Jailbreak Vulnerability & Mobile Security Updates

Zedrick A. Maldonado Burgos
Master in Computer Science
Advisor: Dr. Jeffrey Duffany
Electrical & Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

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.*

Key Terms — *Jailbreak and Rooting, Mobile Security Features, Third Party Modifications, Update Cycle.*

JAILBREAK AND ROOT

Users that buy a mobile device have a range of settings and features that they can configure to their liking depending on their everyday use. These features can take advantage of the hardware so that applications can work in a desired way. Apart from these features users want to edit settings in a certain way or have found an application that is not on the official store of applications for both mobile operating systems. By the thought of this modifications and non-supported applications comes the way or jailbreaking and rooting a mobile device. Jailbreaking can be associated with the iOS operating system and rooting with the Android operating system.

These methods allow the user to have elevated privileges on their device to root level. This means that the user can see all the filesystem of the device and can modify it. One of the first things that a user would install on the iPhone by using the Jailbreak method would be the store that it is called Cydia. This store has a collection of repositories from default that have widgets, new settings for the device, graphical user interface modifications, applications that are not on the App Store and the ability to unlock the smartphone from a carrier via software. In the Android side rooting would allow elevated privileges for the user and would have the same modifications that Jailbreak allows. From the start Android allows more modifications of the operating system by default but by doing the rooting it will give all the access to the phone.

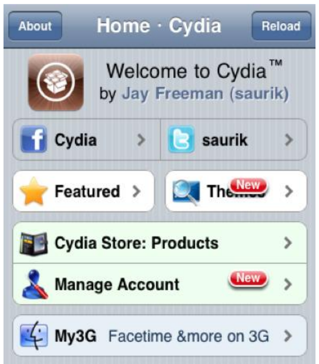


Figure 1
Cydia Store Menu

This type of modification to a smartphone can be done by security teams and hackers exploiting these devices vulnerabilities. They search for different ways to enter the system until they find this vulnerability so that they can install their desired code. Jailbreak and Rooting is known to the end user after these teams that search for this vulnerability made the exploit public and create a software so that users can do this to their device. The way for end users to do this to their device is by downloading the software created by these teams of people. For a user to be able to free their device and gain root access to install the desired modifications the user’s device would need to be on the specific mobile operating system version that is supported by the third-party software. This is needed in order for the software to use the vulnerability that is present on that mobile device version to execute the code and install for example the Cydia Store in the iPhone environment.

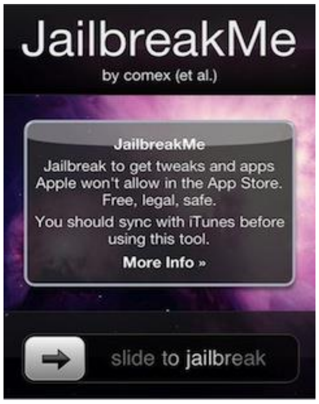
Jailbreak States

The Jailbreak have different types of states. These states are referred as what the user would need to do for the phone have the jailbreak available to them upon boot or do the process every time the user turns off the device. The states are called untethered that is that the user can boot the device, turn off and on without using any other tools. This method is what can be considered the most usable for users as the process for the smartphone be jailbroken only is done once. Tethered means that the device would need to be connected to another device such as a computer for the smartphone be able to enter the operating system for normal use. This method is what a developer may use to test applications that need these elevated privileges. It is not recommended for daily use as if the smartphone needs to reboot or it loses charge and its turned off a computer is needed, and the end user would not be able to use the device. Semi tethered state is when the device can enter the operating system after it is shut down or losses power and the operating system can be use without the ability to run tools or modifications that need the elevated privileges.

These applications to be able to be used would need the user to run the jailbreak tool again. Semi untethered would be the second in line after the untethered method as it retains the patch of the kernel when it is shut down, reboot or losses power and the user would only need to run an application that would be installed on the mobile device. This would allow to run the modifications or tweaks that the user installed using the elevated privileges. This method is a better method if a user needs to have the jailbreak before it launches with the untethered version.

Starting Method of Elevated Privileges

Gaining access to install these tools, modifications and tweaks have been done since the first version of the iPhone and Android. One of the first methods for the iPhone to have the jailbreak was that a user would visit the Safari web browser installed on the phone and visit a website called JailbreakMe. When the user visited the website, a download was done to the phone and an application was installed called installer.app.



JailbreakMe
by comex (et al.)

JailbreakMe
Jailbreak to get tweaks and apps Apple won't allow in the App Store. Free, legal, safe.
You should sync with iTunes before using this tool.

Figure 2
JailbreakMe Message on Home Screen

This application allowed the user to install third party modifications and applications to the phone. On the Android side it was a different method as the device had removable storage and it would allow the user to upload a desired file with ease. In this removable storage the user would save the file that would allow the exploit and it was run at boot. It was installed before the operating system was entered and it allowed the access. This method does not install a third-party store, the user would need to search for an APK and install it manually to have features in contrast with the jailbreak that an application was installed after the successful run of the jailbreak software or exploit.

By users doing this to their phone they open their device to any code that would try to be executed by third parties. These individuals searching to free their phones don't know the intent of the person who created a piece of software or setting. In the community there can be developers that would like to create features to these devices to help others and themselves but there can be malicious intent also taking advantage of this method of elevated privileges. Since the phone is open for modification the developer can create a code inside the desired modification that executes and performs as expected by the end users, but it can be gathering some type of user data like photos, contacts and location.

PIRACY

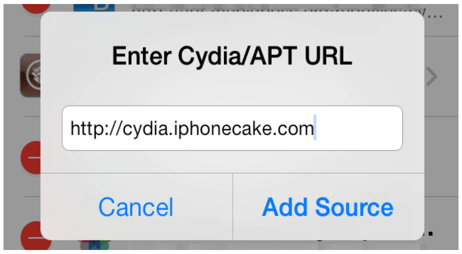
Piracy for paid applications it is found on the Cydia Store and Android users would have the opportunity to have installed a third-party store apart from the Play Store. Users can download a modified paid application to have them available for use in their application library. Some developers to combat this have their applications for free in the official applications store and would have micro transactions to have the user pay for more content, create an account so that the user can log in and use the paid features.

The user account is necessary so that it can be authenticated with the developer database because there are modifications and tools that can be found on elevated privileges stores that have tools to open the inside paid features. For example, a game is free on the application store and has gameplay for 5 levels. For levels 6 through 10 the user would need to pay the developer to have those levels unlocked. By the user having the smartphone open for modification, the user can download a tool to allow to open those levels when that tool is executed.

Micro transaction bypass is a method that can be found on the jailbreak scene, an application is available to do this and is called iAPCrazy. This application needs a Jailbroken device to be installed and to be used by the user. This application allows the user to have available for download the downloadable content and in app purchases that the developer offers inside the application. This method works if the desired application does not authenticate via a user account to verify the user purchases. This method can be installed on a device running iOS 11.1.2.

IPA is the file extension for iOS. This type of applications that can be installed on devices without jailbreak but in the case that the application is an app that has been freed for free use as a piracy method it will need the jailbreak. These files can be installed via the iTunes official software for iOS devices or via the Cydia store by installed a third-party store called AppCake. This store has a variety of applications that are available for free that are paid applications. To install AppCake on a Jailbroken device these are the steps to follow.

If the steps below are not done the AppCake application will not return results on the Cydia Store.



Enter Cydia/APT URL

http://cydia.iphonecake.com

Figure 3
Cydia Repository Input

IOS Process

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

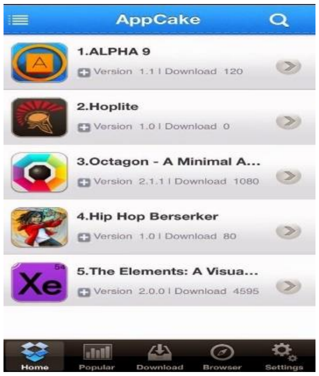

AppCake
1.ALPHA 9
Version 1.1 | Download 120
2.Hoplite
Version 1.0 | Download 0
3.Octagon - A Minimal A...
Version 2.1.1 | Download 1080
4.Hip Hop Berserker
Version 1.0 | Download 80
5.The Elements: A Visua...
Version 2.0.0 | Download 4595
Home
Popular
Download
Browser
Settings

Figure 4
AppCake Application

Android Process

- The android device will need to be root before proceeding.
- After this go to settings.
- In the Security section the checkbox for Unknown sources will need to be checked.
- Use a web browser and visit the AppCake official website.
- On the website download the APK to the smartphone.
- Using the file browser on Android go to the download folder selected for the AppCake APK file.
- Press on the APK and it will proceed to install.

Inside this store the applications for social media with extra features are available for download for example Snapchat Pro, Snapchat ++, Facebook Pro and Instagram ++. Popular games for examples Angry Birds is available for free on this store. Applications that are not permitted on the official applications store can be submitted to be available for users to download. In this category game emulators can be found. These emulators utilize the smartphone hardware to allow the user to play games from other game consoles. The emulators are available but the games for other consoles for example GameBoy, GameCube, Nintendo 64 and PlayStation 1 will need to be found by the user.

To Install

- Press the Sources tab inside the Cydia Store.
- Press Add.
- A window appears that says Enter Cydia/APT URL with the http:// already populated.
- In the field type cydia.xsellize.com.
- Click on the Add Source button.
- On the Cydia search tab enter the name of the installed repository.

This will allow to download the ROM’s to a folder on the device. The user will need to move the ROM’s to the desired emulator to be able to play the game. On the Android OS entering the files system to move files can be done easily by native methods or downloading a third-party app like X-plore File Manager and EZ File Explorer File Manager. These can be downloaded on the Play Store. On iOS the file manager is called iFile. This application is available via Cydia because it needs a Jailbroken device to be installed.

There are methods to install this on a non-jailbroken device but it needs to be on a specific operating system version for example iOS 9.1.

- Open Safari browser on your iPhone.
- Type openappmkt.com on the address bar.
- Wait for the page to load and find OpenAppMkt.
- Tap to install.
- Once installed, search for iFile and then proceed with installing the IPA file.

Social Media Apps

Social media applications can also have extra features that can be installed via these methods. These applications tend to have limits of what users can modify use and save. A social application that can be enhanced is Snapchat. The modification is called Phantom and this would allow the user to use the application without the limit of the developer allowing the user to save videos from the feed, modify the read receipts, hide certain information from other users like a certain activity and upload images and videos from the users photo and video album. This can put the user in a position to be banned if the developer of the application finds certain data that is used not like they have intended or modified. By a user allowing this type of modification to an application that has personal data and access to photos and contacts, the user may be vulnerable to an attack if a developer uploads the modification or tool with this intend as it is giving permission to that modification tool to access the user's application data.

Similar tools can be found for other social media applications. For example, a tool called Social Duplicator can allow a user to have multiple social media account clones on the same smartphone. This is done if the user has more than one social media account and would like to have access to both. What this tool does is that it clones the application so that the user can input the credentials of the other account, having two applications of the same social media.

Performance

The performance on these devices can take a hit when a Jailbreak or Root modification is done. The reason for this is that applications that are installed via these methods may not be optimized for the power saving features of the operating system. For example, an app may try to always connect to a network even though the app is meant to be use offline. This data fetch will drain the battery of the mobile device faster. Another reason for battery drain is that the tweaks that are on the Cydia store are not optimized for the latest operating system. This leads that the tweaks connect to the launch daemons. The Daemons are programs or applications that run as a background process.

Installing pirated applications that do not have the latest update would affect the performance of the user as the developer may have an updated version after the user download a pirated application. Also, the user can download the application that is available to them at that moment, this means that the version that is available for download can be versions behind the current as it takes time to open the app to be vulnerable and be exploited to be available for free.

This performance hit can be seen more clearly in mobile games. To have a playable experience the developers update the game fixing game bugs and boosting performance by optimizing the game to use the mobile device hardware. By a user having a pirated game and want to play the game, it is very likely that the performance is not the same as having the official version having the latest update.

Booting times can be extended as the bootloader need to communicate with the code that was injected with the jailbreak and root. As some jailbreak & root code is running alongside the main operating system opening an application can have a delay before this application can be used. Normally it would be a delay of seconds in contrast as some applications tend to open instantly as mobile devices utilizes flash storage and do not have moving parts.

A test was done with two identical hardware devices to verify the boot time. One device was without jailbreak and the other one did not. The jailbreak used is the Pangu exploit by the Pangu Jailbreak team. Upon boot, the non-jailbroken iPhone booted at 38.8 seconds in contrast to the jailbroken device that booted at 51.2.

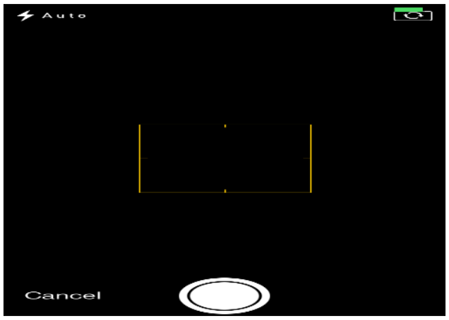
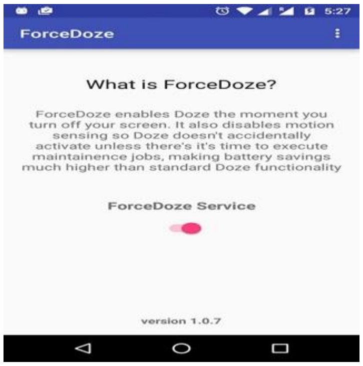


Figure 5
Camera Freeze When Opened iOS

This delay can also affect the performance when applications and processes on the device. A delay that is very noticeable is when opening the camera application on the device. This results in a mild system hang and puts on the screen a default image of the camera app user interface until the hardware is activated and it is in sync with the software. If a user tends to use the camera application frequently this delay can add up to minutes of nonuse.

A benefit of rooting a device is to force enable doze mode. This was introduced in Android 6 Marshmallow as an operating system features for some applications. This is a power optimization feature that is turned on when the device is idle but if it detects movement the device gets out of Doze Mode. By force enabling Doze Mode this feature can be activated even when the device is on movement.



What is ForceDoze?

ForceDoze enables Doze the moment you turn off your screen. It also disables motion sensing so Doze doesn't accidentally activate unless there's it's time to execute maintainence jobs, making battery savings much higher than standard Doze functionality

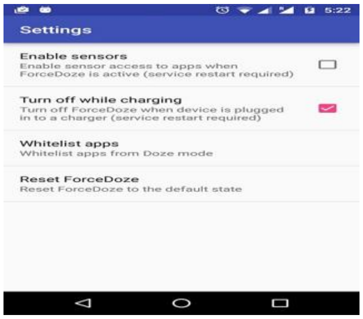
ForceDoze Service ●

version 1.0.7

Figure 6

ForceDoze Activation After Rooting Process

This mode by running modification on the command line on the android developer software client can be activated in a more aggressive manner. By activating via this method, it modifies the smartphone to turn off different hardware and stop background processes. For example, on an Android device the battery would last longer by turning off gyroscope and the GPS antenna. There is an option that these features turn on when the device screen is manually turned on by pressing the unlock button.



Settings

Enable sensors
Enable sensor access to apps when ForceDoze is active (service restart required) □

Turn off while charging
Turn off ForceDoze when device is plugged in to a charger (service restart required) ☑

Whitelist apps
Whitelist apps from Doze mode

Reset ForceDoze
Reset ForceDoze to the default state

Figure 7

ForceDoze Settings After Rooting Process

JAILBREAK VIRUS AND MALWARE

The tools that are available to the public so that they can jailbreak their devices are developed by groups of people and are not gone through the official guidelines of the phone manufacturer. This can lead the user exposed to code that can be malicious to their device or their personal computer when they execute it. When these tools are publicly available there are results of different anti-virus software from different manufactures that are run to scan the software available for download on the desired version.

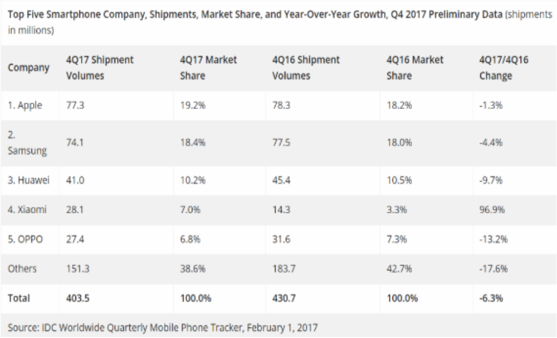
The Pangu jailbreak team did the test on jailbreak software using a list of anti-virus software and found that the jailbreak download return 100% clean of malicious code. This was done on a specific version of a jailbreak in version iOS 9. This is a safe measure that if an individual would like to proceed with the jailbreak should take into consideration. Most of today's Antivirus software comes with a free version or trial and this could be run to scan the file before proceeding [1].

SECURITY UPDATES

The security updates on mobile are the ones that can patch a possible Jailbreak and Root access, this is in the hands of the manufactures of the devices and developer of the operating systems. These teams have an initial approach to the end user security when using these devices but as users put more use on these devices and the apps get downloaded these can open some type of vulnerability. That is why we see updates on mobile devices because the initial stock operating system that comes with a new device changes when a user populates it with the user's personal data.

The users are secure from a recent bug or vulnerability as the manufacturers can create a patch or update. Therefore, seeing how frequent the devices are updated can give a better picture. To have this information we can look at the top Operating Systems IOS and Android and Mobile Phone Manufacturers Apple and Samsung as data from Gartner and TrendForce. The recent market share 2018 for Samsung Mobile is at 20.3% and Apple at 15.7% giving them the two top spots [2] [3].

The following figure shows the current top manufacturers of mobile devices in the years 2016 and 2017. An honorable mention of new manufacturers on the mobile space that are on the rise are Huawei, Xiomi and OPPO. These companies are better known on the Asian markets.



Top Five Smartphone Company, Shipments, Market Share, and Year-Over-Year Growth, Q4 2017 Preliminary Data (shipments in millions)

Company	4Q17 Shipment Volumes	4Q17 Market Share	4Q16 Shipment Volumes	4Q16 Market Share	4Q17/4Q16 Change
1. Apple	77.3	19.2%	78.3	18.2%	-1.3%
2. Samsung	74.1	18.4%	77.5	18.0%	-4.4%
3. Huawei	41.0	10.2%	45.4	10.5%	-9.7%
4. Xiaomi	28.1	7.0%	14.3	3.3%	96.9%
5. OPPO	27.4	6.8%	31.6	7.3%	-13.2%
Others	151.3	38.6%	183.7	42.7%	-17.6%
Total	**403.5**	**100.0%**	**430.7**	**100.0%**	**-6.3%**

Source: IDC Worldwide Quarterly Mobile Phone Tracker, February 1, 2017

Figure 8
Mobile Devices Market Share

The update frequency on mobile operating systems tends to be a yearly update of a big iteration. This is something that users that tend to upgrade on a yearly basis can have as a benefit and wouldn't need to update manually because the new mobile device would have the latest operating system version. In contrast not all users tend to upgrade their devices yearly therefore they can be exposed to bugs and problem of security. Manufactures when announcing a new operating system show a timeline of how back in their product line they provide support. Meaning that a new operating system that is installed out of the box on a new mobile device can be installed on a previous version in the product line.

Managing Online Store for Applications

Mobile devices are very welcome in every user life by their collection of apps that are available today. This market rose and gave the mobile platform a place that users with a specific need can go and download an application. The top platforms for mobile store for applications must take into consideration the content that they can provide to the end user because this can reflect on the stability of their image as a company. This means that the integrity of these applications must be evaluated, and certain guidelines must be followed to maintain some level of quality control in this market. IOS and Android operating systems have a store that users can download applications and have guidelines for when a developer decides to put their application.

The Google Operating System Android developer website has a Launch Checklist that a Developer can use to publish an app. The list has 20 items with links to have more information about the item of interest on that list. It is a very welcoming experience to publish an application on the Android Operating System at first sight. The first item is what shows the Developer Program Policies. In here is what mentions the topics about privacy, security, intellectual property, spam, restricted content, enforcement, monetization, updates, store listing and promotion. [4]

The Apple Operating System IOS developer website has the App Store Review Guidelines. These guidelines have 5 main topics: Safety, Performance, Business, Design and Legal. Each of these categories have multiple sub categories that go into detail into each of them. In these categories the Legal section is what holds the Privacy and user security [5].

Both Operating Systems have in their guidelines that developers have in mind the security of the user. A difference that can be mentioned about the two is that for the Android Marketplace the process does not require a developer paid method in contrast as Apple that requires a developer subscription of $99.

A store for mobile applications should have guidelines for developers to upload applications so that the experience for the end user can be a better representation of them as a company. Having a filter can help in the long run in the security side of the experience because an app that didn't go through this can have for example a keylogger and the user not knowing is there.

Having to move to new architectures in smartphones these stores have required the developer to move to the most recent one. Apple in 2015 decided to move its mobile applications to 64bit architecture. Having plans to not support 32bit completely. In its most recent iOS update 11 don't support 32bit applications. The Androids operating system will require developers by 2019 to have a 64bit version of the application apart from its 32bit version.

This is a move that if a developer wants to be present in this market must make. This move can work as a filter for older apps that some developers did not go through the update in Apples scenario. By removing this non-updated application can help because these applications can have a security vulnerability that an intruder could exploit by knowing that the developer is not going to update that application. This can be known by looking at the log of updates of the desired application.

This also applies to when Android developers make the move to the 64bit architecture. Applications will require this architecture but by also keeping their 32bit version can help in the group of users in the long run. In this case a user with a mobile device that does not support 64bit applications can also run this application in the 32bit version. In contrast with Apple that a user will need to have a new mobile device if the user's application is not supported on the user's device. Both decisions benefit the user because these companies will require the updates from the developers.

In Apple ecosystem devices that are capable of new updates by being 64bit architecture are 11 in total going back to September 20, 2013. Having 5 years in the product line covering 11 iterations of their mobile device is a good number to have the support. This means that the latest operating system updates (currently iOS 11 2018) can be installed on the iPhone 5s that was release on September 20, 2013. This support is official from Apple system update feature. Android devices from around that date April 2013 is the Samsung Galaxy S4 taking into consideration the Samsung brand as the most popular by market share. This device was release with Android 4.2.2 and had official support to 5.0.1. This means that the device had support until two new major operating system releases.

COMPANY POLICY, WARRANTY ON JAILBREAK DEVICES

Apple has on their official support website a description on what they see are the disadvantages on user experience and security when the user Jailbreak their device. The wording they have on this website apart from other information is the following "Apple strongly cautions against installing any software that hacks iOS. It is also important to note that unauthorized modification of iOS is a violation of the iOS end-user software license agreement and because of this, Apple may deny service for an iPhone, iPad, or iPod touch that has installed any unauthorized software." [6]

Magnuson moss warranty act it was passed by congress 1975 says the following "a warrantor cannot, as a matter of law, avoid liability under a written warranty where a defect is unrelated to the use by a consumer of 'unauthorized' articles or service." This means that for a company to not provide the user support for a device that is Jailbroken needs to be justified and linked that the Jailbreak is the reason of the device malfunction. This can vary by the people and group that will be working on the device in question for repair in how they see the wording or a store policy not related to the manufacturer such as a third-party store for repairs [7].

ADOPTION RATE OF UPDATES

The adoption rate on mobile device smartphones is important so that users can have an up to date security patches on their devices and the latest features of the operating system. Users should get a notification on their screen that shows the update available to them. This action will be on the hands of the end user as these devices do not force update to the next release. This action is a reason that a user with a device capable of being updated does not have the new update on their mobile device. A reason that a user does not update can be that the update is of a large file size and it is currently on carrier data and is not allowed and later clears the notification.

Looking at the latest operating system on today's popular mobile devices these are Android Oreo 8.0 and iOS 11. Android Oreo adoption rate is at 5.7% adding versions 8.0 and 8.1. iOS 11 adoption rate is 76%. This adoption rate is by all active devices using Android and iOS as their operating systems. This rate is important as users with devices that are not allowed to be updated to the latest operating system will be missing the new security features and usability. In the side of Android users can opt to install a new version via a ROM. This is a modified version of the latest operating system to be able to run on the desired device. These ROM's are open source and, in the case, that a malicious software would be on the code this would be noticed by the community [8] [9] [10].

This does not mean that it will be 100% secure as the malicious code can be in some way hidden and later found out meaning that several users would be affected. This method would be use by people that know how to do this or pay a third party. This method can cause what is called a "bricked phone" when flashing the device to the desired ROM and would not allow operation of the device. On iOS custom ROM's by the community are not available as the code for iOS is not open source. There has been custom ROM's for iOS but are inclined by the Jailbreak community with the application store Cydia with applications that do not go through the Apple Store developer guidelines. This means that a user with a device that the latest operating system does not support wouldn't have the opportunity to flash a ROM to update.

Security features that users on Android Oreo can use: Users can sideload apps with settings that can filter from where the application is being installed from apart from allowing installation from every source. This is an important feature as Android users have the ability to install applications that are not part of the Android Marketplace. In contrast with the Android version 4.4 that the Samsung S4 comes pre-installed, Oreo 8.0 has a second version of its verified boot. It introduced this feature in 4.4 but it was discovered that an intruder could downgrade the smartphone and bypass this protection. In the new version on Android 8.0 it prevents the user to downgrade to a version that is known to be affected by a known vulnerability.

A feature that will be most commonly use would be the protection on public Wi-Fi. This is important as users connect to public Wi-Fi daily. This would help into connecting to a wireless internet connection and setup a VPN. A feature like this built into the initial setup when connecting to a network and be intuitive would help a bigger number of users be protected by a VPN. In most cases these users wouldn't have the knowledge of ever setting up a VPN or knowing what a VPN does.

Password manager for multiple accounts is a feature that is embedded on the iOS operating system. This helps users into managing their online password by suggesting different passwords for each account. This feature produces different password with a level of complexity that helps by eliminating a password that can be attached to a user by doing social engineering. The user can enter this Password Manager by using the same credentials as their Apple ID. This has been updated so that users can use their fingerprint and their face as a method of authentication. Different password managers have been available to these mobile platforms but by offering this feature on their operating system more users can see the benefit and can start looking for what they are and try other offerings with different features.

Known Vulnerabilities

Both Android and Apple operating system for their mobile platform provide documentation of the security updates that they have worked on. This information is very valuable for the end user that wants to know the state of their mobile platform in the security area. This would also help developers that can add a certain feature to their applications that by the documentation of a recent security update they can implement it on their next application or update to their existing one.

The documentation is presented via most recent updates on the timeline. In this timeline both operating system documentation presents the version that the update was implemented with a hyperlink to a more detailed view of these updates. Each vulnerability that is mentioned has a description with a reference number to the nvd.nist.gov website that is the National Vulnerability Database. This website created in 2000 holds the information of common vulnerabilities and exposures that have been published. Quote from the website nvd.nist.gov regarding the organizations involved "The NVD is a product of the NIST Computer Security Division, Information Technology Laboratory and is sponsored by the Department of Homeland Security's National Cyber Security Division."

A vulnerability is presented with several categories within the page. The vulnerability can be search by a CVE Dictionary Entry. This entry can be found on the security sections on the timeline of the companies like Apple and Google regarding their security update. By looking this entry on the database, it presents the following categories: Tittle, Current Description, Source, Description Last Modified, Impact, References to Advisories, Solutions and tools, Technical Details, Vulnerable Software and Versions [11] [12].

Vulnerability Bounty Programs

These programs officially named Bug Reporting are ways that the manufacturers reach out to the community of hackers and researches by compensating them when the find bugs on the operating system. This can lead to prevent a future Jailbreak as the person who would publish the bug can report the bug directly to Apple and get compensated. The bounty program payout is as follows:

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 9

Bounty Program Pay Different Categories

SUMMARY

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.

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.

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 an 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.

CONCLUSION

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. Users of mobile devices do not have to give up their mobile security for features to make their daily lives easy because the manufacturer has not implemented the feature out of the box. In the other side of the problem, users should be mindful of the procedures they open their device.

REFERENCES

[1] F. Ortega. (2016, Mar 30). *Pangu Jailbreak has tested clean of viruses and malware* [Online]. Available: https://pangu-jailbreak.en.lo4d.com/virus-malware-tests.

[2] A. A. Forni. (August 19, 2016). *Five of Top 10 Worldwide Mobile Phone Vendors Increased Sales in Second Quarter of 2016* [Online]. Available: https://www.gartner.com/newsroom/id/3415117.

[3] Trendforce. (2018, February 13). *Annual Growth of Global Smartphone Market Will Shrink to 2.8%, Vendors Are Faced with New Round of Competition* [Online]. Available: https://press.trendforce.com/node/view/3067.html.

[4] Google Developers. (April 22, 2018). *Launch checklist* [Online]. Available: https://developer.android.com/distribute/best-practices/launch/launch-checklist#top_of_page.

[5] Apple Developers. (May 4, 2018). *App Store Review Guidelines* [Online]. Available: https://developer.apple.com/app-store/review/guidelines/.

[6] Apple Developers. (April 15, 2018). *Unauthorized modification of iOS can cause vulnerabilities, instability, shortened battery life, and other issues* [Online]. Available: https://support.apple.com/en-us/HT201954.

[7] Reese, Poyfair, Richards, PLLC. (1975). *Understanding the Magnuson-Moss Warranty Act* [Online]. Available: https://www.mlmlaw.com/library/guides/ftc/warranties/undermag.htm.

[8] eMarketer Writer. (2015, January 19). *How Often Do Mobile Users Upgrade Their Devices* [Online]. Available: https://www.emarketer.com/Article/How-Often-Do-Mobile-Users-Upgrade-Their-Devices/1011839.

[9] You Mobile Writer. (2018, April 25). *Samsung Smartphone Updates* [Online]. Available: http://samsung.youmobile.org/.

[10] S. Costello. (2018, February 11). *Compare every iPhone Model Ever Made* [Online]. Available: https://www.lifewire.com/compare-iphone-models-1999430.

[11] Apple Developer. (2018, January 23). *About the security contents of iOS* [Online]. Available: https://support.apple.com/en-us/HT208463.

[12] National Institute of Standards and Technology (NIST), U.S. Department of Commerce. (2000). *National Vulnerability Database* [Online]. Available: https://nvd.nist.gov/.