



May 30, 2014

Federal Trade Commission  
Office of the Secretary, Room H-113 (Annex X)  
600 Pennsylvania Avenue NW  
Washington, DC 20580

**Re: Mobile Security Project, Project No.P145408**

ACT | The App Association is the leading organization representing small and mid-sized software companies in the mobile app ecosystem. Our developers build the apps consumers use every day, at home, at work, and at play. As consumer use of mobile devices grows, platform security will be increasingly important. ACT appreciates the opportunity to submit comments on this issue following the FTC's public forum on mobile security.

The app industry has seen astronomical growth in the last few years, from its emergence in 2008 to an estimated \$68 billion industry in 2014.<sup>1</sup> This growth has been driven by small businesses from every state. Consumers now use their smartphones to manage their medical information, find directions, store family photographs, pay bills, and even locate their luggage.

As consumers store more data on their smartphones and tablets, these devices become targets for bad actors. Leading security expert Bruce Schneier explains that "smart phones are going to become the primary platform of attack for cybercriminals in the coming years."<sup>2</sup> As a result, app developers rely on the trust of our consumers in order to do business.

**I. Secure Platform Design**

Consumer trust in mobile platforms provides the foundation for the app economy and entire mobile ecosystem. Consumers today entrust mobile devices with their most important data including bank accounts, medical records, family photos, and more. There is no greater threat to the future of the app ecosystem than a lack of trust in mobile platform, particularly for independent app developers.

For developers and designers there are key assets that make the underlying operating system ("OS") more secure. Application isolation (or sandboxing), data isolation, compartmentalized system resources to prevent permissions escalation, application signing, and robust encryption are just a few of the security-by-design elements that are considered industry best practices.

---

<sup>1</sup> Jonathan Godfrey and Morgan Reed, "App Store after Five Years," ACT (19 July 2013) *available at* <http://actonline.org/wp-content/uploads/2014/04/The-App-Store-After-Five-Years.pdf>.

<sup>2</sup> Bruce Schneier "Android Malware" *Schneier on Security*, (25 Nov. 2011) *available at* [https://www.schneier.com/blog/archives/2011/11/android\\_malware.html](https://www.schneier.com/blog/archives/2011/11/android_malware.html).



As we've made the transition to a mobile environment, we no longer view platforms as they existed in the PC era. Back then, "platform" was widely understood to be the OS. Now, "platform" encompasses the OS, device hardware, app distribution channels, software updating and patching regimes, and the wireless carrier.

In the post-PC world, there are two primary approaches to current mobile platform design: integrated and open. The integrated approach, epitomized by Apple, represents a direct response to the virus and malware problems that plagued the PC era of computing. Google has taken an open approach with Android that is more similar to the PC world.

The integrated model is optimized for security by taking a holistic approach. The provider tightly manages security with its partners across all aspects of its platform. Apple, Microsoft, and Blackberry have adopted this model in the design of their platforms. This typically means that the operating system is directly integrated with the associated app store to tightly control the quality and security of apps in the store and downloadable onto devices.

This generally starts by requiring developers to register with the store and establish credentials in order to submit apps.<sup>3</sup> Whitepapers on platform security from both Apple and Microsoft note the importance of this store curation.<sup>4</sup> "[A] carefully architected store submission and approval process [helps] prevent malware from reaching its marketplace."<sup>5</sup>

Once the app has been downloaded from a store, the mobile OS provides security for consumers. Options like certificate validation, restrictions on unauthorized access and data unless authorized by the user, and providing application programming interfaces ("APIs") for developers in order to comply with security requirements are some of the protections an OS can provide.<sup>6</sup> Limiting access to certain APIs and data stores also serve as best practices for limiting the potential danger from malicious products. This is how the OS protects device owners from malicious apps and hacks.

The tradeoff for this tight integration and security is that it places some limits on what developer can do and how quickly they can launch an app. It also limits what types of apps and software a consumer can access on their device.

The open model prioritizes the creation a completely of open platform where developers and consumers are unlimited in how they can modify and change the software and devices. And while there are certainly secure "open" projects, the lesson of the OpenSSL Heartbleed hack is

---

<sup>3</sup> iOS Developer Program, <https://developer.apple.com/programs/ios/>.

<sup>4</sup> Windows Phone 8 Security Guide (Sept. 2013) ("Windows Security") *available at* <http://www.microsoft.com/en-us/download/details.aspx?id=36173>, and iOS Security ("iOS Security") (Feb. 2014) *available at* [http://images.apple.com/ipad/business/docs/iOS\\_Security\\_Feb14.pdf](http://images.apple.com/ipad/business/docs/iOS_Security_Feb14.pdf).

<sup>5</sup> Windows Security, pg. 7.

<sup>6</sup> Windows Security, and iOS Security.



clear: Simply being “open” does not provide any assurance of security, and in fact can lead to a tragedy of the commons where inadequate resources are assigned.

This does not mean that the open approach cannot achieve an adequate balance of security. Google includes protected user data, application isolation, and secure interprocess communications as key features of Android design.<sup>7</sup> It is, however, also true that the open approach creates challenges, especially when it comes to managing updates, dealing with OS fragmentation, and unlimited software installations.

Providing a secure mobile environment cannot be approached as a static exercise. Platforms must continually respond to evolving external threats to provide safety for their users. While update mechanisms are not usually considered part of the platform, they are critical consumer protection components. An OS must be able to adapt to changes in security threats through an effective patching and updating regime to minimize the “security gap” between the time when malware exploits a weakness and the fix is implemented to prevent it.<sup>8</sup> Mobile devices that run the latest OS are better prepared to handle threats from malicious software.

## II. Secure Distribution Channels

The creation of a distribution channel for apps for modern platforms is a critical part of security for consumers. As the middleman between the developer and consumer, app stores provide protection for consumers and foster trust between consumers and developers. The level of security measures applied when reviewing apps will determine the strength or weakness of the platform and the reputation of the developers who distribute their apps on it.

A curated store scans each app and app update to filter out those containing malware or otherwise violate developer requirements. This review process takes time. Apple’s App Store, a curated store, provides an estimated review time so developers know how long approval will take. On May 29, 2014, the average approval time was four days.<sup>9</sup> While curated stores will never be able to catch all the malicious and infringing apps submitted, they are able to greatly reduce the number of bad apps in an app store. While there have been instances of malware on curated stores such as the Apple App Store, those instances have been few and far between.<sup>10</sup>

In contrast, Google has defined Google Play as a marketplace rather than a store. This has lead security researchers note that supervision and screening of submitted apps is less stringent and

---

<sup>7</sup> Android Security Overview (last visited 29 May 2014) *available at*

<https://source.android.com/devices/tech/security/#android-platform-security-architecture>.

<sup>8</sup> Bruce Schneier, “Our New Regimes of Trust,” *The SciTech Lawyer* (Winter/Spring 2013) *available at*

<https://www.schneier.com/essay-410.html>.

<sup>9</sup> “Average App Store Review Times” (last accessed 29 May 2014) *available at* <http://appreviewtimes.com>.

<sup>10</sup> Christina Bonnington, “First Instance of iOS App Store Malware Detected, Removed,” *Wired* (5 July 2012) *available at* <http://www.wired.com/2012/07/first-ios-malware-found/>.



the priority is not given to security.<sup>11</sup> Because of this, Google Play has faced challenges from increasing malware; the number of malicious apps in Google Play has increased fourfold from 2011 to 2013.<sup>12</sup>

While such review and testing take significant resources given the explosive growth of the app industry, it is still scalable. Platforms must balance the need for security with accessibility. Our developers have overwhelmingly chosen to publish their apps first on curated stores because they have found the balance of safety considerations in curated stores generates greater user trust and provides a better marketplace where they earn significantly more revenue.<sup>13</sup> A marketplace with limited curation has lower consumer trust<sup>14</sup> and earns our developers significantly less money. Because the majority of our members are independent software developers this has become critical, since in an untrusted store consumers tend to download only well-known apps or those from large companies, making it hard for smaller businesses to break into the market.

Although integrated distribution channels currently have a superior track record on security, we believe third party app stores can play an important part of a secure mobile platform, particularly for more open platforms. Third party stores are already demonstrating value in the specialized or enterprise context. These stores work best when they function in concert with the OS.

For example, App47 is an enterprise app store that operates within existing OSs. More and more enterprises are looking to curate an app store for employees, contractors, partners and customers. App47 allows its clients to segment each individual user into their own set of apps, some publicly available, some internally developed, and others available via HTML5. Moreover, they want the user's experience to be a very simple, straight-forward onboarding process while maintaining fine-grain access control over each group of users. Keeping track of who is in which groups, which apps are associated with them, which devices each user has, and which versions of which apps run on those devices that are approved can pose a challenging security problem.

---

<sup>11</sup> Chester Wisniewski, "Interview with Chester Wisniewski" Marketplace (18 Feb. 2013) *available at* <http://www.marketplace.org/topics/tech/difference-between-apples-app-store-and-google-play-user-data>

<sup>12</sup> Zach Miners, "Report: Android malware and spyware apps spike in the Google Play Store," Infoworld (19 Feb. 2014), *available at* <http://www.infoworld.com/d/security/report-android-malware-and-spyware-apps-spike-in-the-google-play-store-236702?page=0,0>

<sup>13</sup> See Jay Yarow, "The Difference in Developer Revenue Between Android and iOS," Business Insider (26 Nov. 2013) *available at* <http://www.businessinsider.com/chart-of-the-day-the-difference-in-developer-revenue-between-android-and-ios-2013-11>; "Developer Economics Q1 2014" Vision Mobile, *available at* <http://www.developereconomics.com/reports/q1-2014/>; Jacob Kleinman, "iOS Developers Still Make More Than Android Devs," TechnoBuffalo (17 July 2013) *available at* <http://www.technobuffalo.com/2013/07/17/android-vs-ios-developer-revenue/>.

<sup>14</sup> Daniel Eran Dilger, "Apple touts secure design of iOS as Google chief admits Android is best target for malicious hackers," Apple Insider (27 Feb 2014) *available at* <http://appleinsider.com/articles/14/02/27/apple-touts-secure-design-of-ios-as-google-chief-admits-android-is-best-target-for-malicious-hackers>,



Third-party app stores can also provide important competition for consumers and businesses seeking improved security. On open platforms, competition for app distribution could force other actors in the space to provide a more secure platform as a way of differentiating themselves to consumers and raise the bar for all stores and marketplaces. Limiting app distribution to a single channel does not provide security if that single channel is not ensuring apps in its store are secure.

### III. Secure Development Practices

Developers have been working to create safe and secure apps for their consumers and there are a number of resources available to help them. Trade associations like ACT have been providing guidance and training on the best security practices for apps and helping developers who find their intellectual property hijacked in malicious apps. ACT has conducted privacy boot camps and hosted other education events in order to help developers implement best security practices and be transparent with their customers.

App developer groups have also provided help to developers on security issues. Developer groups like MoDev hold put on conferences and meetups to encourage developers to meet and talk about security best practices. Third parties such as the Online Trust Alliance, Code Project, and CERT have provided guidance to developers wanting to build secure apps.<sup>15</sup>

Many providers of APIs and platforms have their own guides to security best practices. They provide APIs and services that can be called by mobile applications and server software that is used by mobile applications.<sup>16</sup> Such sites also often feature developer exchanges to share solutions and best practices for mobile security.

It is unreasonable, however, to place the onus on consumers to evaluate app security of an app. Few have the expertise to conduct such an evaluation. That is why intermediaries are important. Third parties provide seals, or alerts when various protocols, such as SSL, are not being used. As developers, we are trying to provide consumers with ways to find safe and secure apps.

---

<sup>15</sup> OTA Guide to Mobile App Privacy & Security (<https://otalliance.org/best-practices/mobile-app-privacy-security>), Code Project guide to Cryptography and Security (<http://www.codeproject.com/KB/security/>), and CERT top 10 secure coding practices

(<https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices>)

<sup>16</sup> See Twitter Security Best Practices (<https://dev.twitter.com/docs/security/best-practices>), Yahoo Developer Network Security (<https://developer.yahoo.com/security/>), Microsoft Guide to Writing Secure Code (<http://msdn.microsoft.com/en-us/security/aa570401.aspx>), and Apple Guide to Securing Your App (<http://www.apple.com/business/accelerator/develop/security.html>).



#### IV. Security Lifecycle and Updates

Existing best practices require security protection and updates be maintained for four years from the release of the mobile device. Updated security protection is critical for consumers and has two parts: updates to the applications that run on the device and updates to the core OS.

For apps, promulgating a patch that fixes a flaw is a race against time. The very nature of a curated store means that updates take time to be approved. While this is expected for updates to content, or features, it creates a conundrum for security. Therefore store providers like Amazon, Apple, and Microsoft have created a process to ensure urgent security updates are distributed to end users quickly, essentially fast-tracking the review. We see this as an industry best practice that helps to maintain a safe environment for both developers and users.

For OS security, a critical element is not merely creating a patch for a discovered security flaw, but ensuring that the maximum number of users possible are aware of, and implement, the patch.

For more than a decade, Microsoft, Apple, and others have been working to ensure that security patches are installed quickly. Microsoft adopted a model where the need for a patch was highlighted for the user, and automatic installation could be selected. Apple was the first smartphone to maintain control over patching regardless of carrier. So far, Apple's model has proven to have the greatest uptake in mobile patching, and Microsoft continues to see strong uptake in Windows 8.

As of May 1, 2014, 88 percent of iOS users have adopted all security patches,<sup>17</sup> for Windows, 77 percent are running an updated version,<sup>18</sup> while only 8.5 percent of Android devices were running the latest OS.<sup>19</sup> We believe the low rate of Android patching is directly related to OS fragmentation, and something that will continue to create security problems going forward.

No one can expect an older operating system to be patched indefinitely but companies will need to continue to patch operating systems no longer for sale for reasonable time after the initial release.

---

<sup>17</sup> iOS Developer App Store Distribution, *available at* <https://developer.apple.com/support/appstore/>.

<sup>18</sup> "AdDuplex Windows Phone Statistics Report for May 2014" *AdDuplex Blog* (May 30, 2014) *available at* <http://blog.adduplex.com/2014/05/adduplex-windows-phone-statistics.html#more> (due to limited roll out of Windows 8.1, the adoption rates for 8.0 were used).

<sup>19</sup> Android Developer Platform Versions, *available at* [https://developer.android.com/about/dashboards/index.html?utm\\_source=ausdroid.net](https://developer.android.com/about/dashboards/index.html?utm_source=ausdroid.net).



## V. Conclusion

App developers depend on the trust of consumers and that trust is in part based on the security of the platform upon which our apps run. As developers work to implement best security practices when building and deploying our apps, we expect platforms to do the same.

Going forward, platforms must be able to adapt to changing security threats through implementation of measures to protect customers both in the app store and on the mobile device. Platforms that take the open approach must direct more energy towards reducing the security holes exploited by malware that reduce customer trust in the platform and developers. Improved security benefits consumers, developers, and platforms alike.

We urge the FTC to look to the platforms following industry best practices around mobile security for the safety of consumers and their data. There is always work that can be done and ACT looks forward to working with platforms and the FTC to ensure safety for all consumers using mobile devices.