State of Mobile App Security

Apps Under Attack

Research Report
Special Focus on Financial, Retail/Merchant and Healthcare/ Medical Apps

Volume 3 – November 2014
(Previously titled: State of Security in the App Economy)

Table of Contents

Executive Summary

Mobile has become a cornerstone of the global economy; use of mobile applications continues to grow rapidly. The concept of there being an app for everything has only moved further away from being a joke, and closer towards becoming a reality. Staggering statistics across various reports indicate that mobile apps, fueled by widespread adoption of mobile devices, are driving a new decade of opportunities.

- 127 billion apps were downloaded for free in 2014, and there were over 11 billion downloads of paid apps. Free app download volume is projected to grow to 253 billion downloads and paid app download volume is projected to grow to 14.78 billion by 2017.[1]
- Global Mobile Apps revenue was $25.84 billion in 2013[2]. Mobile apps are on a path to reach $70 billion in annual revenue by 2017[3].
- Android dominated the Mobile Device Market with 85% market share as of Q2 2014[4], and Google Play worldwide quarterly downloads were about 60% higher than iOS App Store downloads in Q3 2014[5].

Similar to Arxan's analysis in 2012 and 2013, we reviewed the frequency with which mobile apps were hacked in a way that produced cloned or repackaged versions. Unfortunately, cloned apps are likely to be more than just mere harmless copycats. Separate analysis has revealed that over 50% of cloned apps are malicious and therefore pose serious risks[6].

Highlights and key findings

Our analysis of the top 100 paid and top 20 most popular free apps reveals that a majority have been hacked:

- 97% of top paid android apps have been hacked
- 87% of top paid iOS apps have been hacked

- 80% of the most popular free Android apps have been hacked
- 75% of the most popular free iOS apps have been hacked

Unfortunately, the numbers aren't getting better, in fact, for iOS, the numbers are worse than last year. The percentage of the Top 100 paid iOS apps that have been hacked increased from 56% to 87%, from 2013 to 2014, which underlines that the iOS platform is also very susceptible to hacking threats and attacks.

---

[1] Statista - Number of mobile apps downloads worldwide statistics
[2] Kleiner Perkins – Internet Trends May'2014 Report (Comprises virtual goods, in-app advertising, subscription, & download revenue)
[3] Digi-Capital, Investment bank for mobile apps and games
[4] IDC Q2 2014 Report
[5] App Annie Index - Q3 2014
[6] Trend Micro Research: Fake Apps Feigning Legitimacy (2014)

The research also reveals that hacks are occurring on apps across verticals.

1. In Financial Services:
   - Research has shown that hacking or malware has been the predominant method of Credit Card data breaches that occurred from 2005 to 2014[7]
   - Most apps have been hacked. The research of top fnancial apps reveals that:
     – 95% of Android apps have been hacked
     – 70% of iOS apps have been hacked
   - The research also reveals a growing trend of financial app hacking
     – Android app hacking increased from 76% to 95%, from 2013 to 2014
     – iOS app hacking increased from 36% to 70%, from 2013 to 2014

2. In Retail:
   - The study of top retail apps reveals that:
     – 90% of Android apps have been hacked
     – 35% of iOS apps have been hacked

3. In Healthcare/Medical:
   - Hacks are on the rise. A separate analysis revealed that 42% of total records compromised so far in 2014 were from medical and healthcare organizations – more than any other vertical[8]
   - Similarly, our research shows that many sensitive medical/healthcare apps have been hacked – 90% of Android apps have been hacked, 22% of these apps were FDA approved apps

Key Recommendations

- All applications should be built in a way that maintains the confidentiality of the application/code
  – Mobile applications that process sensitive information must be hardened at the binary level to prevent reverse-engineering
  – Mobile application hardening should be done in addition to traditional techniques used to protect web applications

- High-value mobile applications should include Runtime Application Self-protection (RASP)
  – Applications with a high-risk profile running on any mobile platform must be made tamper-resistant and capable of defending themselves and detecting threats at runtime
  – Applications should also check to understand the environment in which they are running, by for example, verifying if the mobile device is rooted or jailbroken

[7] Source: Chronology of Data Security Breaches published by Privacy Rights Clearinghouse, a California-based nonprofit corporation
[8] Source: Identity Theft Resource Center research report, Oct 21, 2014

- The software that is used to enable mobile wallets/payment apps (e.g., Host Card Emulation software) should be protected with secure crypto and app hardening

- The Food and Drug Administration (FDA) in the U.S. applies its regulatory oversight to mobile medical apps that, if compromised, could pose a risk to a patient's safety. The last guidance issued by the FDA was on Sep 25,2013. However, the guidance does not address key vulnerabilities related to reverse-engineering, repackaging, republishing and runtime attacks. Corporations should acknowledge that regulations are "lagging hackers" and ensure that their apps are protected against binary attacks

- Healthcare apps that have sensitive patient info and/or transactions pose great risk to patient's confidentiality if compromised. These apps must be protected from hacking and safeguard sensitive patient info

- Mobile has become a gateway to IoT, as mobile apps provide the means to control many IoT devices. Widespread hacking of apps poses serious risks to the IoT ecosystem
  - A mobile app, which controls an IoT device, must be secured from threats
  - Integrity of the IoT ecosystem must be protected by securing IoT firmware/embedded applications
  - Apps on open IoT platforms (e.g., Apple Watch & Car Play, Android Wear & Android Auto) must be secured as well

- As mobile banking continues to gain widespread adoption, mobile banking providers should put in place protections that:
  - Prevent unauthorized access to mobile banking applications
  - Prevent users from lifting sensitive information stored within mobile applications
  - Detect when the app is not behaving as designed at runtime – so as to reduce risk of fraud

- Organizations should consider mobile app assessments to determine if existing apps are exposed to risks that are unique to mobile environments. Also, as part of the mobile app development lifecycle, organizations should conduct Penetration Tests that, among other things, should assess vulnerability to reverse-engineering and tampering that can result from unprotected binary code. Tests should explore vulnerability to:
  - Application Repackaging
  - IP and Data Theft Exposure
  - Cryptographic Key Exposure
  - Application Tampering
  - System Compromise

Methodology

The 2014 State of Mobile App Security analysis followed the same methodology as last year's research, which included identifying and reviewing hacked versions of top iOS and Android apps from third-party sites outside of official Apple and Google app stores.

Step 1 – Select apps to be included in analysis

- **Paid Apps:** Top 100 iOS Apps from the Apple App Store and the Top 100 Android Apps from Google Play
- **Free Apps:** Top 20 popular free apps for iOS and the same 20 free apps for Android
- **Financial Service Apps:** Top 40 popular financial apps were reviewed with a breakdown of 20 on each platform (iOS and Android)
- **Heathcare/Medical Apps:** Top 40 sensitive healthcare/medical apps were reviewed with a breakdown of 20 on each platform
- **Retail Apps:** Top 40 sensitive retail apps were reviewed with a breakdown of 20 on each platform

Apps were selected during October of 2014. The list of top apps is dynamic, and as such, our 2014 list is different from the list used in prior years. A total of 360 apps were included in the analysis.

Step 2 – Determine if hacked versions of apps exist

A number of techniques and sources were used to identify hacked versions of the apps analyzed as part of our research. Techniques included, but were not limited to, the following:

- Searching unofficial app stores
- Examining app distribution sites
- Reviewing the top torrent sites (a list of sample torrent sites is listed here: http://www.ebizmba.com/articles/torrent-websites)
- Examining file download sites

We looked for hacked versions of applications during October of 2014.

Step 3 – Summarize results to identify key findings and recommendations

We aggregated results across a number of dimensions:

- Top Paid vs. Free apps
- By Platform (Android and iOS)
- By vertical (financial services, healthcare, retail)

We also reviewed to see how results varied from past years to identify trends over time.

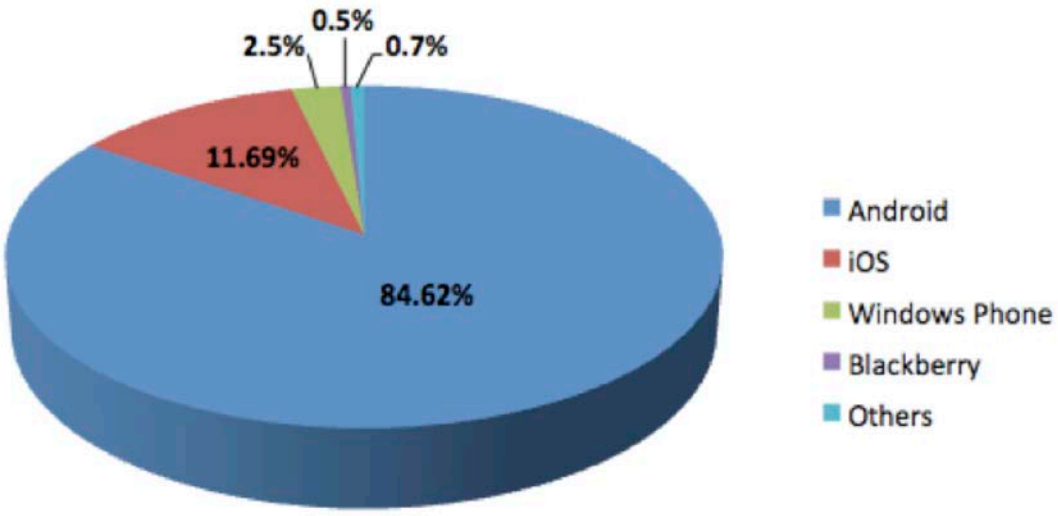
How easy is it for users to gain access to hacked applications – aren't there controls that prevent it?

- Android mobile users can potentially access hacked versions from third-party sites simply by setting their device settings controls to enable the option to accept apps from any source or app market in addition to Google Play
- For iOS users, downloading apps from outside Apple App Store requires the users to first jailbreak their device. Jailbreaking is relatively simple and can be done with widely available automated tools to bypass Apple's device restrictions. Once jailbroken, the user can install apps from third-party app stores directly on the device or download from any website
- Hackers can also republish hacked apps on official app stores under a different app name

Key Findings

Setting The Stage — Android Dominates Mobile Device Market; Security Remains a Challenge

As the following diagram shows, nearly 85% of the mobile device market was comprised of Android devices in Q2 2014. These numbers are an acknowledgement of Android's undisputed leadership among mobile environments. The Android operating system is free for device manufacturers and can be easily modified to match various business needs, which has helped it achieve popularity among smartphone and tablet developers as well as consumers across the world.



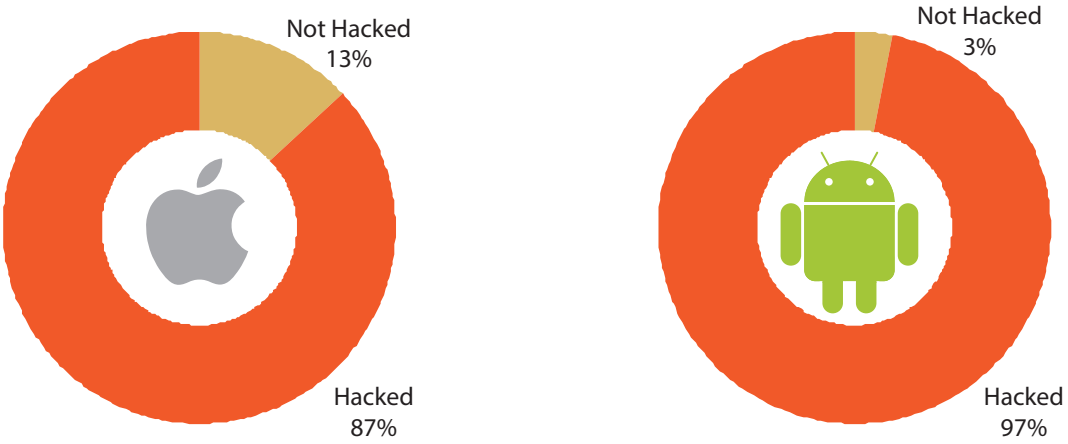
Source: IDC's Q2 2014 Report

Top Paid Apps Findings

Our research reveals, among top 100 paid apps, 97% of Android and 87% of iOS apps have been subjected to hacking.

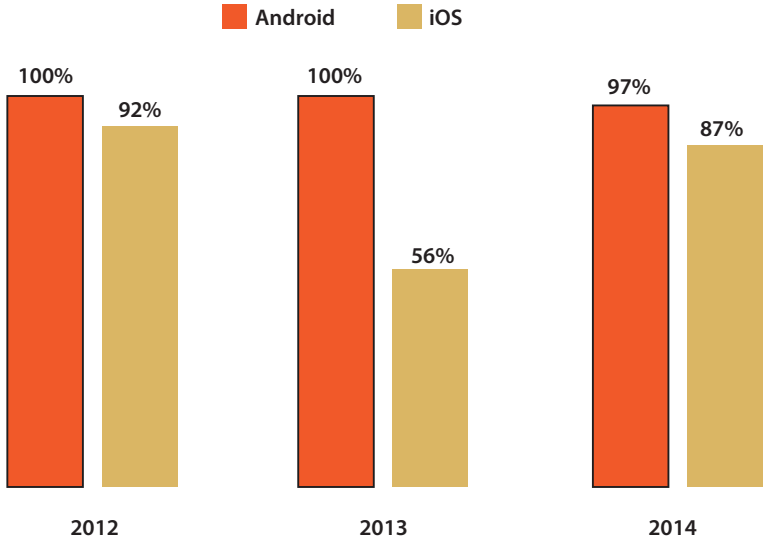
Top 100 Paid Apps

N= (100 per O/S)



The following graph illustrates the historical trend of top 100 Android and iOS paid apps.

Percentage of Hacked Apps



Though the Android data reflects a small percentage decrease, data trends from historical research starting from 2012 to 2014 indicate that the Android platform continues to surpass iOS in the number of apps hacked. Research reveals Android has become the primary target of attack for hackers.

The increase in iOS apps hacking from 56% to 87%, from 2013 to 2014, clearly shows that the iOS platform is also vulnerable to hacking threats and attacks. It continues to be a target for hackers. Even though the iOS app submission process has more checks and controls, the fact remains that hackers are more adept and have become successful in finding newer attack points over time.

In November of 2014, Palo Alto Networks® discovered a new family of Apple iOS & OS X malware named WireLurker, which automates generation of malicious iOS applications, through binary file replacement. See Appendix for details of the findings.

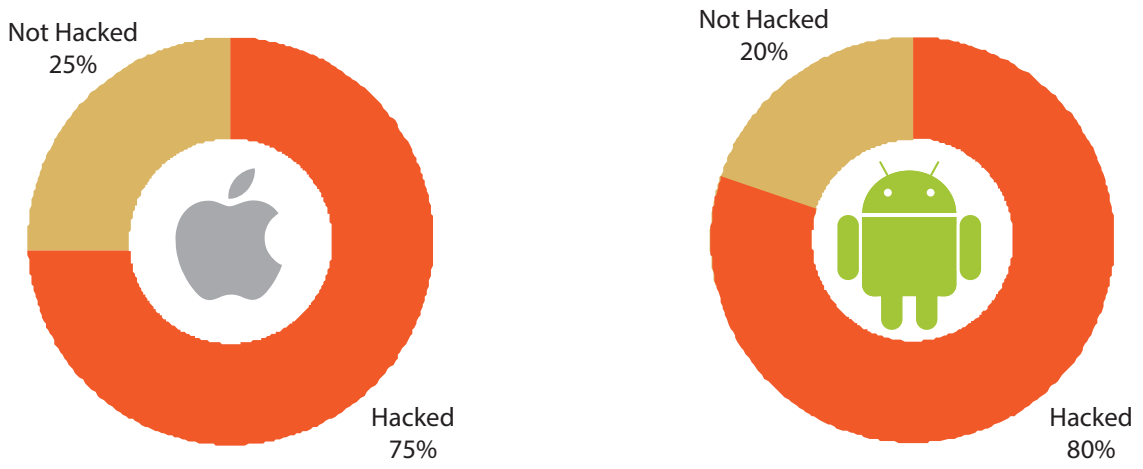
In Nov of 2014, FireEye reported new iOS vulnerability called "Masque Attack", which allows an attacker to substitute malware for a legitimate iOS app. FireEye reported all iOS apps can be replaced except iOS preinstalled apps, such as Mobile Safari, on both jailbroken and non-jailbroken devices. See Appendix for more details.

Popular Free App Findings

Our research reveals, among top 20 free apps, 80% of Android and 75% of iOS apps have been subjected to hacking.

20 Popular Free Apps

N= (20 per O/S)



Android app hacking has increased from 73% to 80%, iOS app hacking has increased from 53% to 75%, from 2013 to 2014

Hackers continue to target free mobile apps, many of which have valuable IP. More significantly, and similar to paid apps, they can be designed to process high-value transactions and manage sensitive data (such as patient info) user access or authorization credentials.

Findings From Related Research

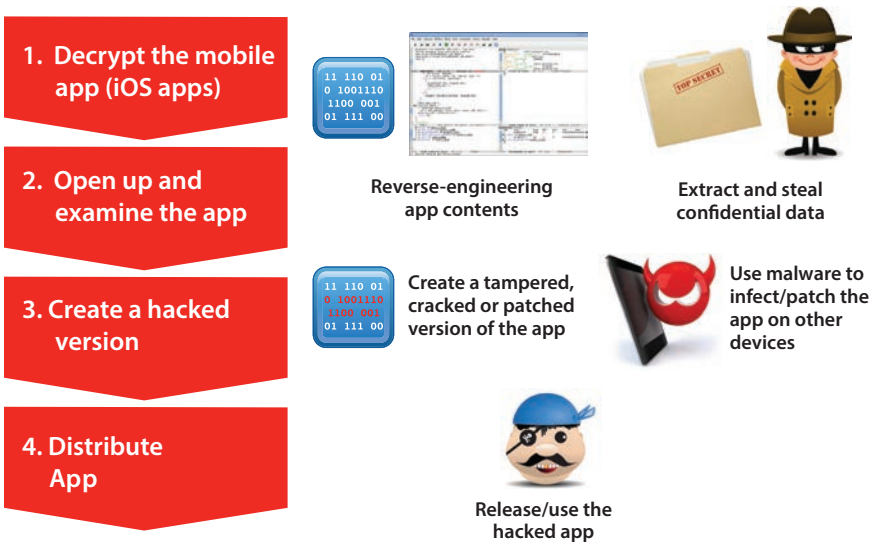
Columbia Research reveals roughly a quarter of all Google Play apps are Clones. See Appendix for additional details.

Trend Micro Research paper reveals cloned and fake apps pose serious risks and approximately 50% are malware rather than harmless copycats. See Appendix for additional details.

Findings from Arxan's assessment of Mobile Apps from various global organizations revealed that apps were exposed to reverse-engineering and binary code tampering in 90% of the cases. Moreover, in 94% or more of the apps assessed, the level of "Function Name" and "Static Data" protection was low. See Appendix for additional details.

A Few Simple Steps and Readily Available Tools Make It Fairly Easy To Hack

Anatomy of an App Hack



Hackers will leverage widely available tools to perform these steps. See the Appendix for a list of tools readily available for legitimate uses, but are often abused by hackers/cybercriminals to create clones and/or malicious apps.

Financial Services App Findings

Our research reveals, among 20 popular Financial Services Apps, 95% of Android apps and 70% of iOS apps have been subjected to hacking.

20 Finance Apps

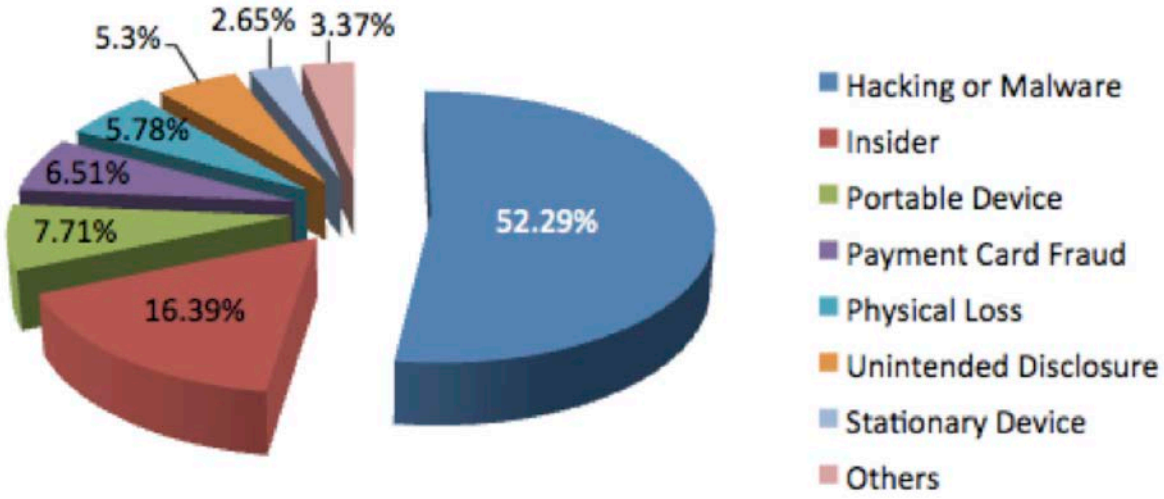
N= (20 per O/S)

Research also reveals the damaging trends of financial app hacking. Hacking of Android apps has increased from 76% to 95%, from 2013 to 2014. And for iOS apps, hacking has increased from 36% to 70%, from 2013 to 2014.

Findings From Related Research
INTERPOL-Kaspersky Lab joint report reveals dangerous trends of Mobile Banking Malware.

Based on their findings, the total number of banking Trojans targeting mobile devices grew from 423 in August of 2013 to 5,967 in July 2014. See Appendix for details of the findings.

Privacy Rights Clearinghouse, a California-based nonprofit corporation published the Chronology of Data Security Breaches, Security Breaches 2005–Present. The following graph illustrates the different methods used.



Findings From Related Research
Per McAfee, the total count of mobile malware has increased by 17% from Q1 to Q2.

Significant number of these Malwares were designed to exploit digital wallet service & popular messaging apps.
See Appendix for details of the findings.

As mobile banking continues strong adoption, statistics from various reports and our research clearly indicate growing trends of malicious apps designed to exploit mobile banking apps. Application self-protection especially at runtime becomes paramount to safeguard confidentiality and integrity of mobile banking applications.

Retail/Merchant App Findings

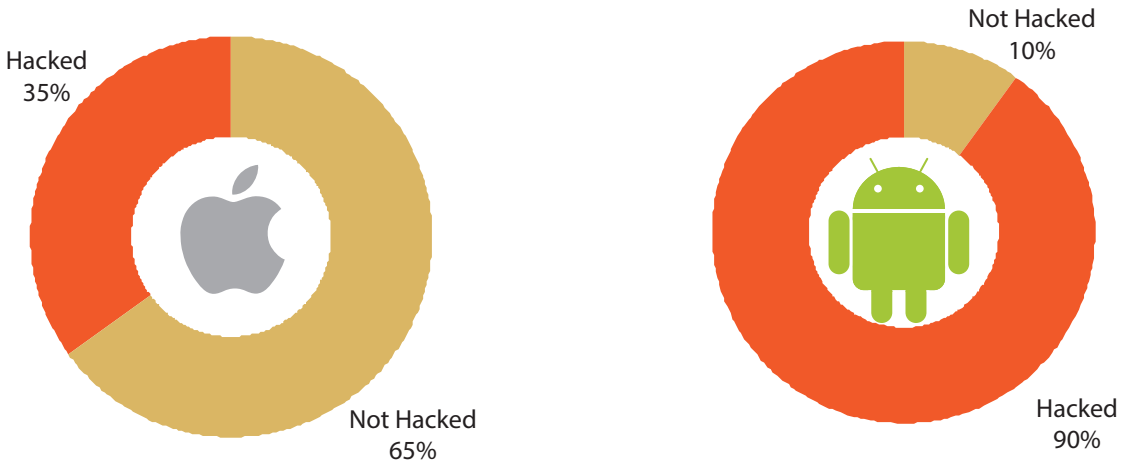
Our research reveals, among 20 popular Retail/Merchant Apps, 90% of Android apps and 35% of iOS apps have been subject to hacking.

Our research covered two types of apps including popular retail apps that consumers would download for online shopping from their favorite brands, and merchant apps that businesses would leverage on mobile devices to provide point of sale transaction and payment capability to their customers.

Given the growth of mobile devices being adopted in both segments, this category represents a new and growing landscape for mobile app hackers.

20 Retail/Merchant Apps

N= (20 per O/S)



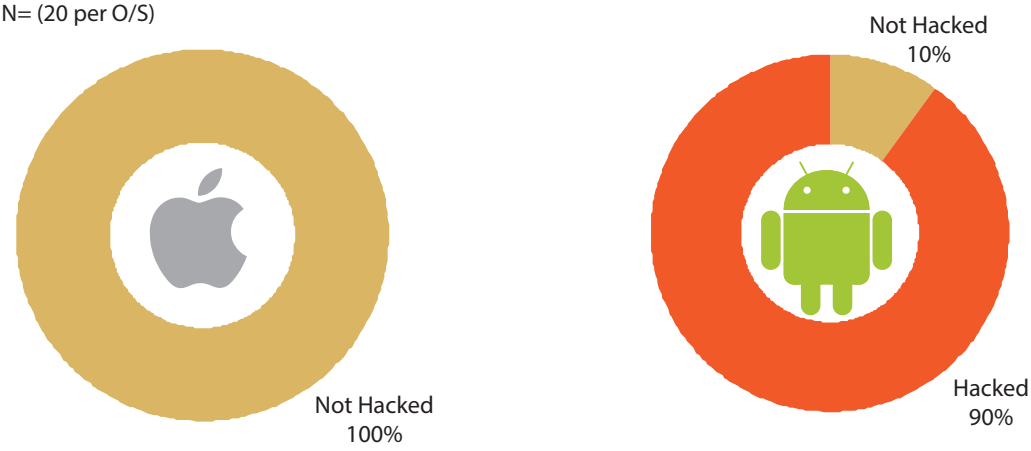
Popular retail and merchant apps can have sensitive code that ensures the completion of transactions and dictates sensitive data flow. There can also be security, critical business logic and intellectual property that provide differentiation to the brand.

Sensitive Medical/Healthcare Apps Findings

The research reveals, among 20 sensitive medical/healthcare apps, 90% of Android apps and no iOS apps have been subject to hacking.

20 Medical/Healthcare Apps

N= (20 per O/S)



Medical/Healthcare apps are increasingly being offered on App stores for patient access to records, and as well as patient services.

22% of sensitive medical/healthcare Android apps hacked are FDA approved. FDA approval alone doesn't guarantee application security.

Regulatory initiatives are not up to pace with dynamics and challenges of mobile health app industry.

Healthcare apps are quickly evolving to provide more than informational value of plan benefits and operations. Many are now providing high-value services including dynamic access to consumer personal identifiable information (PII). PII ranges in type of data captured in relation to personal records (social security, account number, employee ID, patient data, credit card data, etc.).

With regards to medical apps, they are particularly sensitive and are under preliminary scrutiny and guidelines of the Food and Drug Administration (FDA) in the United States. FDA categorizes some of these apps as medical devices given their unique and sensitive nature. Mobile app developers of such applications are on stand-by from the FDA regarding future compliance requirements. It is clear that the regulatory initiatives are not up to pace with dynamics and challenges of mobile health app industry, as 22% of the hacked apps are on the FDA approved list.

Identity Theft Resource Center reports that medical and healthcare organizations, accounted for the majority of data records compromised in 2014 — with 42.4 percent of all records as of Oct 21, 2014. Based on mobile health app developer's survey, the main market barrier for the next five years is lack of data security. See Appendix for details of the findings. So, it is imperative that dramatic changes be made in how medical and healthcare apps are protected to stem the current tide of attacks and address data security issues so use of apps will continue to grow.

Conclusion

As consumers continue to adopt the "always connected" lifestyle, Mobile is transforming the world in extraordinary ways. Data no longer sits within the four secure walls of enterprise network - it's on our mobile devices, it's in the cloud or somewhere else. Mobile apps live in the wild and threat vectors are constantly evolving.

It's evident from our research and various reports from leading industry experts that mobile applications are vulnerable to reverse-engineering, repackaging, republishing and susceptible to becoming malicious weapons. To combat these threats, organizations must adopt pre-emptive and reactive measures:

- By building self-defending mechanisms into the app so the mobile app is self-protected while resident on the device
- By providing runtime protections and self-repairing measures

These measures will mitigate risks and reduce the attack surface of mobile apps significantly.

OWASP, a leading application security industry authority, has acknowledged and prioritized the need for mobile application security, and recommended binary protection to mitigate the business and technical risks that mobile apps face. See Appendix for Top 10 Mobile Risks.

Leading analysts, like Gartner, Forrester, and others are also identifying the need for binary protection for all sensitive and high-value applications. Gartner is emphasizing the need for Runtime Application Self-protection (RASP), a security technology that is built or linked into an application or application runtime environment, and is capable of controlling application execution and detecting and preventing real-time attacks.

> **"Make application self-protection a new investment priority, ahead of perimeter and infrastructure protection. It should be a CISO top priority."** ***– Gartner***
>
> **"It ('application hardening and runtime protection') is a critical component in the strategy to secure enterprise software, embedded systems, mobile apps and the much-bandied 'Internet of Things'."** ***– 451Research***

About Arxan Technologies

Arxan provides the world's strongest application protection solutions. Our unique patented guarding technology 1) Defends applications against attacks, 2) Detects when an attack is being attempted, and 3) Responds to detected attacks with alerts and repairs. Arxan offers solutions for software running on mobile devices, desktops, servers, and embedded platforms – including those connected as part of the Internet of Things (IOT) -- and is currently protecting applications running on more than 300 million devices across a range of industries, including: financial services, high tech/independent software vendors (ISVs), manufacturing, healthcare, digital media, gaming, and others. The company's headquarters and engineering operations are based in the United States with global offices in EMEA and APAC. For more information, please visit www.arxan.com.

Appendix

Palo Alto Networks® makes startling revelations on iOS vulnerability

- Palo Alto Networks® recently discovered a new family of Apple iOS & OS X malware named WireLurker, which automates generation of malicious iOS applications, through binary file replacement
- WireLurker monitors any iOS device connected via USB with an infected OS X computer and installs downloaded third-party applications or automatically generates malicious applications onto the device, regardless of whether it is jailbroken
- WireLurker is capable of stealing a variety of information from the mobile devices it infects and regularly requests updates from the attackers command and control server
- WireLurker trojanized OS X and iOS applications using repackaging through executable file replacement. This technique is both simple to implement and effective

FireEye discovers new iOS vulnerability called "Masque Attack":

- FireEye mobile security researchers have discovered that an iOS app installed using enterprise/ad-hoc provisioning could replace another genuine app installed through the App Store, as long as both apps used the same bundle identifier
- FireEye reports all iOS apps can be replaced except iOS preinstalled apps, such as Mobile Safari. This vulnerability exists because iOS doesn't enforce matching certificates for apps with the same bundle identifier. This vulnerability found on iOS 7.1.1, 7.1.2, 8.0, 8.1 and 8.1.1 beta, for both jailbroken and non-jailbroken devices

Impact

An app installed on an iOS device using this technique may:

- Mimic the original app's login interface to steal the victim's login credentials.
- Access sensitive data from local data caches.
- Perform background monitoring of the user's device.
- Gain root privileges to the iOS device.
- Be indistinguishable from a genuine app.

Source: Nov 5, 2014 Palo Alto Networks: WireLurker - An New Era in OS X and iOS Malware
Source: Nov. 10, 2014 FireEye - Masque Attack: All Your iOS Apps Belong to Us

Appendix

Columbia University Research Reveals Android Apps are Vulnerable

Columbia University research revealed:

- Roughly a quarter of all Google Play free apps are clones: these apps are duplicative of other apps already in Google Play
- Developers often store their secret keys in their apps software, similar to usernames/passwords info, and these can be then used by anyone to maliciously steal user data or resources from service providers such as Amazon and Facebook. These vulnerabilities can affect users even if they are not actively running the Android apps

Source: Columbia Engineering Team - A Measurement Study of Google Play, June 18, 2014

Appendix

Trend Micro Research Reveals Fake/Cloned/Repackaged Apps Pose Serious Risks

Trend Micro research reveals:

- Fake apps were more likely to be high-risk apps or malware rather than just mere harmless copycats.
- As of April 2014, of the 890,482 sample fake apps discovered from various sources, 59,185 were detected aggressive adware and 394,263 were detected as malware. Among the fake apps, more than 50% were deemed malicious
- Over 65% of repackaged apps had modified advertising SDKs (via insertion or deletion). Cyber-criminals add mobile ad SDK to their own creations or replace the mobile ad SDKs in already-existing apps so they would receive the revenue instead of the original developers
- Malicious apps insert download code into legitimate ones so these would silently download other APKs, which may cause the victims to incur additional network charges
- Repackaging apps for use in malicious scheme is becoming the norm and therefore pose serious risks

Source: Trend Micro Research Paper – Fake Apps: Feigning Legitimacy

Appendix

Arxan's Mobile App Assessment

At Arxan Technologies, we assess and measure mobile apps for critical exposures – including, but not limited to:

- Source Code Exposure
- Function Name Exposure
- Static Data Exposure
- Symbol Exposure
- Jailbreak Detection Exposure
- Authentication Exposure
- Cryptography Exposure
- Licensing Exposure
- Payment Exposure

Findings from the Arxan's assessment of mobile apps from various global organizations revealed that apps were exposed to reverse-engineering and binary code tampering in 90+% of the cases. Moreover, in 94% of the apps assessed, the level of "Function Name" and "Static Data" protection was low.

The exposed static data elements for the majority of the mobile apps assessed were related to sensitive information such as passwords, usernames, account IDs, and cryptographic keys. Such exposures enable hackers to easily target these critical elements in app binaries, which can result in the app and brand being compromised.

Further, in about 25% of the apps tested, Arxan found that some of the most basic of security measures, like Stripping of symbols from an app before shipping, were not done. Leaving the symbols in an app is like giving the hacker the table-of-contents and index to your app. It's something that can be addressed very easily and definitely something that you don't want to overlook!

Appendix

INTERPOL-Kaspersky Lab joint report reveals dangerous trends of Mobile Banking Malware

Based on their findings, the total number of banking Trojans targeting mobile devices grew from 423 in August of 2013 to 5,967 in July 2014.

Key findings revealed:

- 59% of malware detections related to programs capable of stealing users' money
- The number of modifications for mobile banking Trojans increased 14 times over 12 months, from a few hundred to more than 5000

Appendix

Readily Available Tools Make It Easier To Hack

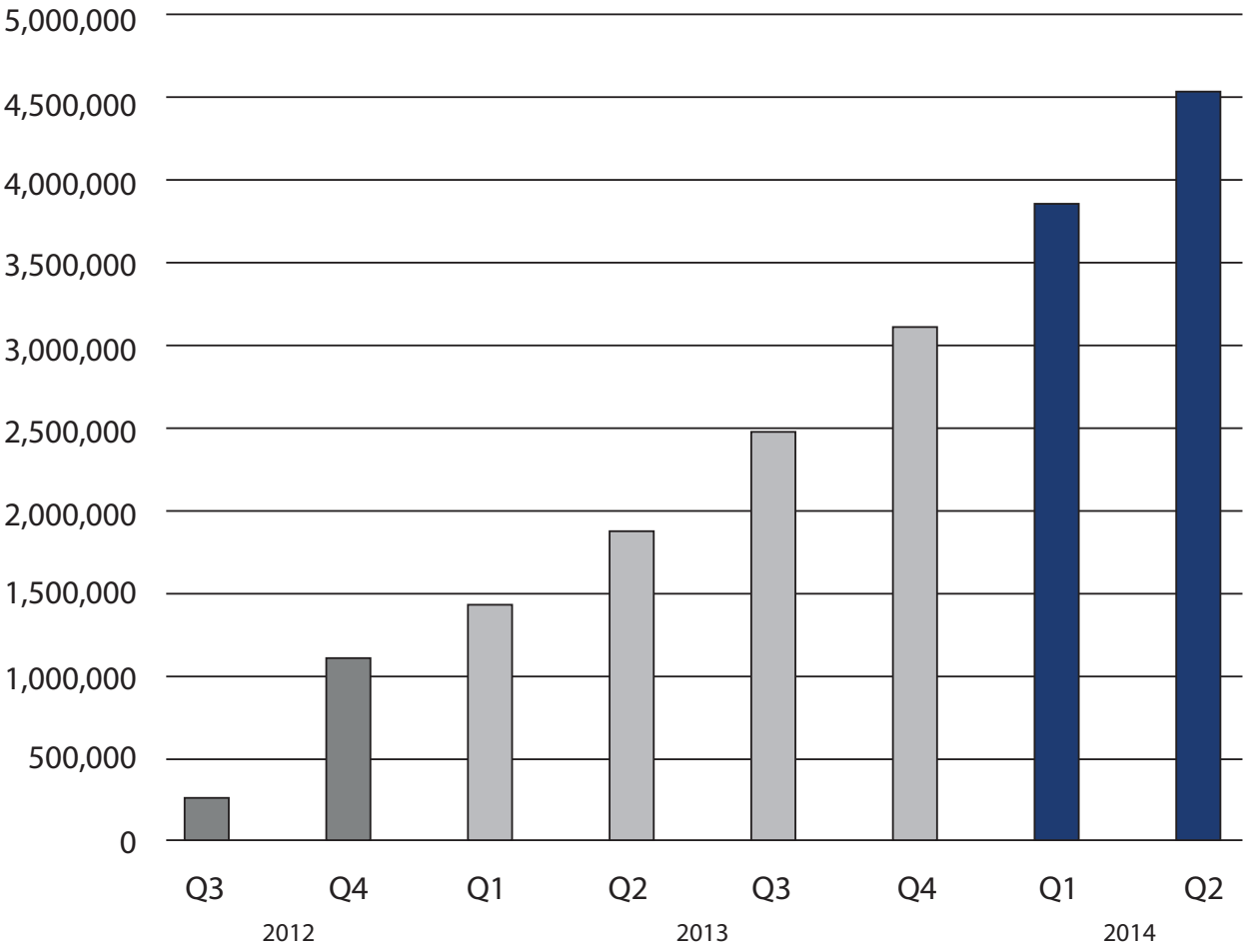
Category	Example Tools
App Decryption / Unpacking / Conversion	• Clutch • APKTool • Dex2jar
Static Binary Analysis, Disassembly, Decompilation	• IDA Pro & Hex Rays (Disassembler/Decompiler) • Hopper (Disassembler/Decompiler) • JD-GUI (Decompiler) • Baksmali (Disassembler) • Info dumping: class-dump-z (classes), nm (symbols), strings
Runtime Binary Analysis	• GDB (Debugger) • ADB (Debugger) • Introspy (Tracer/Analyzer) • Snoop-It (Debugging/Tracing, Manipulation) • Sogeti Tools (Dump key chain or filesystem, Custom ramdisk boot, PIN Brute force)
Runtime Manipulation, Code Injection, Method Swizzling, Patching	• Cydia Substrate (Code Modification Platform) (MobileHooker, MobileLoader) • Cycript / Cynject • DYLD • Theos suite • Hex editors
Jailbreak Detection Evasion	• xCon, BreakThrough, tsProtector
Integrated Pen-Test Toolsets	• AppUse (Custom "hostile" Android ROM loaded with hooks, ReFrameworker runtime manipulator, Reversing tools) • Snoop-It (iOS monitoring, Dynamic Binary Analysis, Manipulation) • iAnalyzer (iOS App Decrypting, Static/Dynamic Binary Analysis, Tampering)

Appendix

Total count of McAfee's mobile malware increased by 17% in Q2 2014

Significant number of these malware exploits were designed to exploit digital wallet service & popular messaging app. Mobile malware samples grew by 167 percent between Q1 2013 and Q1 2014.

Total count of McAfee's mobile malware increased by 17% in Q2 2014.



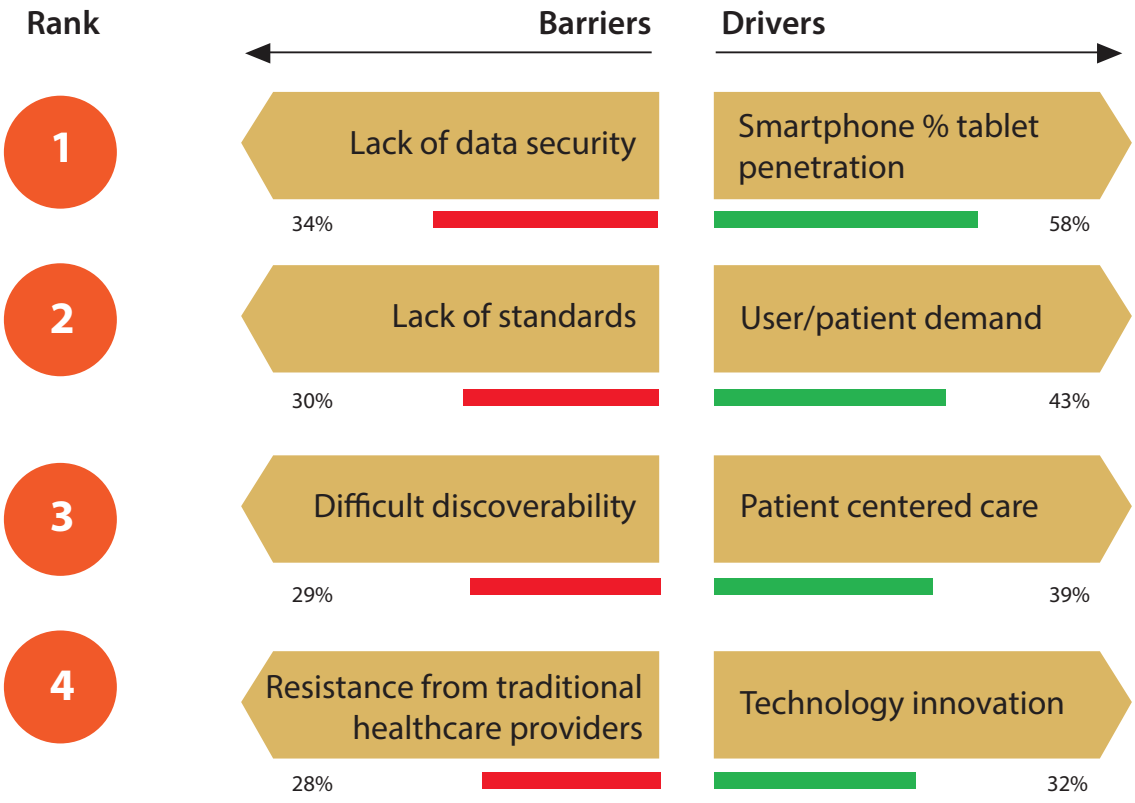
Source: McAfee Labs Threats Report August 2014

Appendix

Identity Theft Resource Center

Reports medical and health care organizations accounted for the majority of records exposed at 42.4% as of Oct 21, 2014. Last year, businesses accounted for 84% of breaches. The dramatic switch in targets, or impacted industries, could be indicative of a lack of education or resources in the health care field.

According to today's and future mHealth (Mobile Health) app publishers, the main market drivers for the next five years are the increasing penetration of capable devices (58%) and user/patient demand (43%). The potential showstoppers are lack of data security (34%) and standards (30%).



Source: research2guidance mHealth App Developer Economics survey 2010, 2011, 2012 and 2014, n=2032

Appendix

OWASP Top Ten Mobile Risks

Early 2014, OWASP, leading application security industry authority, published the Top Ten Mobile Risks based on new vulnerability statistics in the field of mobile applications. Following diagram is the representation of the mobile application threat landscape according to OWASP.

OWASP concluded that the lack of binary protections within a mobile app exposes the application and it's owner to a large variety of technical and business risks, resulting in the following business impacts:

- Privacy Related and Confidential Data Theft
- Unauthorized Access and Fraud
- Brand and Trust Damage
- Revenue Loss and Piracy
- Intellectual Property Theft
- User Experience Compromise

OWASP also identified the risks involved with Client Side Injection. Client-side injection results in the execution of malicious code on the mobile device via the mobile app, and direct injection of binary code into the mobile app via binary attacks. This will result in the following business impacts:

- Fraud
- Privacy Violations