Jailbreak and Mobile Security

Author: Zedrick A. Maldonado Burgos
Advisor: Jeffrey Duffany, Ph.D
Department Electrical and Computer Engineering & Computer Science Department

Abstract

In these modern times mobile devices are part of the everyday life of each individual. These devices contain a major part of each user information in comparison to their personal computers. On a mobile device people can access their bank account and make transactions with ease and eliminating lines in the bank as the mobile devices are always connected to a network. By having compute power and ease of transport in a person's pocket these devices are becoming the primary computing device of people. In this paper there are the two sides of vulnerabilities that are the use of these to implement code that allows modifications called Jailbreak and Rooting. The other side would be the patching and security that developers go through to prevent unauthorized access and strengthen end user security. Mentioning their update cycle and vulnerabilities database overview.

Introduction

In this paper we can see that the main mobile devices to be looked at are the iPhone by Apple that is directly associated with the iOS operating system. As for the Android side of operating system we see hardware by Samsung mobile as it is the most market share among Android devices. For the Jailbreak process there is from the beginning of this practice the JailbreakMe exploit by Comex that it was a simple method of just doing the gesture of sliding the button on the screen to the right to initiate the Jailbreak process and install the first store for third party applications on the iOS environment. There is the mention of another Jailbreak software from the Pangu Jailbreak team that it is a tool that requires a computer and the mobile device connected to it to be able to Jailbreak the phone. By looking at the mentioned and going into detail we can see the contrast of the two worlds of mobile usage, the part about using the exploits in benefit of the end user and how this can also affect the user by utilizing not known sources. The other part being how manufacturers of these mobile devices handle such exploits in their mobile operating system updates and small iterations of the same version of operating system.

Background

To have an understating of the jailbreak and rooting methods of the mobile operating systems there are some methods that can be looked at. The states of the jailbreak mean the different ways a user can start and use the device when a jailbreak is desired to be executed on the device. The user should be aware of these states and choose the one that fits the current desired use. Searching for the author of the jailbreak from official sources can help to prevent the execution of undesired sources as third party can modify the application to gain access to the device. When rooting and Android device is good to have a backup of the information in case the mobile device needs to be formatted. When installing third party APK files on the Android operating system is good practice to verify the source and an available review for any viruses. Allowing some time to pass before proceeding with a jailbreak or rooting is good as a new iteration of the exploit could be updated and be more stable. Meaning that if the user did it day one, it would have to go to the jailbreak and rooting process again.

Problem

This research shows how mobile device users utilize their devices in their daily lives. Meaning that these users would search for ways to have the most out of their devices. In this research it can be seen as two parts of users, users that tend to jailbreak and root their mobile devices to have features that the manufacturer does not provide currently as an out of the box experience. By this happening the research shows different ways of benefit and non-benefits by this practice. The other side of users is the one that wait for the operating system updates to have official features by the manufacturer of their chosen device. Not opening their device for third party unofficial code.

Methodology

The research was outline by looking at the timeline of the modifications that have been realized during the years on mobile devices. These modifications were installed on mobile devices by jailbreak methods such as visiting a website that when the slide to unlock was done inside it ran a code on the device therefore installing an app that allowed third party software. Installing custom firmware on the device that were pre-modified by the community is a method that does not require a special software. This would be to install at the boot level of the device. In Android this would mean to put the firmware inside its flash storage device and install it via the recovery mode. In iOS the end user would need to use iTunes, put the mobile device in recovery mode and install the firmware via iTunes

Figure 1
JailbreakMe Message on Home Screen

Figure 1 is the homescreen of the website JailbreakMe by Comex. This website utilized the Safari web browser vulnerarbilities in that specific operating system version, in this case the first version was 1.1.2. This used a TIFF exploit against the Safari browser, after the process it installed the installer.app on the mobile device. This opened the possibility to install third party modifications, tools, apps and tweaks.

Figure 2
Cydia Store Home Screen

In figure 2 it shows the starting page of the Cydia Store by Jay Freeman (Saurik). This store is the successor of the installer.app that started the third party software and tweaks. This store allows developers to publish their software for free or charge their desired amount for themes, tweaks, applications and tools. In here the end user is allows to install repositories to open the amount of installable products.

Results and Discussion

We see the install of a modern third-party store for third party applications, tweaks and tools called Cydia. This store was created by Jay Freeman known as Saurik. This store is able add online repositories such as to make available stores to download free applications that are paid apps on the App Store. The tweaks available in these stores make the use of social media apps more robust as it offers a set of options that users can take advantage during their daily use. Performance on the Jailbroken device is something to consider when jailbreaking a device as it can slow the performance on a daily used app for example the camera app. The benefits of jailbreaking and rooting can also be seen as it can offer tools, modifications and widgets that can make the daily use of the device more pleasant.

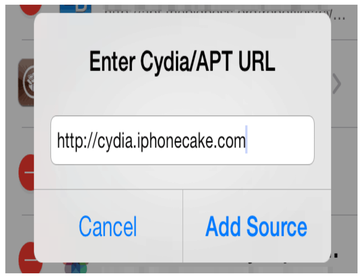

Figure 3
Adding repository to Cydia

Figure 3 is an example on installing a repository on the Cydia Store:
1- Press the Sources tab inside the Cydia Store.
2- Press Add
3- A window appears that says Enter Cydia/APT URL with the http:// already populated
4- In the field type cydia.iphonecake.com
5- Click on the Add Source button
6- A warning shows informing the user that the source contains pirated content and advising the user of copyright work.
7- It will prompt with an Add Anyway button.
8- After adding this source to the Cydia store the AppCake application is available for download
9- On the Search inside Cydia type AppCake and it will appear on the results.

Category	Max Payment
Secure Boot Firm Component	$200,000
Extraction of Confidential material protected by the secure enclave processor	$100,000
Execution of arbitrary code with kernel privileges	$50,000
Unauthorized access to iCloud account data on Apple servers	$50,000
Access from a sandboxed process to user data outside of that sandbox	$25,000

Figure 4
Apple Bounty Program (Bug Report)

This program was introduced by Apple to have the community of security researchers and hackers submit their findings. After the person submits their findings via a report, Apple decides in what category it is in and it would follow with a payment process.

Conclusions

Exploiting the vulnerabilities of a system is something that will be present for years to come. Security will keep getting better as vulnerabilities are discovered and are published. By being public knowledge, these flaws are put into consideration at the end user level when they are to make a purchase. By manufactures working on new security updates mobile devices can be a welcoming experience to replace a mobile computer for not hardware extensive tasks giving the user a level of sureness. The vulnerabilities as can be seen with Jailbreaking and Rooting can be in benefit of the user for features outside of the manufacturer and developer standards or features that are not available yet on the operating system. Mobile operating system security updates should support older devices even though if they do not have the latest features, this way the user should not get penalized on security by not having the latest model. Manufacturers seeing this movement of users tending to free the device should hear this community of users and implement certain tweaks, widgets or applications that are available via these markets. This way users can have a device that is not opened for third party code execution as they would have the desired feature available with official support. Jailbreaking and Rooting can give a push to these developers and mobile operating system can keep getting more secure as time passes.

Future Work

One way to have a better understanding of the execution of these tools, widgets and modifications is to find one the mentioned and see the code. This way one can compare this modification, widget or app and compared it to a official app that went through the official application store guideline. Something to consider would be to search for the known vulnerabilities that are published and see how that code works and how it could be opened to execute a third-party code. A scenario that can be worked on would be to document the error messages that are received when a third-party store would be installed on a non-jailbroken or rooted device. On Android it would good to get a smartphone and try to flash the rom for a different version of the official supported operating system and document the findings. Also, an example of how a device works when it is bricked when a jailbreak or rooting it is not done correctly. Another research would be to see the uploaded and reported bugs that has been delivered to the Bug Reporting programs and see what would be the process to submit a bug that could be found on a researcher end.

Acknowledgements

Thanks for the support and guidance of the Dr. Jeffrey Duffany. His insights helped to see other ways to look into the research.

References

[1] https://ioshacker.com/cydia/use-multiple-social-accounts-apps-social-duplicator-tweak
[2] https://ioshacker.com/cydia/use-multiple-social-accounts-apps-social-duplicator-tweak
[3] https://www.gartner.com/newsroom/id/3415117
[4] https://press.trendforce.com/node/view/3067.html
[5] https://theleaker.com/android-o-8-0-update-smartphoneslist/#Android_O_80_Oreo_Update_Supported_Devices
[6] https://www.techrepublic.com/article/ios-and-android-security-a-timeline-of-the-highlights-and-the-lowlights/
[7] https://developer.android.com/distribute/best-practices/launch/launch-checklist#top_of_page
[8] https://developer.apple.com/app-store/review/guidelines/
[9] https://developer.apple.com/support/membership-fee-waiver/
[10]https://androiddevelopers.googleblog.com/2017/12/improving-app-security-and-performance.html
[11] https://liliputing.com/2013/09/64-bit-chip-iphone-5s-matters.html
[12] https://www.anandtech.com/show/7335/the-iphone-5s-review/4
[13]https://www.emarketer.com/Article/How-Often-Do-Mobile-Users-Upgrade-Their-Devices/1011839
[14] http://samsung.youmobile.org/
[15] https://www.makeuseof.com/tag/security-upgrade-android-8-oreo/
[16] https://developer.apple.com/support/app-store/
[17] https://developer.android.com/about/dashboards/
[18] https://www.lifewire.com/compare-iphone-models-1999430
[19] https://support.apple.com/en-us/HT208463
[20] https://source.android.com/security/bulletin/2018-05-01
[21] https://nvd.nist.gov/
[22] https://fossbytes.com/best-android-file-manager-explorer-apps/
[23] https://support.apple.com/en-us/HT201954
[24]https://motherboard.vice.com/en_us/article/yp3nax/jailbreaking-iphone-rooting-android-does-not-void-warranty
[25]https://www.mlmlaw.com/library/guides/ftc/warranties/undermag.htm
[26] http://iphonedevwiki.net/index.php/Daemons
[27] https://www.cultofmac.com/393135/does-jailbreaking-your-iphone-really-slow-it-down-yes/
[28] https://beebom.com/how-force-doze-mode-android/
[29] https://pangu-jailbreak.en.lo4d.com/virus-malware-tests