Jeremiah Everett
ICTN 4040
Enterprise Information Security

Mrs. Constance Boahn
Dr. Phil Lunsford
April 5th 2016

Android and iOS Security

This paper will discuss security for the Android OS and Apple's iOS. So for a little background we will look at when Android and iOS were first released. Android was released to the public on the HTC Dream in October of 2008, and Apple's iOS came out in March of 2008. Since the time of release more and more malware has been created and need for better security has been realized. In the article Android Security: A Survey of Issues, Malware Penetration, and Defenses, they state that increased popularity of the Android device and associated monetary benefits attracted malware developers, and this resulted in a big rise of Android malware apps between 2010 and 2014.

Now we will look at what is currently being offered. Android currently has it's latest version of Marshmallow 6.0.1 which has just come out as of April 5th 2016. And Apple's iOS currently has 9.3.1 which was released March 31st 2016. One of the main features for Android security is SELinux (Security-Enhanced Linux). This means that the security model for Android is based on application sandboxes. Which is that each application runs in its own sandbox. SELinux moves from DAC (Discretionary Access Control) to MAC (Mandatory Access Control). This is set to enforce an administrator set security policy. This set policy takes away user defined Access Control. It is also set by

a Linux kernel security module. SELinux is based upon the principle of least privilege model and is used by the United States Department of Defense. SELinux started to be used in version 4.3 of android and was called a permissive release. It then moved forward in and was considered partial enforcement in 4.4. As of 5.0 it had moved to full enforcement of SELinux. Here is a diagram showing Android's security architecture taken from Android Security: A Survey of Issues, Malware Penetration, and Defenses.

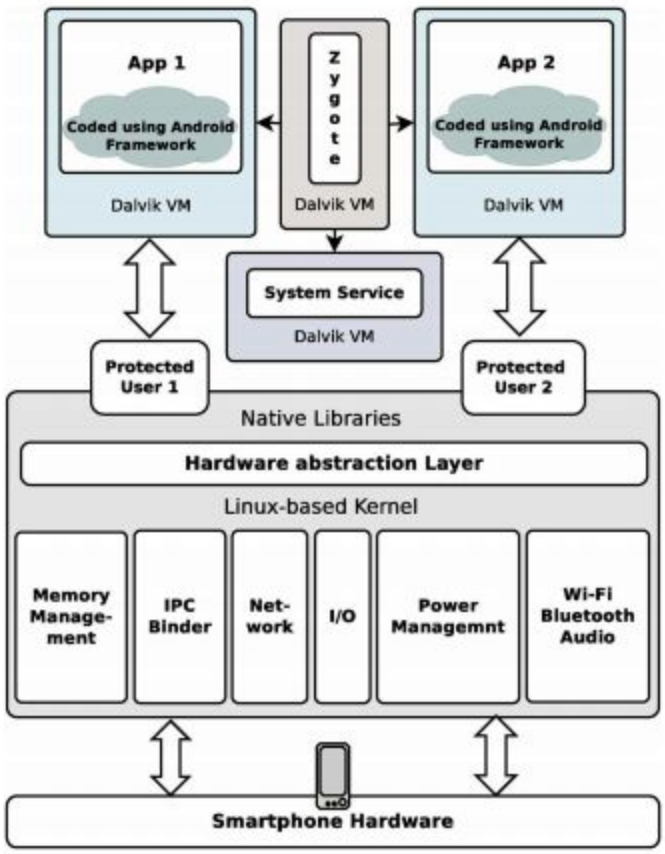
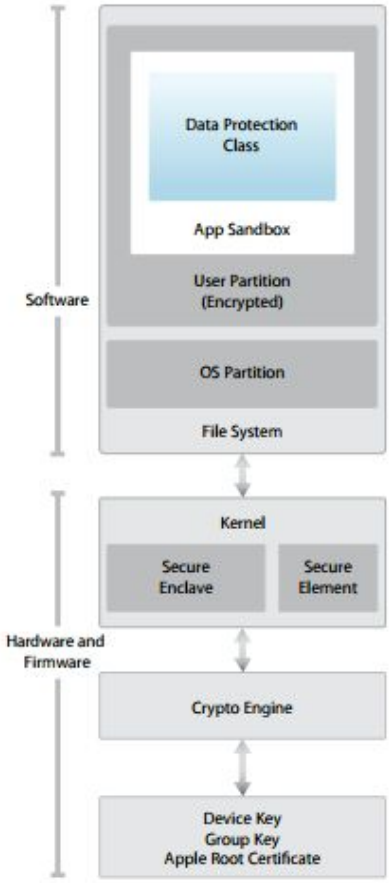


Fig. 1. Android Architecture [34].

Apple is now currently offering the iPhone 6, 6 Plus, 6S, 6S Plus, and now the SE (Special Edition). The latest which is the SE version was released for sale on March 21st of 2016, but was not available until the March 31st of 2016. As mentioned before the latest version for these phones is 9.3.1 which was also released on March 31st of

2016. What wasn't mentioned is the fact that this latest version was released to fix a problem with the previous release of version 9.3. Version 9.3 was known to cause apps to become unresponsive after opening links in Safari or other apps. Now as for apps running in iOS, these must be downloaded from the apple app store. The information I was able to find on Apple comes mainly from the white paper released by Apple in September of 2015, titled iOS Security. It also states that all the 3rd party applications are run in sandboxes. Below is a diagram of the security architecture straight from Apple's iOS security guide.



Security architecture diagram of iOS provides a visual overview of the different technologies discussed in this document.

Next we will cover some best practices for cell phone security. One of the easiest and most important best practice is having your phone lock itself and having a password to unlock it. This feature can be enabled or disabled on both Android and iOS. Fitting right with this is the next best practice of keeping your device on you. This means not leaving it out of your possession, or even in a locker that is not locked. Another best practice is having an anti-malware app installed on your mobile device. This is because more and more malware threats have been being created and they are targeting mobile devices.

Android and especially Apple's iOS have been in the news. Apple's iOS has specifically been in the news because of the security encryption that it has protecting the phone's data. On February 16th of 2016 a federal judge ordered that Apple help FBI agents to unlock an iPhone owned by Syed Rizwan Farook. Syed Rizwan Farook along with his wife Tashfeen Malik are the suspects in the San Bernardino terror attack. The terror attack was on a holiday party of about 80 people. The shooters mentioned above used semiautomatic rifles and pistols. The shooters walked in and fired at the crowd killing 14 and wounding at least 21 others. The shooters were later killed in their SUV as they were having another shoot out with police.

When all this occurred on December 2nd of 2015 the couple went back to their home and destroyed two cell phones and removed the hard drive from their computer. Despite this the authorities recovered an Apple iPhone. Needing more information on this couple the FBI wanted access to the iPhone. Apple was then giving the order to assist the FBI to access the data on iPhone. One of the main reasons the FBI wanted

assistance is due to the fact that an iPhone will erase itself after 10 failed password attempts. As we all heard Apple refused to assist and claimed that it would be wrong and only create a vulnerability to their product. First I'd like to show that Apple didn't say it was impossible to help, they just refused to help. So being that it is possible to gain access to this data I was surprised that the FBI even asked for help in the first place. I find it hard to believe that the FBI does not have the resources on their own to gain access to the device's data. I think that the court order was done just to set precedence so that they could order gain access to any iPhone they wished to use as evidence. As of March 29th of 2016 the FBI had found a 3rd party which was able to allow them to have access the iPhone. Reports state that iPhone that was being used was the iPhone 5c. The FBI has now asked for the court order asking for Apple's help to be vacated. This has proven to be a victory and a loss for Apple, as it won in court being that it didn't have to assist the FBI. But it lost in reputation that its iPhone's were secure and unable to be hacked or broken into. I wish I could report on how the FBI was able to unlock the iPhone 5c and get at the data but so far I have not found that information. Apple also wants to know how it was done so that they can patch this vulnerability. What I did find is that in a report from CNNMoney by Jose Pagliery, it states "The Obama administration adopted a little-known cybersecurity rule in 2010 called the "vulnerabilities equities process." The rule kicks in when the government discovers a powerful, never-before-seen hack. Some of the government's top technical minds at the NSA, Secret Service and other agencies must meet with the president's National Security Council to discuss whether or not to share flaws so they can be fixed."

This means that because of a rule that the government created itself, it may have to explain to apple what the vulnerability is and how the hack was performed. Honestly I cannot see the FBI now wanting to help Apple in anyway since Apple itself didn't want to help the FBI. Another reason the FBI wouldn't want this vulnerability to be patched is because they also may want to use it again and again. This will not be the last time they find a criminal with an iPhone.

Do you think that the US Government has treated Google's Android any differently? Let's find out. According to an article from The Verge by Russell Brandom there have been 9 cases that asked Google for help with Android phones. The article states "New research from the American Civil Liberties Union shows 63 different cases in which the government compelled help from Apple or Google in unlocking a handset. It's unclear how many of the orders were filled, although companies often complied with such orders where possible before last year. The bulk of the cases target Apple, but nine of the orders also look to compel Google's help, typically to reset the password on a given device."

It appears as though Google has been helping in these cases where possible. Google does say in the article that "We carefully scrutinize subpoenas and court orders to make sure they meet both the letter and spirit of the law,"..."However, we've never received an All Writs Act order like the one Apple recently fought that demands we build new tools that actively compromise our products' security. As our amicus shows, we would strongly object to such an order."

Overall we can see that cell phone security is not perfect, and even the laws that govern cell phone security are not perfectly black and white. These issues are things that both software development companies, and governments both need to grapple with in the coming years as they strive towards fair, equitable, and safer systems going forward.

References

Faruki, Parvez, Ammar Bharmal, Vijay Laxmi, Vijay Ganmoor, Manoj Singh Gaur, Mauro Conti, and Muttukrishnan Rajarajan. "Android Security: A Survey of Issues, Malware Penetration, and Defenses." *Android Security: A Survey of Issues, Malware Penetration, and Defenses* 17.2 (2015): 998-1022. Web. 5 Apr. 2016. * <http://ieeexplore.ieee.org.jproxy.lib.ecu.edu/stamp/stamp.jsp?tp=&arnumber=6999911&tag=1>.

Enck, William, Machigar Ongtang, and Patrick McDaniel. "Understanding Android Security." *IEEE Security & Privacy* January/February (2009): 50-57. Web. 5 Mar. 2016. * <http://ieeexplore.ieee.org.jproxy.lib.ecu.edu/stamp/stamp.jsp?tp=&arnumber=4768655&tag=1>.

BIERSDORFER, J. D. "Keeping Up With Android Security Patches." *Keeping Up With Android Security Patches*. The New York Times, 2016. Web. 05 Apr. 2016. <http://www.nytimes.com/2016/03/23/technology/personaltech/keeping-up-with-android-security-patches.html?partner=bloomberg>.

Jones, Michelle. "ValueWalk: Apple Inc. IOS Security Bashed By Researcher." *Newstex Global Business Blogs*. Newstex, 21 July 2014. Web. 5 Apr. 2016. <http://search.proquest.com.jproxy.lib.ecu.edu/docview/1641766227/citation/96BE1A8B83294A30PQ/1?accountid=10639>.

Mohamed, Ibtisam, and Dhiren Patel. "Android vs. IOS Security: A Comparative Study." *Information Technology - New Generations (ITNG)* 12 (2015): 725-30. Web. 5 Apr. 2016. <http://ieeexplore.ieee.org.jproxy.lib.ecu.edu/xpls/icp.jsp?arnumber=7113562>.

"Security-Enhanced Linux in Android." *Security-Enhanced Linux in Android*. Web. 05 Apr. 2016. <http://source.android.com/security/selinux/index.html>.

"IOS Security." *IOS Security*. Apple, Sept. 2015. Web. 5 Apr. 2016. <https://www.apple.com/business/docs/iOS_Security_Guide.pdf>.

ANDRUSEWICZ, MARIE. "Apple Opposes Judge's Order To Help FBI Unlock San Bernardino Shooter's Phone." *NPR*. NPR, 17 Feb. 2016. Web. 05 Apr. 2016. <http://www.npr.org/sections/thetwo-way/2016/02/17/467035863/judge-orders-apple-to-help-investigators-unlock-california-shooters-phone>.

Johnson, Kevin, Jon Swartz, and Marco Della Cava. "FBI Hacks into Terrorist's IPhone without Apple." *FBI Hacks into Terrorist's IPhone without Apple*. USA TODAY, 29 Mar. 2016. Web. 05 Apr. 2016. <http://www.usatoday.com/story/news/nation/2016/03/28/apple-justice-department-faroo k/82354040/>.

Pagliery, Jose. "There's a Slim Chance the FBI Will Have to Tell Apple How It'll Break into Terrorist's IPhone." *CNNMoney*. Cable News Network, 24 Mar. 2016. Web. 05 Apr. 2016. <http://money.cnn.com/2016/03/24/technology/apple-fbi-vulnerability-iphone/>.

Brandom, Russell. "Feds Ordered Google's Help Unlocking Nine Android Phones since 2012." *The Verge*. 30 Mar. 2016. Web. 05 Apr. 2016. <http://www.theverge.com/2016/3/30/11330892/fbi-google-android-unlocking-phone-cou rt-order>.