MOBILE APPS SECURITY MANAGEMENT

Roy Griffin, Sara Forkey, and Young B. Choi
Department of Business, Leadership, and Information Systems
College of Arts & Sciences
Regent University
1000 Regent University Drive
Virginia Beach, VA 23464
USA
e-mail: {roygrif | sarafo1}@mail.regent.edu, ychoi@regent.edu
Tel: (757) 352-4949

Abstract

In this Research paper we will identify various security management techniques for Mobile Apps. The authors will also discuss how to detect an intrusion in the consumers' mobile device due to malicious apps and how to handle an infiltration. The authors will also discuss mobile app security and developing and maintaining security app programs, as well as, security management models and practices.

1. Introduction

Mobile devices have exponentially increased in their use in the general population for the last few years. Most consumers have in their possession some form of mobile device whether it is a smart phone or an iPad in which they can download applications, otherwise known as apps, from which they can play games, keep their lives organized through calendars, or even do online banking. "While most of the data services are being accessed directly through the GPRS, the App Store is a service, which allows users to browse and download applications from the WEB Store that were developed with the Phone SDK and published through the phone vendor. Depending on the application, they are available either free, or at a cost. The applications can be downloaded directly to target device, or downloaded onto a computer. These APP stores was first introduced by Apple IPhones, later released by many of the other market contenders of high-end internet phone vendors like Blackberry, Nokia, Android, Palm and etc, etc" (TM Forum 2014)[1] With the emergence of a mass production of these apps, it is imperative that the end user be vigilant on keeping their mobile device safe from harm from the cyber community. Just because an app is available for download off of the Internet does not deem it safe from malicious intent. It is difficult for the end user to determine whether the app is legitimately safe and free from viruses. These challenges are making the agencies more aware that special attention needs to be directed towards the management and protection of these apps.

2. Mobile Apps

Mobile applications have become one of the world's focal points when it comes to technology. There are millions of apps that are being used today on multiple mobile devices. When looking at this situation from a whole, there are many issues to take into consideration. Our main thought is security and how well we can protect our information from all being affected by all of these programs. Creating a security app to put on these devices for protection is the best way to go about this scenario. We need to know how to manage the security for our own personal data. Isaiah 41:10 states "Fear not, for I am with you; be not dismayed, for I am your God; I will strengthen you, I will help you, I will uphold you with my righteous right hand" (Bible.ESV)[2]. Placing a security management app on your portable device eases the minds of the consumer by assuring the end user that their device is protected from malicious attacks and can be monitored with the latest software available.

3. Security

More and more companies lately are paying more attention to the security of their data due to recent infiltrations in major corporation's systems. For instance, the major company Target was attacked

[1] TM Forum
[2] Bible.ESV

and billions of customers' personal data was compromised. "Before the attack, Target installed security software designed by FireEye, a security firm based in Milpitas, Calif., according to two researchers who spoke on the condition of anonymity, citing client confidentiality. FireEye's software, as it turns out, worked as designed. It isolates incoming web traffic and looks for suspicious activity. In Target's case, the software sounded multiple alarms as criminals uploaded tools to siphon out customers' credit and personal data." (The New York Times, 2014)[3] When the technicians reviewed the details of the infiltration, they communicated that it was not necessary to follow-up with any actions or interventions and was eminently dismissed. This proved fatal to the Target Corporation resulting in thousands of dollars lost, key personnel that resigned from their positions, and ultimately a vast amount of customer loyalties were lost. Other corporations learned from the mistakes that Target has made and are vigilantly monitoring their systems for infiltrations that could ultimately be of malicious intent. All mobile devices are prone to attacks from viruses, worms, and other malicious attacks that could render the end user a victim to a data breach.

When creating a security application, an organization needs to think about their values and come up with a vision and mission statement. "Research shows, however, that the writing of a mission statement is directly linked to greater returns on investment in companies. Additionally, businesses with mission statements have double the return on equity than those who have not written one" (Blake, 2010)[4]. This gives the audience an idea on what to expect from the actual company putting the application out for download. If it seems like they are about ethics and good moral values in regards to protecting privacy and sensitive data, then it would be more likely to draw people in to download the security software. Usually, people tend to download the most trustworthy app over the one that is less likely to be reputable. Most people are pro-safety. They will go above and beyond to protect their portable devices from being infiltrated by harmful software.

In order for a project to stay above the target time line, strategic planning must be put in place. This takes a team effort while not only the project manager having to work hard but also the employees within the crew. Everyone works together to make sure it all comes together by a specific date. Once the outline has been developed, proper planning for security implementation is created. The manner of when and how the company could put updates out to allow for continuous protection would be important. All these things need to be taken into consideration when managing mobile app security. Constant updates are needed to keep up with all the devices and new applications being developed. If nothing else, just recognizing malware so it protects your device. Now this would be a difficult task but certain apps are developed to obtain specific types of information such as the types of software you tend to download and how well it may perform on your given device. It takes all this information and puts it together. This allows for easier comparison and results in order to serve the customer much better.

4. Contingencies

When managing security for your mobile device, the security app that is being creating should be prepared to deal with the impact of an intrusion on the mobile device. "The BIA becomes the foundation of the plan you will build for your recovery. This is the process that will determine what needs to be recovered and how quickly" (Okolita, 2009)[5]. The response to an incident in such a case should be given multiple choices depending on the threat. Obviously if it were a virus, it should be quarantined and then deleted. If it is malware or a junk app trying to pull your information, the user gets choice of what is to be done regarding removal or accepting the risk involved. Users tend to just click continue and not worry about what impact it could have on their system. If a disaster was to happen such as destroying their data or bricking (locking) the phone or tablet into an unusable condition, then some sort of disaster recovery should be put in place. Customers would be safe and their data would be recoverable. A good idea or this situation can been seen in cloud use. Many developers and software companies are not going to this type of situation. This is actually being done in the local school systems around the Hampton Roads area.

5. Information Security Policies

Policies, standards, and practices should be put in place to makes sure that production and continuing services such as monitoring and updating new threats are kept up to par. These are more like guidelines to follow when performing a duty or task, which allows for directions to be carried out, as they

[3] The New York Times
[4] Blake
[5] Okolita

should be. When creating these policies, we have to think about all aspects of the operation such as developers and users. Obviously the developer has to follow certain standards when creating security apps. Although when a user has installed one of these apps onto their device, they must manage this to a certain degree as well. If they choose to manually update the definitions or set certain standards, then their roles must be done appropriately as well. "By merging the business needs with the security and technology standards and requirements early in the process, it's possible to both reduce development times and increase the security posture of a project all at once" (Colson, 2011)[6]. If a security app explains the best way to manage ones item that the software is placed on, then the person may want to follow the directions to the tee. These directions are given for a reason and this reason is to ensure the safety of your data.

The guidelines for effective policies should be defined very clearly so everyone can understand how to operate the application. This comes in the play when the software is being created. The person managing or overseeing the entire project should make sure this is one of the main operations done correctly. It allows for easy user access and higher download possibilities the easier the user experience is. Complicated items never really receive too much attention because there are just too many people that do not know how to use technology.

6. Developing the Security Program

In order for a manager to have their application be effective, they must be able to create it so that it works on multiple devices. This allows them to have a broad range of options and possible income. The only downfall to offering a wide range is that it creates more of a security issue because of different holes in the devices that could possibly be penetrated by intruders. "Decision-makers need to prioritize the management of applications or risk losing everything. In most cases, application security strategies should be able to identify software and its components, recognize the presence of risk and mitigate the potential damage proposed by these threats" (COPPEREGG, 2013)[7]. This is where managers should over-see a large operation and should consider different components to be placed within their software. Just as though Apple has features that Android does not. Each has their own uniqueness when which causes smaller companies to modify their code in each of their own programs offered. There is a great misconception in the community that Apple products have no "bugs" while the Android products have the most. While the Android platform does seem to have the most known issues and greater infiltrations, the Apple platform has a great many glitches in its software and apps as well. A great many end users decide to "jail-break" their iPhones so that they can manipulate the apps that they install on their devices, while the Android users seem to have the luxury of being able to manipulate their devices as they see fit. This security concern should be taken into account when developing the individual programs for each system.

7. Security Management Models

Since there are a large variety of different operating systems to create applications for, blueprints, frameworks, and security models should be drawn up prior to the actual start of operations for writing code. This will allow us to see the relationships between each component and items inside the software. It will also allow us to see what kind of access controls is needed and what criteria should be met. With the emergence of more BYOD (Bring Your Own Device) to work programs at multiple corporations, the usage of MDM (Mobile Device Management) is more important than ever. "Most Tier 1 MDM vendors have some application management capabilities; two examples include MobileIron and AirWatch, but there are many more. We expect the overlap between MAM and MDM tools to increase in 2012, as many MDM vendors already have a solid application offering and app store capability." (Gartner 2012)[8]

8. Security Management Practices

Well-designed applications go by benchmarks and what standards have been met along the way of development. "Benchmarking is a systematic process for comparing business performance or processes in different organizations, or between groups of organizations, to learn whether, and how, things may be done better" (Hall, 2012)[9]. These act as blueprints of the project at hand. This allows for everyone working in

[6] Colson
[7] Copperegg
[8] Gartner
[9] Hall

the team to see what should be happening and different points along the way. Standards should be met and the ones managing the operation should recommend security practices. "In a world dominated by mobility, interaction and loss of privacy, it is necessary to adopt new practices of security and control that enable organizations to meet the challenges of a moving society exposed to continuous data leakage." (Dwivedi, 2010) [10] While it would be nice for standards and benchmarking to be a common practice and the same for each corporation, they are not. It is up to each corporation to ensure that they hold the highest standards for their products and place their customers' safety and well being above themselves.

9. Responsibility

Ultimately whose responsibility is it to keep the applications safe for mobile devices? Is it the responsibility of the data programmer who created the application and knows every single line of code inside and out? Is it the responsibility of the cell phone carrier such as Verizon Wireless or AT&T because they made the app available for the consumer to purchase on their mobile device? Is it the responsibility of the end user to ensure that they are purchasing a legitimate app for their phone and that their personal information will remain safe and secure on their phone? The answer should be all of the above in all cases, but sometimes this is not the case. Sometimes the end user would like to purchase an app that is unsafe and not even know it. "The growing popularity of wireless technology may have finally attracted enough hackers to make the potential for serious security threats a reality. The world of computers and communications, the more widely a technology is used, the more likely it is to become the target of hackers. Such is the case with mobile technology, particularly smartphones, which have exploded in popularity in recent years. Many users download mobile applications with little regard to whether they're secure, providing a ready way for hackers to attack the device." (Leavitt, 2011)[11] Unfortunately, for a regular end user, it is near impossible to detect an app that has malicious intent. Sometimes the apps that are virus stricken are poorly written and do not work very well. This is a sign for the end user to know that this app is not one that they should be placing on their mobile device. However, there are other times where the program is written in such a cunning way that the end user has no idea that they have an illegitimate app on their device until it is too late and their data has been compromised. This then becomes a very unfortunate mistake for the end user and can become very costly as well.

10. Detection and Prevention

How is a typical end user able to detect that a malicious app has been downloaded onto their mobile device? Unfortunately, it is very difficult for the average end user to detect a malware intrusion before any damage has been done to their phone and their personal data. ""We've seen malware designed to secretly track users' physical locations via GPS, make phone calls, send text messages , exploit ad networks and even gather potentially sensitive data ," said Jeffrey Wilhelm, a senior analyst at anti-virus software giant Symantec. "That said, the fact of the matter is that mobile malware will likely only continue to be of interest to cybercriminals if they can figure out a way to monetize it. At this point in time, they are still very much in the exploratory phase of figuring out how to do that."" (Poremba, 2011)[12] First and foremost, the end user should stick to legitimate companies that they know and trust. Not all apps from well-known companies are going to be 100% safe all of the time, but apps from "off-vendor markets" are going to be more risky and more likely to contain malware. The end user should also trust their gut instinct. If an app seems too good to be true, then it most likely will be. A free app from an off the wall named company with lots of bells and whistles will most likely be harmful for your mobile device. Also, a good idea is to read the user reviews before hitting that download button for your latest app. "Other users will tell you if there were problems with an app, including potential malware. And if you find that an app you downloaded was malicious, Wilhelm recommends adding your own review at the app's marketplace." (Poremba, 2011)[13] Word of mouth is a great forum that is still being utilized today, but blogging and placing your thoughts and opinions on websites such as FaceBook have become most customary and an even faster form of getting the word out to the public. Before giving into that temptation of downloading your very first app on your brand new mobile device, a very wise idea would be to download a security app for your mobile device. There are a vast amount of security management apps that you can download to your mobile

[10] Dwivedi
[11] Leavitt
[12] Poremba
[13] Poremba

device to protect yourself from a malware attack. Anti-virus apps such as TrendMicro and Symantec are a good idea to have on your mobile device to protect yourself from harm. It is also a good idea to keep your mobile device up to date on the latest software updates and patches. Keeping your mobile device's software safe from harm is just as important, if not more so, than keeping it physically safe from physical theft and harm as well.

11. How to Detect

What should an end user do if their mobile device becomes infected with a malicious app? How can the end user detect that their device has become infected? This question can be answered with a number of other questions. Is the device working to optimal performance or has the performance become increasingly slower and slower? Has the battery life on the device become increasingly shorter and shorter and now the device runs out of "juice" faster than ever? Are the calls being dropped or even interrupted with weird noises in spots that have previously not been any problem then before? These are all sure signs that your mobile device has probably been infected by a malicious app that you have downloaded onto your device. So, what is the next course of action for the end user? Malware detection software might be a good tool to download onto the device for detection and cleanup of this atrocity. There are many malware protection apps that can be downloaded such as Malware-bytes, which can aid the end user in detection and deletion. It is recommended that the end user also run a malware app scan routinely as well. This will also keep the mobile device clear of known malware and the end user will have some piece of mind that their device is safe and secure from cyber intrusion. Anti-virus software is also a good idea to have on your mobile device as well. This kind of software can detect viruses as well as other forms of malicious attacks that can infiltrate your system and cause chaos for your personal data. Also, it is always a good idea to keep your systems software up to date through the device manager or systems settings on your mobile device. This allows the device to download certain patches and fixes for bugs and glitches in the system, allowing the system itself to run optimally, and thus allowing the anti-virus software and the anti-malware detection devices to run optimally as well.

12. Conclusion

Consumers will always be fascinated by the latest and greatest technology that is being developed and placed into the market. They will always crave to have the newest technology that is available to them whether it is the newest iPhone or the latest Android phone. Mobile apps operate much in the same concept as this, however consumers tend to download more and more apps since most of them are available for free or at a reduced price. Consumers also yearn to have the newest mobile app that they can find, and if they cannot find it for their version of their platform, they could potentially download an app that contains a malicious virus that could be detrimental to their personal security. Mobile apps are downloaded for multiple reasons. Whether it be to organize your personal life through a calendar, make your life easier through an app that stores all of your passwords, to just a simple game app, the end user expects these apps to be safe and secure. It is the ethical responsibility for the developers of these apps to ensure that they are free from harm and safe for end users to download and utilize, but it is the ultimate responsibility of the end users to take it upon themselves to manage the security of their apps and render them safe from malicious attacks. Keeping the device up to date on the latest software upgrades and patches is the responsibility of the end user as well and this will ensure that their mobile device is up to the challenge to face the murky waters of the Internet.

References:

*Harris, Elizabeth A. and Perlroth, Nicole. (2014, March 13) Target Missed Signs of a Data Breach. Retrieved from The New York Times. http://www.nytimes.com/2014/03/14/business/target-missed-signs-of-a-data-breach.html

*Bible.ESV

*Blake. (2010, December 09). The Importance of a Mission Statement. Retrieved from Think Big Partners : http://www.thinkbigpartners.com/start-a-business/202-the-importance-of-a-mission-statement.html

*Colson, S. (2011, November 19). Project Management. Retrieved from InfoSpace: https://infospace.ischool.syr.edu/2011/11/19/information-security-why-policy-matters/

*COPPEREGG. (2013, Feb 28). 3 components of monitoring application performance, security. Retrieved from Copperegg: http://copperegg.com/3-components-of-monitoring-application-performance-security/

*Hall, P. (2012, Aug 31). Why is Benchmarking Important in Business? Retrieved from Small Business Advice: http://smallbusinessadvice.org.au/business-tools/benchmarking-important/

*Okolita, K. (2009). What is a Business Impact Analysis. Retrieved from CSO Online: http://www.csoonline.com/article/2124593/emergency-preparedness/how-to-perform-a-disaster-recovery-business-impact-analysis.html

*TM Forum (2014) *Mobile Data and App Store Analytics.* Retrieved from TM Forum: http://www.tmforum.org/MobileDataandApp/9475/home.html

*Redman, Phillip. (2012, September 07) There's an App for That: The Growth of Enterprise Application Stores. Retrieved from Gartner. https://www.gartner.com/doc/2150915?ref=SiteSearch&sthkw=mobile%20app%20security%20management&fnl=search

*Dwivedi, H., Clark, C., & Thiel, D. Mobile Application Security.

*Leavitt, N. (2011). Mobile security: finally a serious problem?. Computer, 44(6), 11-14.

*Poremba, S. (2011). How to Detect Malicious Android Apps Before They Infect You. Retrieved from TechNewsDaily: http://www.technewsdaily.com/7260-android-malware-detection.html