ISSN (Print) : 2249-1880
SAMVAD: SIBM Pune Research Journal, *Vol X, 53-58, December 2015* ISSN (Online) : 2348-5329

App Abuses: A Study of Increasing Risk in User's Adoption of Free Third-Party Mobile Apps in India

Hitesh Keserwani*

Assistant Professor, Amity Business School, Amity University, Lucknow, India;
hiteshkeserwani@gmail.com

Abstract

Technological risks are those that are genuinely new, which emerge from new technologies and processes. Developing risks are those that are not new, but whose manifestation and implications are emerging. Mobile malware is one such risk though it is relatively low, but with the emergence of free app, the diversity in data, technology and collaboration has also increased the threat of malicious apps (malware) and App vulnerabilities in the embedded processes of mobile phones, which leads to a deeper analysis. The Norton Report (2013), a global survey of end-users, showed that 38 percent of mobile users had already experienced mobile cybercrime. Mobile users are storing sensitive files online (52 percent), store work and personal information in the same online storage accounts (24 percent) and sharing logins and passwords with families (21 percent) and friends (18 percent), putting their data and their employers' data at risk. Yet only 50 percent of these users take even basic security precautions. According to McAfee Labs threat report, June 2014 The Company has discovered a suspicious Android app, Android/BadInst. A, on the Google Play app store that automatically downloads, installs, and launches other apps without user permission, which is usually required when manually installing apps from Google Play. Because this confirmation procedure at installation plays a critical role in securing a mobile platform, allowing apps to skip this process poses a significant risk to device users, including the silent installation of more dangerous malware. Companies must recognize that fraud awareness, prevention and mitigation are everyday issues that need to be a permanent fixture on the organization's agenda. Apps like WhatsApp must be vigilant in ensuring their compliance with regulatory and legal issues. But lack of user security awareness is the primary contributor to several harmful cyber threats. Consequently, the hardware, operating system and apps all affect the total security state of the device, and this risk increases when a user uses potentially old or insecure devices as to limited knowledge . Most android phones offer to keep user data on cloud. However, like most technology changes, cloud computing presents its share of risks and challenges, which are too often overlooked or not fully understood by people those are frequent to embrace it. As the free apps risk profile and threat landscape in the mobile app is rapidly increasing, People need to change their mindset and approach towards using mobile phone risk to mitigate the emerging risk of android platform. This study takes an in depth look at the risks associated with third party free apps as an example of mobile app risk and suggests credible models so that risk appetites can be aligned with the exposures being faced.

Keywords: Cloud Computing, Legal Issues, Mobile Apps, Security, Technology

1. Introduction

Since its creation over 20 years ago, SMS or Short Message Service has revolutionized the way we communicate. In 2011, 7.8 trillion SMS messages were sent globally, highlighting that SMS is a mass communications medium used by billions of people around the globe. In recent times, however, a new wave of mobile communications services called Mobile Instant Messaging (MIM) applications have gained considerable momentum. Applications like WhatsApp, Viber and Line allow mobile users to send real-time text messages to individuals or groups of friends at no cost. Driven by the evolution and rise in smartphones, along with the decreasing cost and convenience of mobile data plans, it is forecast that these MIM applications will continue to grow unabated

* *Author for correspondence*

and ultimately lead to significant decreases in SMS traffic. One of the most interesting MIM applications on the market today is WhatsApp. WhatsApp is a cross-platform instant messaging application for smartphones. It enables users to send and receive location information, images, video, audio and text messages in real-time to individuals and groups of friends at no cost. Given the availability of WhatsApp across multiple mobile platforms and the fact that it has reached a critical mass of users, it has become a necessity to study the risks associated with third party free apps as an example of mobile app risk and suggests credible models so that risk appetites can be aligned with the exposures being faced. App design is a science and an art. It takes a talented eye to see what works, in terms of both content and palpable features, and what doesn't. Making mistakes is easy; it even happens to major developers like Google and Facebook. These companies frequently release apps that are less than optimally user-friendly, and often have to respond to user complaints with upgrades or bug fixes. Unfortunately, an upgrade isn't always enough. Sometimes, an app needs to be stripped down and re-structured in order for it to be accessible to and fun for users. Here's where "partner apps" come in: independent developers can design apps with innovative layouts that sync information from popular apps, such as Facebook, and display it in a more interesting way. Independently-designed third-party apps at times outperform, out-display, and generally outshine their official counterparts. They show off content better than their official counterparts do, and these apps' growing user bases are living proof that, sometimes, the original isn't the best. For users who download apps from alternative app stores, there's the added task of having to enable downloads from these new sites in order to be able to get the apps on your Android device. In order to do that, a user will need to go into their Settings menu, click on "Security" and then again on "Unknown Sources." Users should also be aware that malware can sometimes be a problem but, if they download an Android security app first and exercise prudent judgment with the content they procure, malware and related security risks can be greatly mitigated.

2. Emerging Third Party Apps and Security Concerns

When deploying a new technology, organizations should be aware of the potential security and privacy impact these technologies may have on the organization's IT resources, data, and users. New technologies may offer the promise of productivity gains and new capabilities, but if these new technologies present new risks, the organization's IT professionals, users, and business owners should be fully aware of these new risks and develop plans to mitigate them or be fully informed before accepting the consequences of them. State, Local and Tribal privacy statutes may be different for each organization; security administrators should consult with the organization's privacy officer or legal counsel to ensure the collection and sharing of data collected using mobile devices is legal. Organizations increasingly rely on third-party software/ applications when computing in the cloud and utilizing mobile computing in order to fully benefit from these forms of computing in business (flexibility and quick to market). Organizations are finding it challenging to ensure that the software they are using is secure and not introducing security risks or vulnerabilities and causing decline to their security posture. Most software used within organizations today is from a third-party source but most organizations do not have the means to evaluate the security of this software. The reliability of third-party software transfers the security of the software into the hands of multiple developers (often a third-party may be outsourcing to another third-party), organizations often assume that the necessary due diligence and security checks have been undertaken. Unfortunately, with so many involved, often this is not the case. The software may not be developed or tested by the same quality and security standards used within your organization. A lot of the time organizations conform to secure development cycles, but with hundreds of third-party libraries being used in a single application, huge amounts of code are likely to not be getting the same level of security checking required. Organization should have sufficient knowledge of where or how the piece of software will be put to use to help understand the risk of threat when using the software. A clear understanding of the software security development lifecycle is key to understanding and managing risk because if you are aware of the process you have the knowledge to ask the right questions and ensure the important security steps and practices are covered.

3. Perceptions of Privacy and Security Violations

App Permissions on the Android platform (and others) the user is informed and must explicitly opt to continue installation of an app if it requires access to personal data,

such as their address book or location. The use apps on smart phones, such as the iPhone or Android platforms, potentially create privacy concerns for users. These apps may access, process and transmit personal data that is stored on the device (such as photos or contact information) or which is available through the various sensors embedded into the devices (for instance location, or even, in the case of some devices, physiological data such as heart rate). Previous research has shown that app users are often unaware of the extent to which apps can access personal data (Kelley et al. 2012; Liccardi et al. 2014) and the potential privacy and security issues that this access can cause. Despite the presence of this supposedly informing feature, many users still find app behavior 'creepy' (Shklovski et al. 2014) which suggests that it is not succeeding in fully reassuring or empowering app users.

4. A Case of "Happy Calendar 2011"

User A prefers to block disclosure of her birthday. Accordingly, her privacy setting for this information category is "Only me", which means her birthday cannot be seen by other users on Facebook except herself. When this user adds the app "Happy Calendar 2011" to her profile, she is asked to grant the app permissions to access her and her friends' birthdays and to publish them. Like most users, User A immediately grants the app all requested permissions. Later, User A finds out that "Happy Calendar 2011" created an album in her profile and posted all her friends' birthdays that she can access, as well as her own, in a calendar image with their profile pictures being visible in the corresponding date fields. Moreover, User A's friends received a wall post notifying them of the creation of this album and how they can access it. As a result, the "birthday", which User A intended to keep private, is now accessible by her friends. It is considered a case of privacy violation in which the third-party app overrides users' global privacy settings.

5. Facebook Apps

The popular social media site has been plagued by privacy issues over the years. Its highest-profile problem was in October 2010, when Facebook admitted that its top 10 most popular applications including FarmVille and Texas Hold`em shared user data, including names and friends' names, with advertisers. A Wall Street Journal investigation uncovered the Facebook privacy breach and said it affected tens of millions of users, including some that had used Facebook's most stringent privacy settings. Facebook had previously been in trouble for transmitting user ID numbers to advertising companies when users clicked on ads.

6. Carrier IQ

The year 2011 closed out with another privacy-oriented brouhaha, this time surrounding Carrier IQ, which sells analytics software for mobile devices. The software is used in an estimated 142 million smartphones. A systems analyst/amateur security researcher discovered this software on his smartphone, and found that it was capturing battery life, connections, text messages, emails and other actions. A slew of accusations followed, with Carrier IQ and its carrier customers being taken to task for allegedly keylogging, spying and tracking. But more detailed analysis by other professional security researchers found that the systems analyst who originally raised the issue was confusing Carrier IQ's actions with those of debug statements mistakenly left in the Android code by phone maker HTC's programmers. As it turns out, Carrier IQ was simply collecting performance data for optimizing the end users' experience. Nevertheless, the original discovery prompted Sprint and HTC to reportedly no longer include the Carrier IQ software on their devices.

7. The Yahoo Security Breach

No company is more aware of the danger posed by poor third-party code than Yahoo, which has suffered a number of high-profile incidents in recent years. In 2010, Yahoo acquired the online publishing platform Associated Content and rebranded it as Yahoo Voices. Even though the rebranding process didn't take long, Yahoo didn't immediately integrate the Yahoo Voices accounts into its own authentication process; rather, it relied on its existing platform. Two years later, a hacker found a SQL-injection (SQLi) vulnerability and used it to penetrate the Yahoo Voices servers, collecting more than 400,000 usernames and passwords. A similar attack occurred later that year, when a hacker used SQLi to gain access to AstroYogi, an India-based astrological website. The problem for Yahoo

was that it contracted with AstroYogi and rerouted users from its Lifestyle site to the affected astrological website, which operated under the Yahoo brand. Because user credentials had to be sent to the vendor, the hacker had access to the credentials of any user visiting the astrology site. In this particular case, the hacker appeared to be benign (going public with the hack only after Yahoo ignored requests to fix the vulnerability), but Yahoo's reputation certainly took a hit.

8. Snapchat

A recent case of Snapchat who finally let users knows that third-party apps are saving their pictures and videos. A third-party website named SnapSaved.com allowed users to covertly save incoming messages by giving their login details to the site. This let SnapSaved access Snapchat's servers on their behalf and store their images permanently on the site, which was itself hacked by unknown individuals. SnapSaved was a website (it's now offline) while SnapSave is an app. The two programs offered an identical service and used similar branding but appear to be unconnected, with the creator of SnapSave (that's the app) telling tech site Engadget: "Our app had nothing to do with it and we've never logged usernames/passwords."

9. Possible Security Risks and Concerns from Third-party Software Utilization

- Security testing and quality of testing may not meet your organizations standards or compliance.
- Third-party software may contain security related weaknesses or flaws enabling internet attacks and security vulnerabilities compromising business data and assets.
- The code libraries utilized may not be actively maintained.
- Multiple code libraries are used.
- Multiple third-party suppliers are utilized increasing the area for compromise.
- Software performance and functionality may be hindered.
- Patching is usually not carried out quickly enough once a vulnerability is realised.
- Reasons for slow patching may include;
- Time needed for testing and validation.
- Lack of management tools.
- Having inadequate resources.
- Concerns over service levels.
- Patch inadequacies.

10. Challenges of using third-party software

- OS's have stepped up and have become more resistant to attack leaving third-party software as the culprit of majority of security compromises. Recent findings indicate that vulnerabilities in third-party software account for majority of occurrences of malware on Windows endpoints.
- Organizations are ultimately responsible for ensuring controls are in place to mitigate the security risk and to manage the liability of using third-party software. Once the software or code is part of the organizations system the organization becomes responsible for the security, quality and safety of the software.
- Software vulnerabilities are directly linked to business risk. A flaw in the software can impact customer satisfaction, brand or business image, revenue, time to market and competition for market leadership.
- The relationship between software security and business risk is placing emphasis on the importance of securing third-party software and ensuring it is developed with quality, safety and security in mind.

11. Suggestions

The following steps can be taken to mitigate the security risk and determine the integrity of the software:

Some questions which may point you in the right direction may include (the answers to the questions will be unique to each business/organization/ individual and will assist in achieving an informed decision of software usage under varying circumstances):

- Is it possible to test the third-party code for security flaws in a test environment before going live?
- Once live can the third-party component be tested?
- Will the third-party software/plugins be accessible publicly?
- Do you know of any listed vulnerabilities with the third-party software or code?
- If you are compromised because of a third-party flaw, what is the worst outcome for your business?

Through great consideration you've decided to use the third-party software, further steps that can be taken:

Implement security measures that will assist in assuring that the third-party software meets your industry security standards and compliance requirements. Treat assessment of third-party software with the same meticulousness you would in-house software. Put policies in place that the third-party software management must conform to when developing to ensure your security and compliance requirements are effectively met.

- Third-party software suppliers should use mature development practices and provide a track record that quality, safety and security requirements are met.
- Ensure the highest quality code is being used.
- Ensure appropriate testing is undertaken at development so that defects can be resolved early on in the development cycle.
- Demand visibility and insight into the quality and security of the third-party code.
- Security testing of the software is essential (unit testing, assessments, pen testing code, scanning the software both automatically and manual testing is recommended, compliance audits).
- It's essential that third-party software/applications are managed and patched regularly. As with operating system patching should be prioritized and be made a routine practice. Automated application patching tools can make this less cumbersome. Although patch management of third-party applications and software has become more challenging within the mobile computing environment, it's essential that organizations rise to the challenge as the risk to data security and compliance is great. Antivirus, web filtering software, application firewalls and whitelisting combinations can help to achieve a defense-in-depth approach. Having control over the third-party software/applications is a proactive means of managing security. Through taking back control and choosing the third-party software suitable to your business risk level you are able to mitigate the security risk. Do not allow unauthorized third-party software/application, not only are they likely to be laden with vulnerabilities they will also be more challenging to patch. Unauthorised third-party software may also have an effect on the business compliance.

12. Conclusion

In this mobile environment where pressure for rapid development is high, organizations are now heavily reliant on third-party code and software usually from multiple sources and suppliers. Organizations need to remain observant about potential hazards in the security of third-party software. Have a team that can remain abreast of the security issues and who are aware of the threats and vulnerabilities. Collaborate with the broader security industry to keep on top and proactively work together to increase the security posture all round. Be responsible with your third-party software choice; be

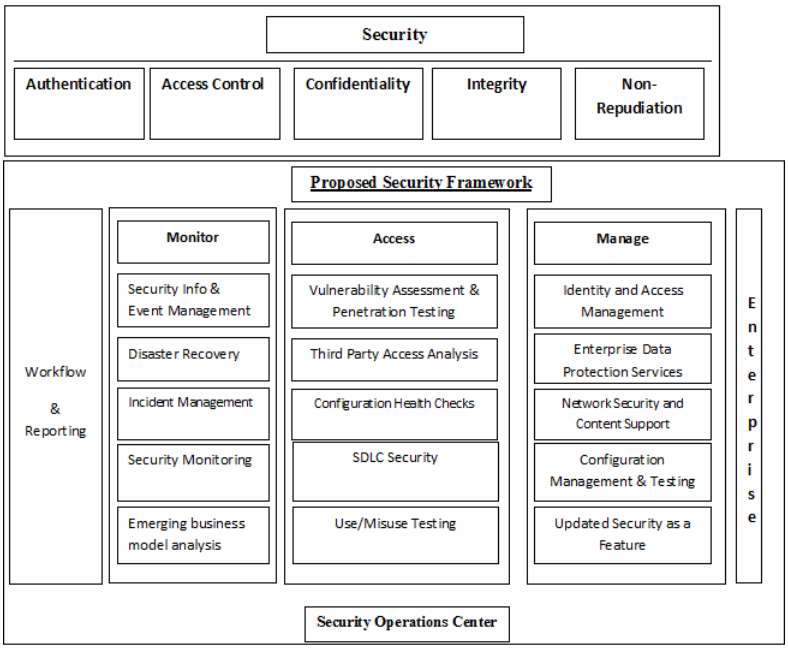

Figure 1. Proposed model to mitigate emerging third party apps vulnerabilities .

mindful of all compliance warnings. Today Data security is of paramount importance and any security breach will not be looked upon lightly. Any breach, albeit through a third-party software flaw, will still be the organizations responsibility. The key message is limit the use of software that may cause your organization a security issue and ensure that if third-party software is required that it is properly maintained and patched.

References

1. Debatin, B., Lovejoy J., Horn A., and Hughes B. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer Mediated Communication, 15*(1), 83-108.
2. Facebook Statistics. 2010. Retrieved from http://www.facebook.com/press/info.php?statistics.
3. Hull, G., Lipford, H., & Latulipe C. (2010). Contextual gaps: Privacy issues on Facebook. Ethics and Information Technology.
4. Mylonas, A., Meletiadis, V., Mitrou, L., Gritzalis, D. (2013). Smartphone sensor data as digital evidence. *Comput Secur. 38*, 51-75.
5. Pearce, P., Felt, A.P., Nunez, G., & Wagner, D. (2012). *Android: privilege separation for applications and advertisers in android.* Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security (pp. 71-72).
6. Shehab, M., Marouf, S., & Hudel, C. (2011, July). ROAuth: *Recommendation based open authorization.* Proceedings of the 7th Symposium On Usable Privacy and Security (SOUPS), Pittsburgh, PA.
7. Steel, E., & Fowler G. (2010 October). Facebook in privacy breach. *The Wall Street Journal.*
8. Retrieved from http://www.windowsecurity.com/articles-tutorials/misc_network_security/third-party-software-security-threat-part1.html
9. Retrieved from http://www.independent.co.uk/life-style/gadgets-and-tech/the-snappening
10. Retrieved from http://www.forbes.com/sites/jameslyne/2014/01/31/yahoo-hacked-and-how-to-protect-your-passwords