM - ARP	Public Sector ⚠	3.2	iOS	63ee4eff-6d9c-4fd3-b818-02de5b238923	2 days ago

4

Mobile Threat Events

Monitor mobile threat events via mobile apps. Modify business logic to reduce fraud and claims to increase margins and customer satisfaction.

Questions?

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.

- eMail: king@zimperium.com
- More info: zimperium.com/ziap-in-app-protection

Secure your app