AGENDA & SPEAKERS

- Introduction
- Inside OWASP Mobile Top 10
- Large Scale Analysis of 3rd Party Apps
- Recommendations
- Q & A

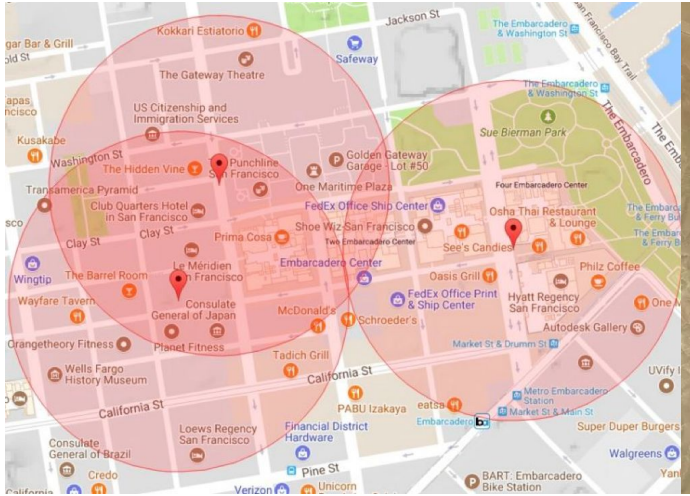
Tony Ramirez
Mobile Security Analyst

MOBILE APPS ARE TRACKING YOU

STRAVA™

Mobile App	Training
Striver	Cliiiimb
Straza Mate	Xert
Run An Empire	Tacit Training
IpBike	movecoach
Fitness AR	WattsBoard
Teaming	myWindsock.com

HARVESTED DATA OF APP USERS GEO

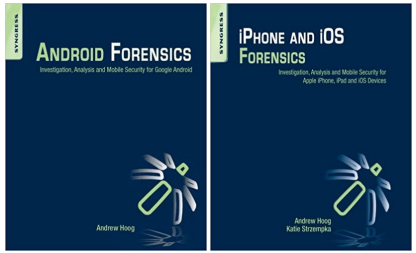


HARVESTED DATA OF MILITARY GEO

NowSecure™

DEEP MOBILE SECURITY EXPERTISE

Books & Speaking



DEFCON

black hat

RSA CONFERENCE IEEE OWASP

Open source

FRIDA

Mobile threat research is in our DNA

- Dream team of security researchers
- Every waking moment spent:
  - Discovering critical vulns
  - Identifying novel attack vectors
  - Creating/maintaining renowned open-source mobile security tools/projects

The NowSecure Mission

- Save the world from unsafe mobile apps
- Educate enterprises on the latest mobile threats
- Maximize the security of apps enterprises develop, purchase and use

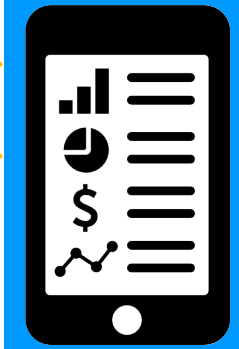
INSIDE THE MOBILE APP ATTACK SURFACE

DATA AT REST

- Data caching
- Data stored in application directory
- Decryption of keychain
- Data stored in log files
- Data cached in memory/RAM
- Data stored in SD card
- OS data caching
- Passwords & data accessible
- No/Weak encryption
- TEE/Secure Enclave Processor
- Side channel leak
- SQLite database
- Emulator variance

CODE FUNCTIONALITY

- GPS spoofing
- Buffer overflow
- allowBackup Flag
- allowDebug Flag
- Code Obfuscation
- Configuration manipulation
- Escalated privileges
- Android rooting/iOS jailbreak
- User-initiated code
- Confused deputy attack
- Multimedia/file format parsers
- Insecure 3rd party libraries
- World Writable Files
- World Writable Executables
- URL schemes
- GPS spoofing
- Integrity/tampering/repacking
- Side channel attacks
- App signing key unprotected
- JSON-RPC
- Automatic Reference Counting
- Dynamic runtime injection
- Unintended permissions
- UI overlay/pin stealing
- Intent hijacking
- Zip directory traversal
- Clipboard data
- World Readable Files



DATA IN MOTION

- Wi-Fi (no/weak encryption)
- Rogue access point
- Packet sniffing
- Man-in-the-middle
- Session hijacking
- DNS poisoning
- TLS Downgrade
- Fake TLS certificate
- Improper TLS validation
- HTTP Proxies
- VPNs
- Weak/No Local authentication
- App transport security
- Transmitted to insecure server
- Zip files in transit
- Cookie “httpOnly” flag
- Cookie “secure” flag

API BACKEND

- Platform vulnerabilities
- Server misconfiguration
- Cross-site scripting
- Cross-site request forgery
- Cross origin resource sharing
- Brute force attacks
- Side channel attacks
- SQL injection
- Privilege escalation
- Data dumping
- OS command execution
- Weak input validation
- Hypervisor attack
- VPN

NowSecure™

Inside OWASP & OWASP Mobile Top 10

OWASP MOBILE TOP 10

2011 OWASP Group determined Mobile is Different

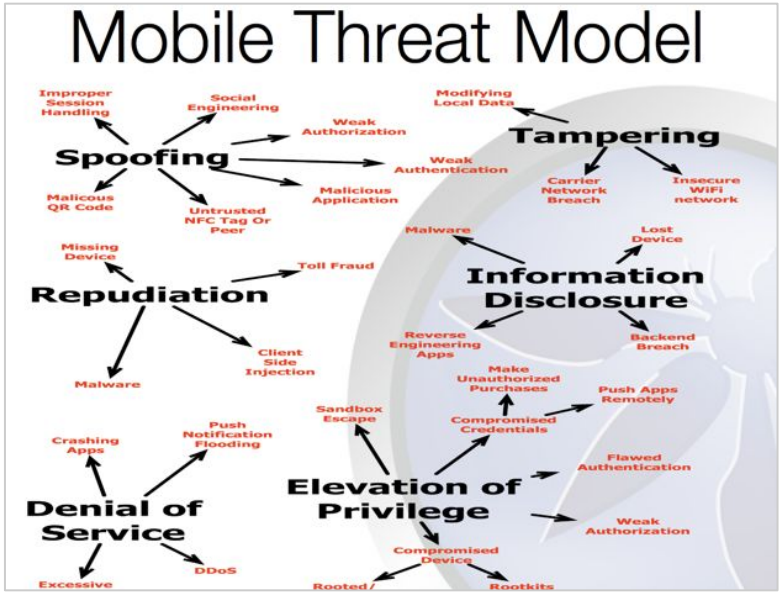
- Mobile OS Platforms vary widely
- Mobile apps very different from traditional web app model due to wildly varying use cases and usage patterns

Must consider more than the “Apps”

- Remote web services
- Platform integration (iCloud, GCM)
- Device (in)security considerations

Intended to be platform-agnostic

- Focused on areas of risk rather than individual vulnerabilities
- Weighted utilizing the OWASP Risk Rating Methodology

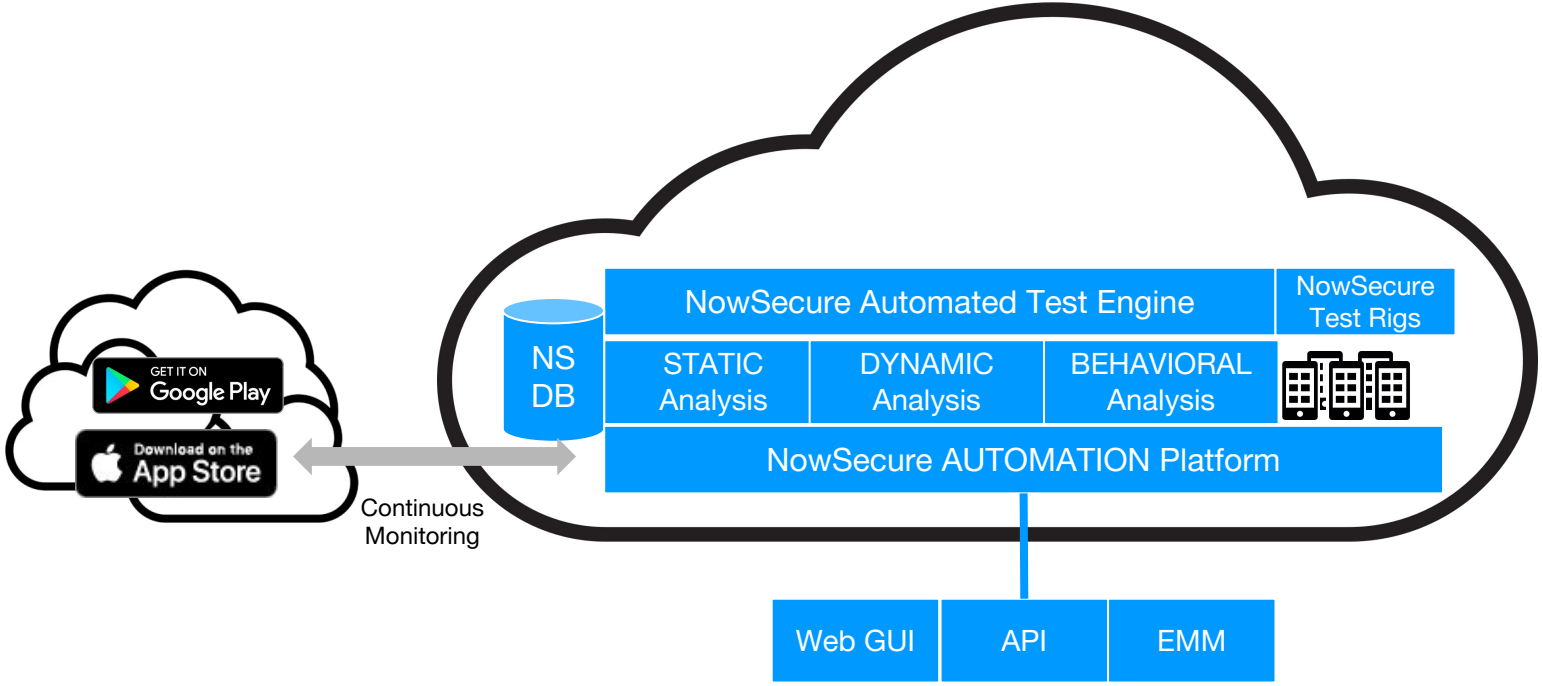


OWASP MOBILE TOP 10

M1 - Improper Platform Usage	Misuse of features like Touch ID, permissions, Keychain	
M2 - Insecure Data Storage	Data Leakage, client-side injection, weak server-side controls	
M3 - Insecure Communication	Poor handshake, SSL/TLS/Cert issues, transfer in clear text	
M4 - Insecure Authentication	Improper identity mgmt, weak session mgmt	
M5 - Insufficient Cryptography	Lack of crypto, improper crypto use	
M6 - Insecure Authorization	Improper local auth, forced browsing	
M7 - Client Code Quality	Code mistakes eg. Buffer overflows, format string vulns	
M8 - Code Tampering	Binary patching, method hooking/swizzling, memory mods	
M9 - Reverse Engineering	Exposure to attacker reversing tools	
M10 - Extraneous Functionality	Dev/QA inadvertent disabling security, hidden backdoors	

Analysis of Mobile App Store Apps for OWASP Mobile Top 10

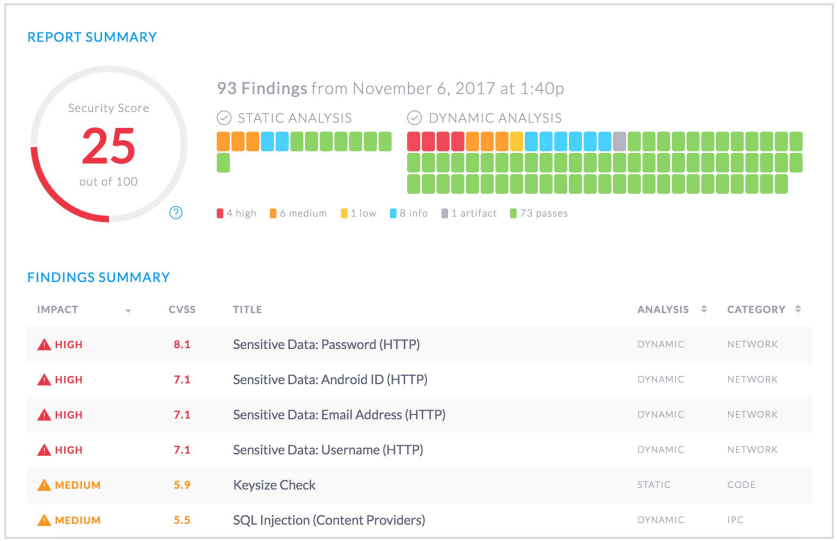
NOWSECURE APP STORE ANALYSIS ENGINE

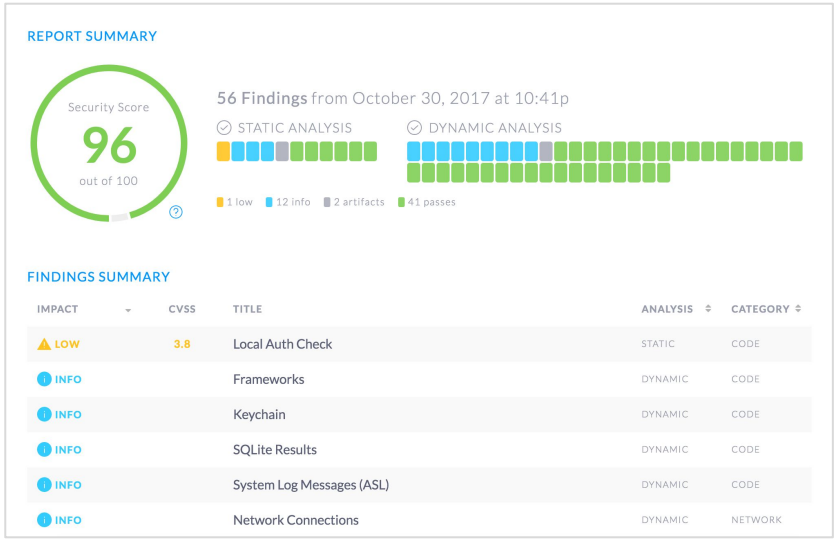


NowSecure INTEL

AlwaysOn AppStore Cloud Analysis for EMM & Security teams

INSIDE MOBILE APP RISK SCORING





INDUSTRY STANDARD CVSS SCORES

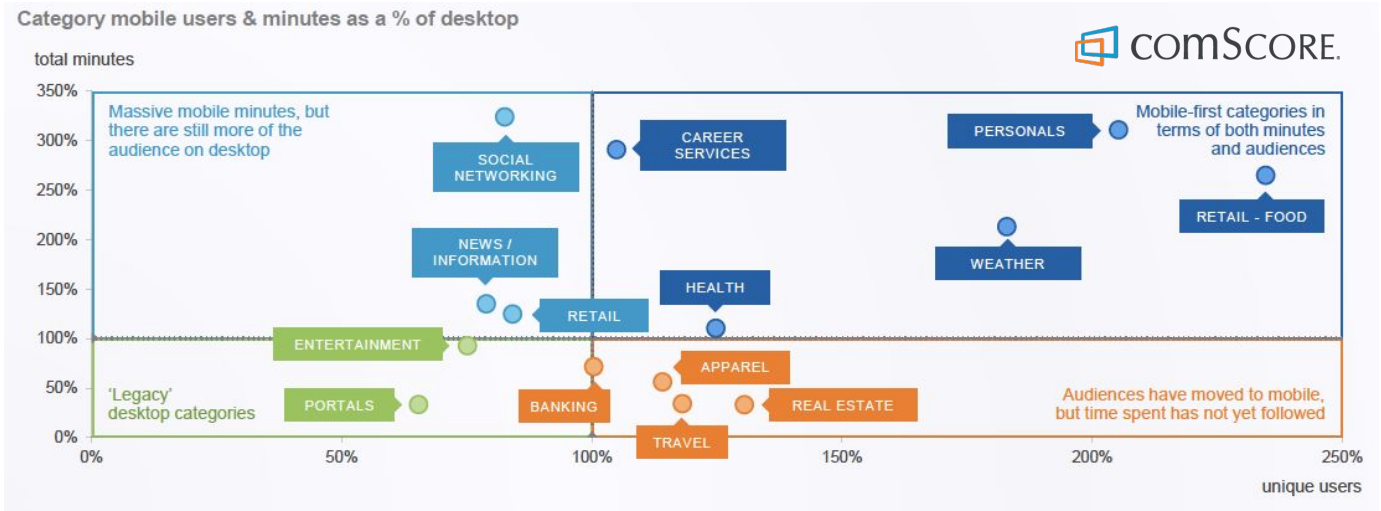
INDUSTRY REGULATORY COMPLIANCE

OWASP:	Mobile Top 10: M3-Insecure Communication
GDPR:	Risks violating Article 25 Risks violating Article 32
FFIEC:	May violate D3.PC.Am.Int.7
PCI:	May violate requirement 4.1

NowSecure™

NOWSECURE APP STORE ANALYSIS PROJECT

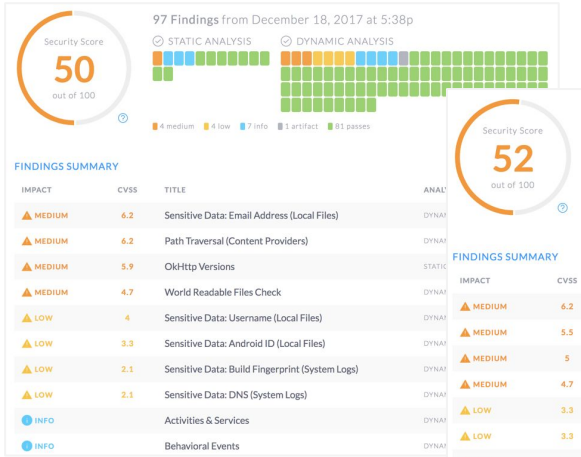
- 45,000 public apps posted to Apple App Store and Google Play store
- Broad distribution of categories



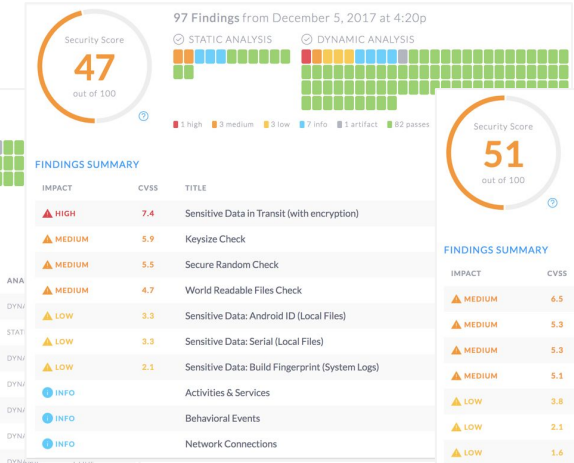
NowSecure™

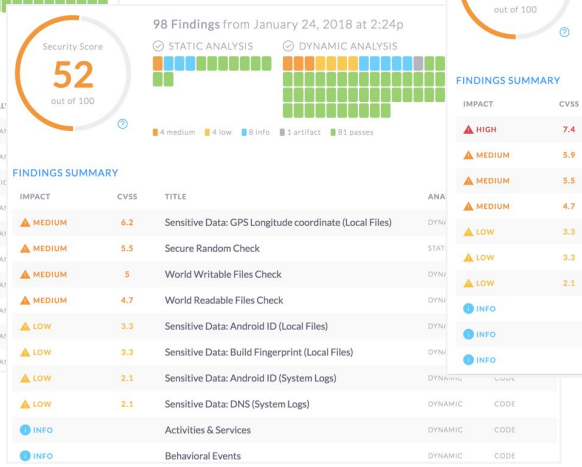
RISKY APPS THAT YOU MIGHT BE USING

POPULAR
BUSINESS EMAIL

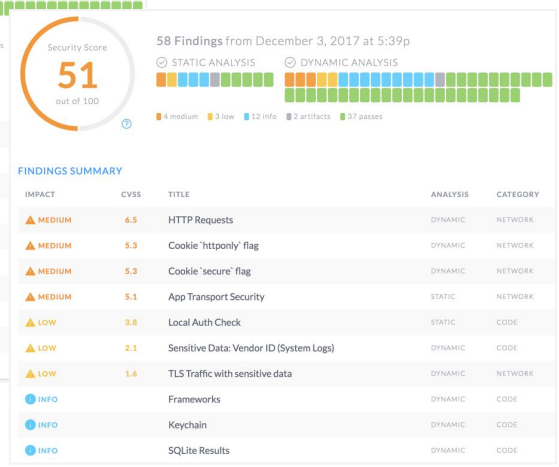


POPULAR
BUSINESS CRM





POPULAR
BUSINESS CHAT APP



POPULAR BUSINESS
TRAVEL APP

NowSecure™

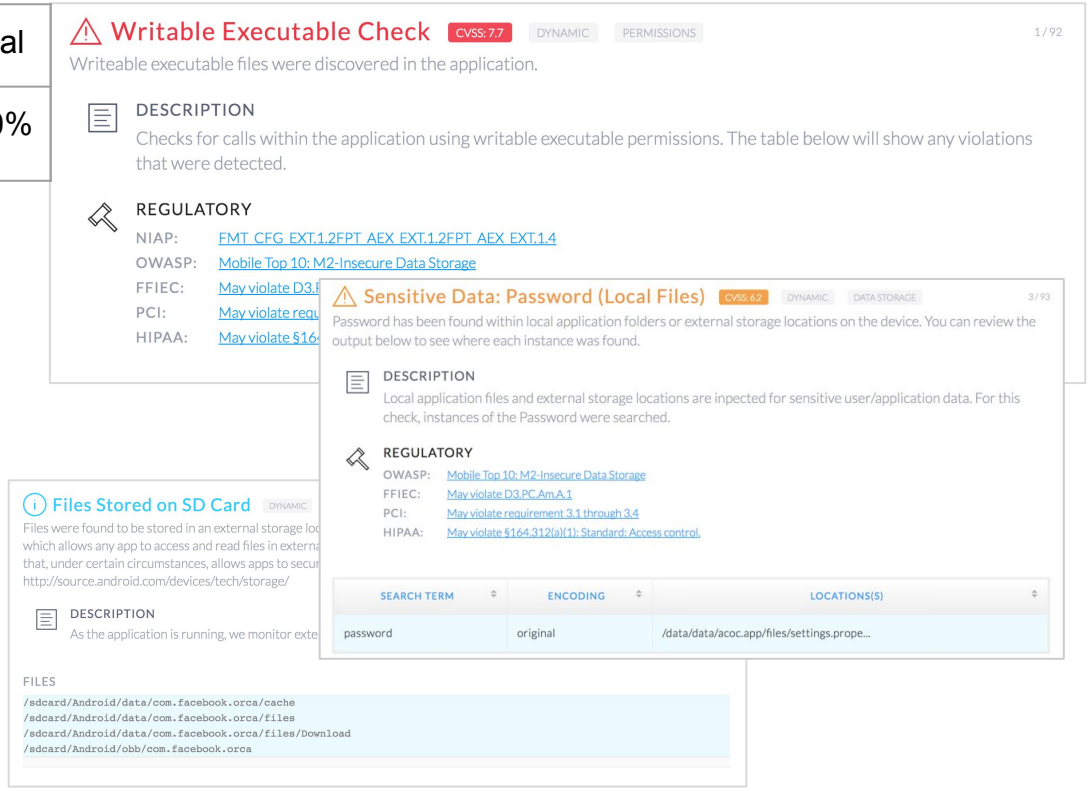
OWASP MOBILE TOP 10 - 3rd PARTY ANALYSIS [TOP 7]

M1 - Improper Platform Usage	Misuse of features like Touch ID, permissions, Keychain	
M2 - Insecure Data Storage	Data Leakage, client-side injection, weak server-side controls	50% Fail

TESTING FOR RISK -- DATA AT REST

	Android	iOS	Total
M2-Insecure Data Storage	85%	16%	50%

- Local log/file data
  - Account Credentials
  - PII
  - Email
  - Geolocation
  - IMEI/Serial Number
  - WiFi
- World Writable Executables
  - 52% of Android Apps
- External storage
  - Risk depends on your policy



NowSecure™

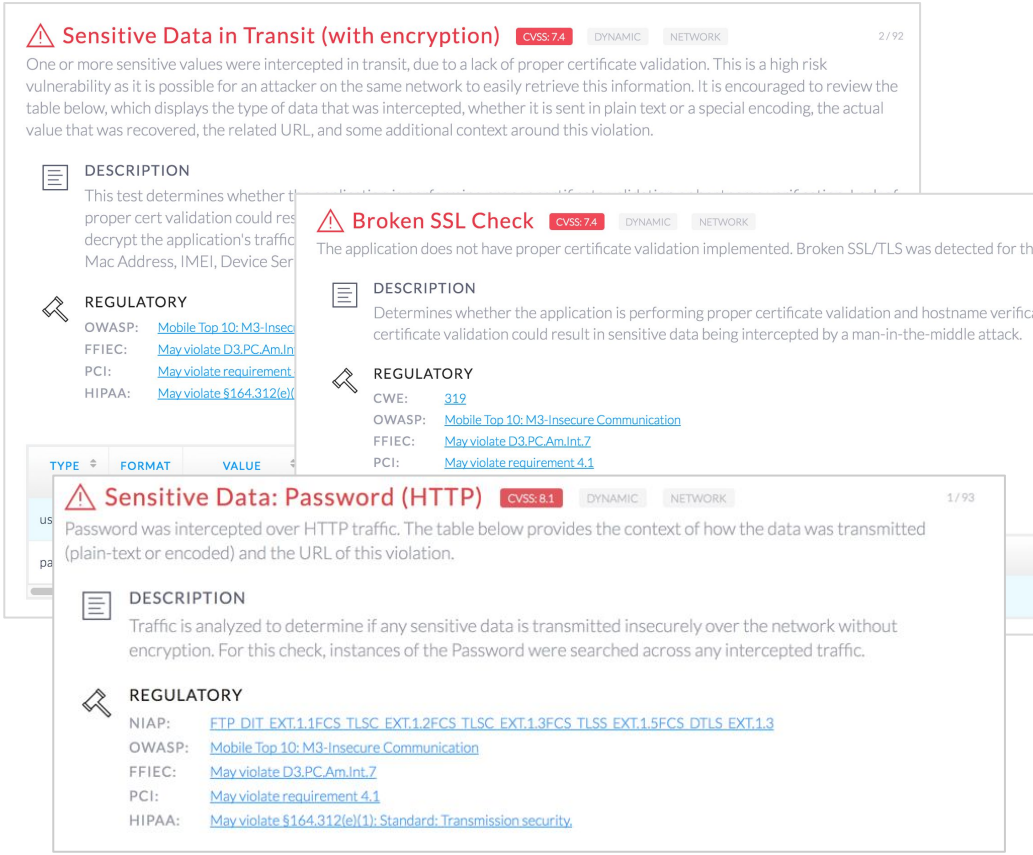
OWASP MOBILE TOP 10 - 3rd PARTY ANALYSIS [TOP 7]

M1 - Improper Platform Usage	Misuse of features like Touch ID, permissions, Keychain	
M2 - Insecure Data Storage	Data Leakage, client-side injection, weak server-side controls	50% Fail
M3 - Insecure Communication	Poor handshake, SSL/TLS/Cert issues, transfer in clear text	48% Fail

TESTING FOR RISK -- DATA IN MOTION

	Android	iOS	Total
M2-Insecure Communication	20%	76%	48%

- Assume that the network layer is not secure and is susceptible to eavesdropping
- Frequent lack of proper iOS ATS and cross-platform SSL implementations
- Unencrypted data OTA
  - Account Credentials
  - PII
  - Email
  - Geolocation
  - IMEI/Serial Number
- 30% of iOS apps use HTTP (not HTTPS)



NowSecure™

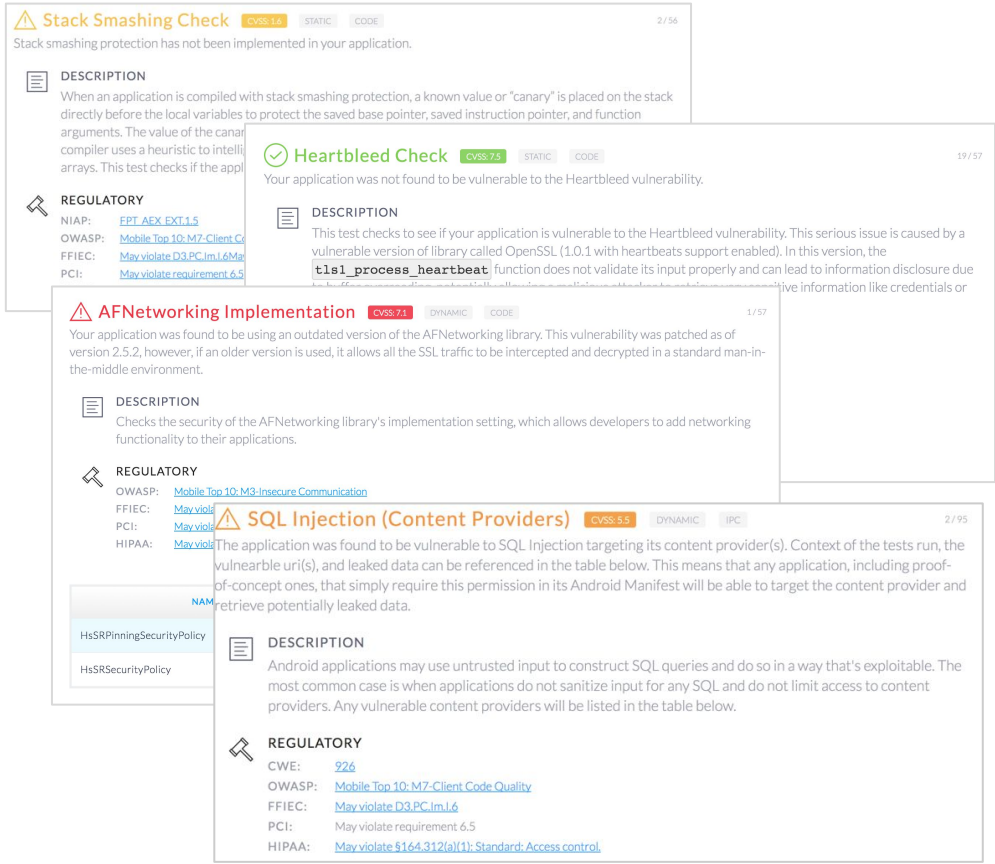
OWASP MOBILE TOP 10 - 3rd PARTY ANALYSIS [TOP 7]

M1 - Improper Platform Usage	Misuse of features like Touch ID, permissions, Keychain	
M2 - Insecure Data Storage	Data Leakage, client-side injection, weak server-side controls	50% Fail
M3 - Insecure Communication	Poor handshake, SSL/TLS/Cert issues, transfer in clear text	48% Fail
M4 - Insecure Authentication	Improper identity mgmt, weak session mgmt	5% Fail
M5 - Insufficient Cryptography	Lack of crypto, improper crypto use	
M6 - Insecure Authorization	Improper local auth, forced browsing	2% Fail
M7 - Client Code Quality	Code mistakes eg. Buffer overflows, format string vulns, 3rd Party	32% Fail

TESTING FOR RISK -- CODE & 3rd PARTY

	Android	iOS	Total
M7-Client Code Quality	59%	4%	32%

- iOS clearly has strong code quality practices
- Nearly all apps have 3rd party/OSS libraries
  - Open source often untested/unvetted
  - Inconsistent pattern of upgrading to latest more secure library versions
- Android app challenges
  - 1465 arbitrary code injection 1133 SQL injection
  - 112 Debug flag on



NowSecure™

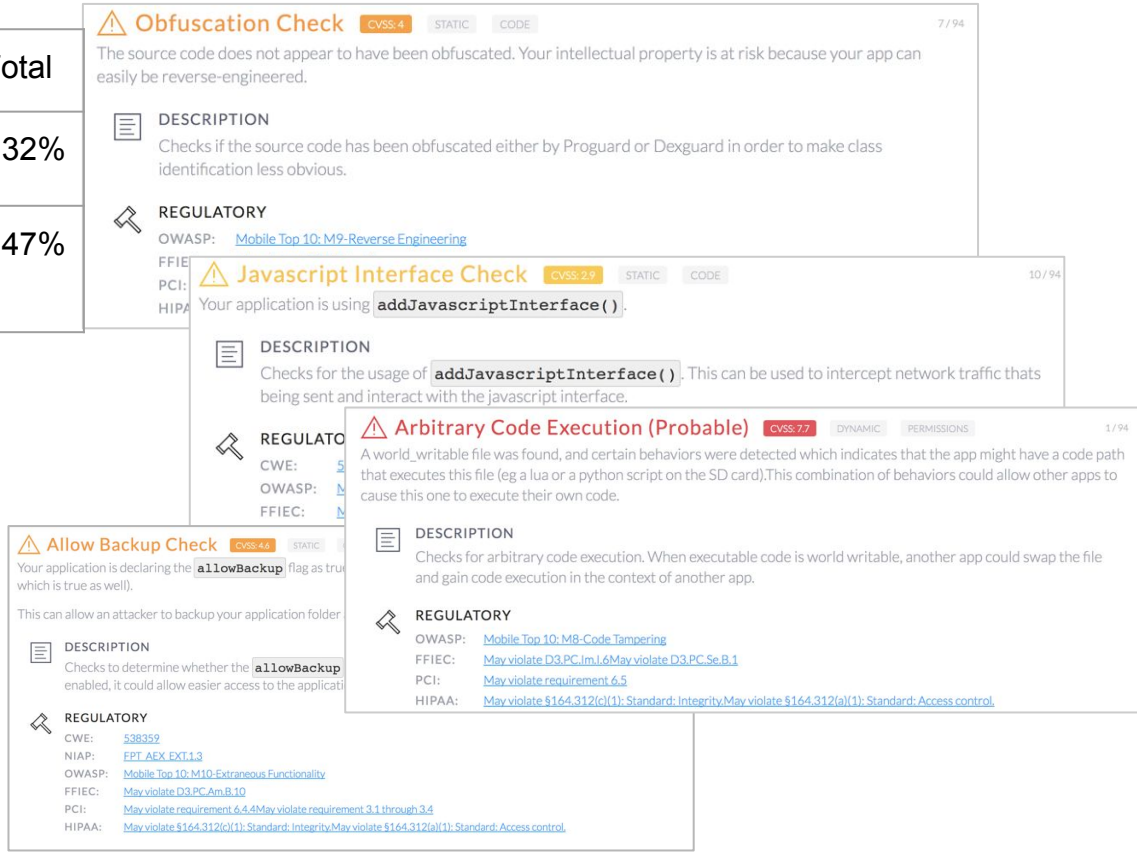
OWASP MOBILE TOP 10 - 3rd PARTY ANALYSIS [TOP 7]

M1 - Improper Platform Usage	Misuse of features like Touch ID, permissions, Keychain	
M2 - Insecure Data Storage	Data Leakage, client-side injection, weak server-side controls	50% Fail
M3 - Insecure Communication	Poor handshake, SSL/TLS/Cert issues, transfer in clear text	48% Fail
M4 - Insecure Authentication	Improper identity mgmt, weak session mgmt	5% fail
M5 - Insufficient Cryptography	Lack of crypto, mproper crypto use	
M6 - Insecure Authorization	Improper local auth, forced browsing	2% Fail
M7 - Client Code Quality	Code mistakes eg. Buffer overflows, format string vulns	32% Fail
M8 - Code Tampering	Binary patching, method hooking/swizzling, memory mods	
M9 - Reverse Engineering	Exposure to attacker reversing tools	32% Fail
M10 - Extraneous Functionality	Dev/QA inadvertent disabling security, hidden backdoors	47% Fail

TESTING FOR RISK -- TAMPERING

	Android	iOS	Total
M9-Reverse Engineering	64%	0%	32%
M10- Extraneous Functionality	92%	2%	47%

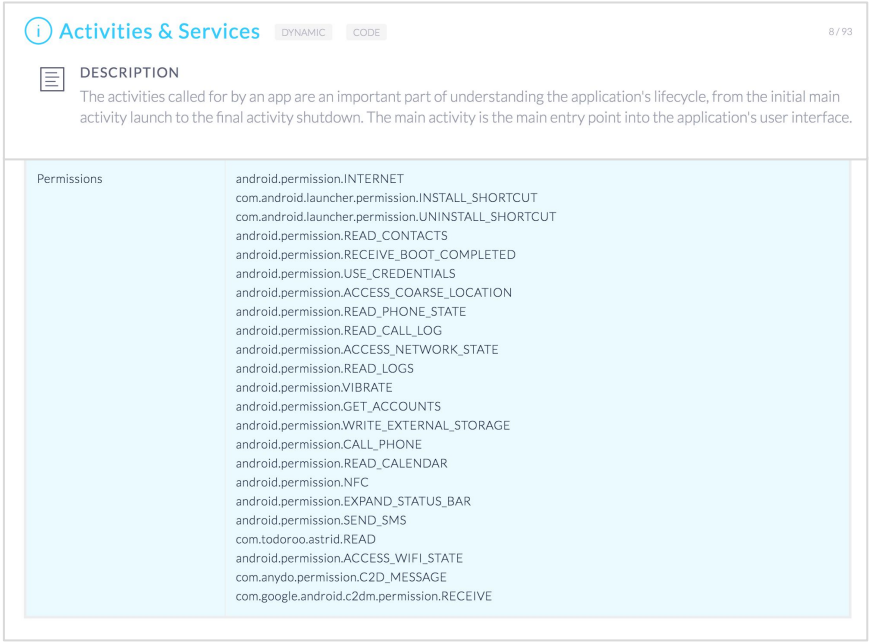
- Obfuscation insufficiently used by Android developers
- 90% of Android apps allow backup of data
- 1465 Android apps allow arbitrary code execution



NowSecure™

TESTING FOR RISK -- PERMISSIONS & ENTITLEMENTS

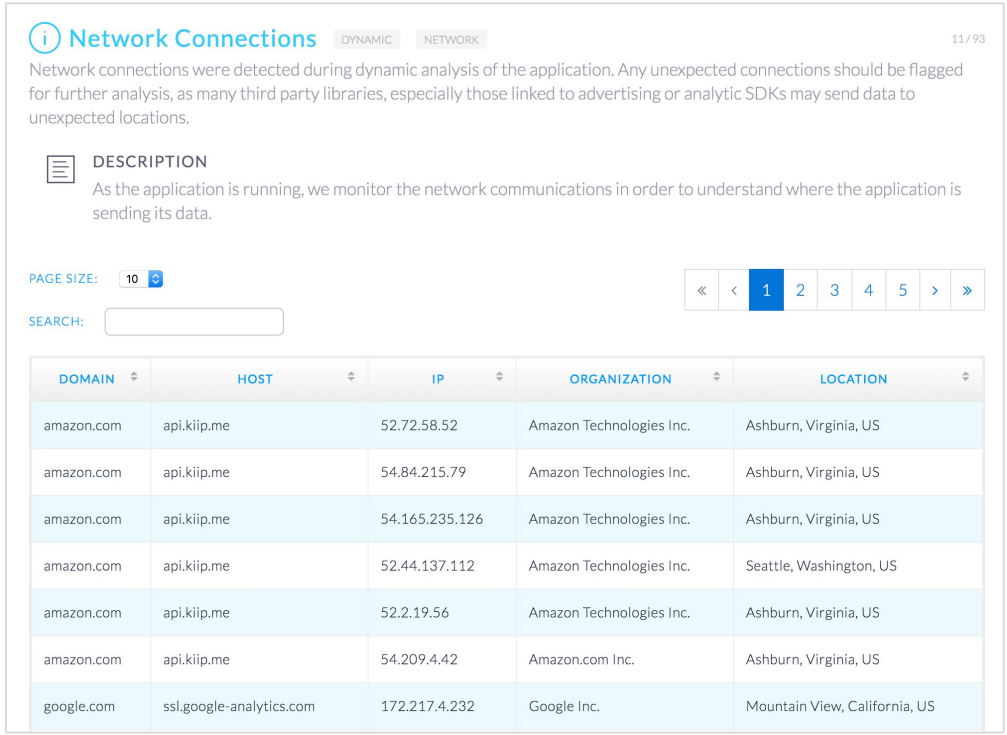
- Risk Dependent on your corporate policies
- Sample potentially risky permissions
  - Contact list access
  - Write external storage
  - Calendar
  - Send SMS
  - NFC



NowSecure™

TESTING FOR RISK -- IP ADDRESSES

- Risk Dependent on your corporate policies
- 3rd party libraries, SDKs are common culprits
  Ad networks frequently uniquely identify users and geo-locate them insecurely
- Apps frequently have 100s of connections (this one had 250)



Network Connections DYNAMIC NETWORK 11 / 93

Network connections were detected during dynamic analysis of the application. Any unexpected connections should be flagged for further analysis, as many third party libraries, especially those linked to advertising or analytic SDKs may send data to unexpected locations.

DESCRIPTION

As the application is running, we monitor the network communications in order to understand where the application is sending its data.

PAGE SIZE: 10

« ‹ 1 2 3 4 5 › »

SEARCH:

DOMAIN	HOST	IP	ORGANIZATION	LOCATION
amazon.com	api.kiip.me	52.72.58.52	Amazon Technologies Inc.	Ashburn, Virginia, US
amazon.com	api.kiip.me	54.84.215.79	Amazon Technologies Inc.	Ashburn, Virginia, US
amazon.com	api.kiip.me	54.165.235.126	Amazon Technologies Inc.	Ashburn, Virginia, US
amazon.com	api.kiip.me	52.44.137.112	Amazon Technologies Inc.	Seattle, Washington, US
amazon.com	api.kiip.me	52.2.19.56	Amazon Technologies Inc.	Ashburn, Virginia, US
amazon.com	api.kiip.me	54.209.4.42	Amazon.com Inc.	Ashburn, Virginia, US
google.com	ssl.google-analytics.com	172.217.4.232	Google Inc.	Mountain View, California, US

NowSecure™

OWASP MOBILE TOP 10

M1 - Improper Platform Usage	Misuse of features like Touch ID, permissions, Keychain	
M2 - Insecure Data Storage	Data Leakage, client-side injection, weak server-side controls	50% Fail
M3 - Insecure Communication	Poor handshake, SSL/TLS/Cert issues, transfer in clear text	48% Fail
M4 - Insecure Authentication	Improper identity mgmt, weak session mgmt	5% Fail
M5 - Insufficient Cryptography	Lack of crypto, mproper crypto use	
M6 - Insecure Authorization	Improper local auth, forced browsing	2% Fail
M7 - Client Code Quality	Code mistakes eg. Buffer overflows, format string vulns	32% Fail
M8 - Code Tampering	Binary patching, method hooking/swizzling, memory mods	
M9 - Reverse Engineering	Exposure to attacker reversing tools	32% Fail
M10 - Extraneous Functionality	Dev/QA inadvertent disabling security, hidden backdoors	47% Fail

Recommendations & Next Steps

BEST PRACTICES RECOMMENDATIONS

FOR ENTERPRISES

1. Recognize the risks of 3rd party apps on BYOD and COPE devices
   - ***Assume all are untrusted until validated***, no matter who the developer
2. Put controls and processes in place to analyze and monitor 3rd party app risk
   - Inventory & analyze your existing mobile apps leveraging EMM/MDM
   - Adapt processes to review and approve all new mobile apps before introduction
   - Leverage automated tools for in depth testing and continuous monitoring

FOR APP DEVELOPERS

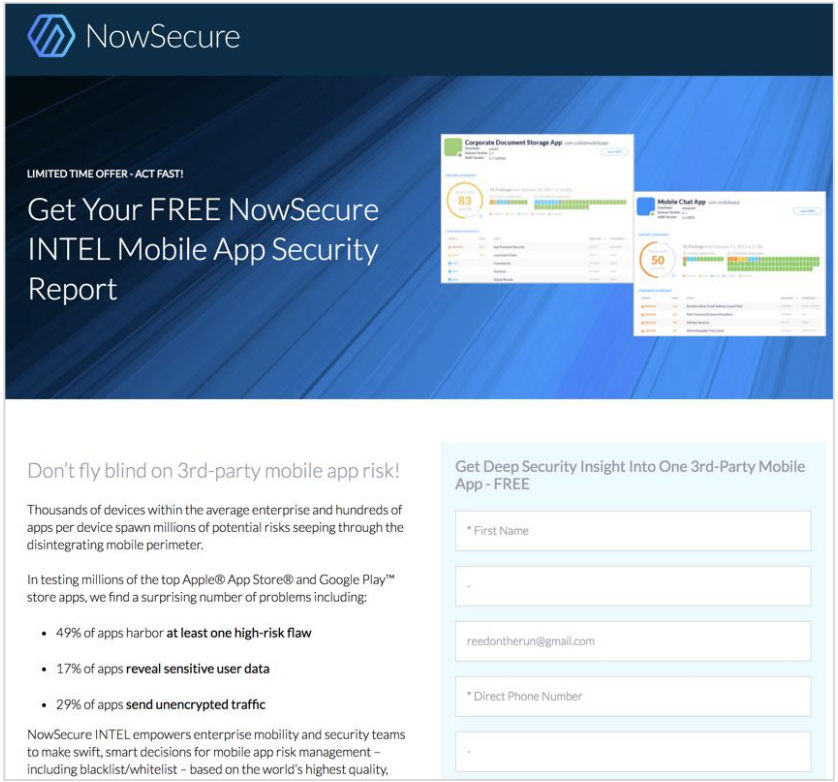
1. Train developers on secure coding best practices & fully vet 3rd party libraries
   - Leverage the NowSecure Guide to Secure Mobile App Development Best Practices
2. Ensure all mobile app releases are properly security pen tested
   - Leverage automated mobile appsec testing tools in SDLC lifecycle
   - Leverage 3rd party expert mobile app Pen Testing

3. Find a reputable source to stay up to date on the latest threats
   - Sign up for Nowsecure #MobSec5 at www.nowsecure.com/go/subscribe
   - Read our blog at www.nowsecure.com/blog

NowSecure™

GET A FREE MOBILE APP SECURITY REPORT

- Free for OWASP Members
- Delivered by NowSecure Mobile App Security Experts
- Choose a 3rd Party Mobile app used in your business
- Surf to request: http://bit.ly/2BB8sAk



NowSecure™

NOWSECURE COMING ATTRACTIONS

WEBINAR: "Top OSS for Mobile AppSec Testing: The Latest on R2 & FRIDA"
Delivered by the creators of R2 & FRIDA from NowSecure Research Team
Tomorrow: Weds Feb 21, 2019
Register Now: https://www.nowsecure.com/events/

RSA Conference 2018

RSA 2018

April 16-20, 2018
Meet us at **booth 3229** (**North Expo)**
in San Francisco, CA!

Open Q&A

Tony Ramirez, Security Analyst

NowSecure
+1 312.878.1100
@NowSecureMobile
www.nowsecure.com

Subscribe to #MobSec5

A digest of the week's mobile security news that matters

https://www.nowsecure.com/go/subscribe