RIIS Android Mobile App Security Index

Executive Summary

As part of our ongoing research into mobile security, RIIS LLC has put together an Android Mobile Security Index. We analyzed mobile apps developed by 20 Fortune 500 companies across a variety of industries. We looked at each of these apps and rated them using the industry standard https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

We analyzed these apps using the following OWASP criteria:

- Insecure Data Storage
- Weak Server Side Controls
- Insufficient Transport Layer Protection
- Client Side Injection
- Poor Authorization and Authentication
- Improper Session Handling
- Security Decisions via Untrusted Inputs
- Side Channel Data Leakage
- Broken Cryptography
- Sensitive Information Disclosure

Of the 20 apps, the top 5 had no security issues identified but the other 15 had room for improvement. These apps expose enough information that we would recommend turning on the screen lock on your phone if you are using these apps.

The findings show that Geico, Chase, Wells Fargo, State Farm and the IRS2GO app are the best protected apps in our list having no OWASP security issues. The bottom five apps from StubHub, Walmart, Speedway, LiveNation/Ticketmaster and Delta Airlines each have at least 3 of the OWASP Top 10 mobile security risks present in their Android apps.

Android App Rank	Company	OWASP Score
1	Geico	0
2	Chase	0
3	Wells Fargo	0
4	State Farm	0
5	IRS	0
6	E*TRADE	1
7	CVS	1
8	Dominos	1
9	AllState	1
10	Amway	1
11	American Airlines	1
12	Rite Aid	1.5
13	Fidelity	2
14	Travelocity	2
15	Facebook	2
16	StubHub	3
17	Walmart	3
18	Speedway	3
19	LiveNation / Ticketmaster	3
20	Fly Delta	4

Lower scores mean fewer issues from the OWASP top 10 were identified.
All apps were re-analyzed in August 2013.

Key Findings

Leaders

The top ranking apps were:

	Company	Score	Insecure Data Storage	Weak Server Side Controls	Insufficient Transport Layer Protection	Client Side Injection	Poor Authorization and Authentication	Improper Session Handling	Security Decisions via Untrusted Inputs	Side Channel Data Leakage	Broken Cryptography	Sensitive Information Disclosure
1	Geico	0	0	0	0	0	0	0	0	0	0	0
2	Chase	0	0	0	0	0	0	0	0	0	0	0
3	Wells Fargo	0	0	0	0	0	0	0	0	0	0	0
4	State Farm	0	0	0	0	0	0	0	0	0	0	0

Most of the financial apps analyzed - Chase, Wells Fargo and E*TRADE - had very low scores having little or no OWASP issues. Geico & State Farm's Pocket Agent App also had no OWASP issues.

Room for improvement

The bottom ranking apps were:

	Company	Score	Insecure Data Storage	Weak Server Side Controls	Insufficient Transport Layer Protection	Client Side Injection	Poor Authorization and Authentication	Improper Session Handling	Security Decisions via Untrusted Inputs	Side Channel Data Leakage	Broken Cryptography	Sensitive Information Disclosure
16	StubHub	3	0	1	1	0	0	1	0	0	0	0
17	Walmart	3	0	1	0	0	1	1	0	0	0	0
18	Speedway	3	1	0	0	0	0	1	0	0	0	1
19	LiveNation / Ticketmaster	3	1	0	0	0	1	0	0	0	0	1
20	Fly Delta	4	1	0	0	0	1	0	0	0	1	1

LiveNation and its sister app from Ticketmaster as well as Delta's Fly Delta app each exposed user login information. Each of these apps compromise a user's login credentials. Delta encrypts the login information stored on the phone but the encryption key can be found by decompiling the code. The LiveNation app does not use any encryption and stores the login information in cleartext.

To gain access to this user data, a hacker would need access to the person's unlocked phone so they can backup the app's runtime data and APK. We recommend enabling the screen lock if you have any of these apps on your phone.

Takeaways

1.The safest apps did not store any login information or sensitive user data on the Android device.

2.It is common practice (and a fundamental security flaw) to store the username and password encrypted in a SQLite database or shared preferences folder with a hardcoded encryption key which can be found by decompiling the APK.

3.Most of the Financial apps are doing a good job of storing the data on the backend web server and not on the Android device.

4.Exploits based on these security issues are limited to a hacker backing up single devices requiring physical access to a person's phone. A more widespread attack would require a malware app that is specifically written to exploit any security issues identified.

5.Some of the apps are storing user information in cleartext in SQLite and shared preferences where they can easily found, e.g. Facebook inbox messages and LiveNation login information. This is not a recommended approach.

6.Many of the apps contained test data in their APKs, mostly this was unit tests but some apps such as the Amway Business app had large files of test data.

Detailed Table

Rank	Company	OWASP Score	Insecure Data Storage	Weak Server Side Controls	Insufficient Transport Layer Protection	Client Side Injection	Poor Authorization and Authentication	Improper Session Handling	Security Decisions via Untrusted Inputs	Side Channel Data Leakage	Broken Cryptography	Sensitive Information Disclosure
1	Geico	0	0	0	0	0	0	0	0	0	0	0
2	Chase	0	0	0	0	0	0	0	0	0	0	0
3	Wells Fargo	0	0	0	0	0	0	0	0	0	0	0
4	State Farm	0	0	0	0	0	0	0	0	0	0	0
5	IRS	0	0	0	0	0	0	0	0	0	0	0
6	E*TRADE	1	0	0	0	0	0	0	0	0	0	1
7	CVS	1	0	0	0	0	1	0	0	0	0	0
8	Dominos	1	0	0	0	0	1	0	0	0	0	0
9	AllState	1	0	0	0	0	0	0	0	1	0	0
10	Amway	1	0	0	0	0	0	0	0	1	0	0
11	American Airlines	1	0	0	0	0	0	1	0	0	0	0
12	Rite Aid	1.5	0	0	0	0	0.5	1	0	0	0	0
13	Fidelity	2	0	0	0	0	0	0	0	0	1	1
14	Travelocity	2	0	0	0.5	0	0	1	0	0	0.5	0
15	Facebook	2	1	0	0	0	0	0	0	0	0	1
16	StubHub	3	0	1	1	0	0	1	0	0	0	0
17	Walmart	3	0	1	0	0	1	1	0	0	0	0
18	Speedway	3	1	0	0	0	0	1	0	0	0	1
19	LiveNation / Ticketmaster	3	1	0	0	0	1	0	0	0	0	1
20	Fly Delta	4	1	0	0	0	1	0	0	0	1	1

Methodology

We only analyzed apps for which we had valid user accounts.

The apps were analyzed as follows for encryption key and http issues:

- Connect phone or tablet to PC using USB cable
- Backup the app's runtime data using adb backup command
- Convert the backup data into readable format using Android Backup Extractor
- Look for user information in shared preferences and database folders
- If encrypted data is found then search for encryption key
- Pull the APK off the phone using adb pull command
- Decompile the APK using dex2jar and JD-GUI
- Look for encryption key by searching for encrypt and decrypt routines in decompiled source
- Decrypt encrypted runtime user information.
- Proxy http and SSL traffic
- Attempt man-in-the-middle attack
- Log into app on web server

We award 1 point for an identified security issue or 0.5 point for a suspected issue that we haven't been able to exploit. Lower scores mean fewer issues from the OWASP top 10 were identified.

The OWASP security issues are as follows:

1.Insecure Data Storage - Sensitive information is stored in cleartext and left unprotected.

2.Weak Server Side Controls - Backed APIs and web server are not secure.

3.Insufficient Transport Layer Protection - http or https traffic are not secure.

4.Client Side Injection - Hybrid apps have SQL injection of XSS issues.

5.Poor Authorization and Authentication - Access can be achieved due to insecure tokens or poor login authorization.

6.Improper Session Handling - The app rarely if ever asks the user to login after the initial login as the session never expires.

7.Security Decisions via Untrusted Inputs - The app does not use a minimal permissions required model.

8.Side Channel Data Leakage -Sensitive data is leaked in log or temp files or via 3rd party libraries, and when test data is included in the production app.

9.Broken Cryptography - Encryption is incorrectly implemented or the key is visible in the SQLite database or in the decompiled APK source code.

10. Sensitive Information Disclosure - API keys, passwords, SSNs can be easily found.

How Does Your App Score?

Our team of mobile security professionals will audit your code and provide you with a score. We can then work together to help you improve your score and truly secure your mobile app. Contact us today.

About RIIS

RIIS is an IT consulting firm based in Troy, MI. Our primary service includes accelerated application development through visualization and automated tools for web and mobile technologies. We help companies get the applications they need, faster! Industry experience includes software, e-commerce, advertising, defense, insurance, banking/finance, and telecommunications.