Apple iOS Security

Tyler Jeffords

East Carolina University

Abstract

As we all know mobile security is on the rise and with around two hundred seventy five million iPhones sold since 2007 Apple iOS security has a lot to live up to (Global Apple iPhone sales, 2013). Can iOS security compete with other mobile operating systems out there? Well today I will be discussing the strengths and weaknesses of Apple iOS and how it matches up with other mobile operating systems on the market. Did you know iOS was originally known as iPhone OS but leased the name iOS from Cisco in 2010 before the release of the iPad. I mean come on you can't have an iPad running iPhone OS. My research comes from a wide variety of places such as discussion forums, magazines, websites, textbooks and Apples Guide to iOS Security. Though my research I have learned about the system architecture, encryption, data protection, and access security on the device. I have come to a conclusion that iOS security can not only compete in the today's market but it is the top dog. Apple has spent a numerous amount of hours developing its security boot chain and ensuring that all applications remain safe for its customers.

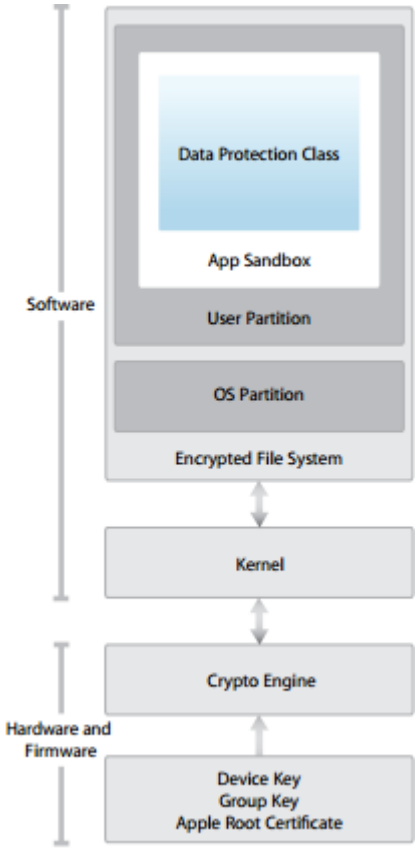
Apple iOS Security

Being an Information & Computer Technology major and owning an iPhone for over three years now I have always been interested in Apple's iOS security. The latest version of iOS is 6.1.3. For the past few months I have been researching the security platform and techniques used by Apple to make their devices less susceptible to malware and other harmful viruses. With Apple owning around 30 percent of the world's smartphone market today, its security must stand out to remain competing in the smartphone and tablet market (Tero Kuittinen, 2013). Information security is a vital decision when purchasing a mobile device, no one wants a device that they do not feel their personal information, photos and other valuable data are not protected. I will go over what steps Apple takes to ensure that their costumer's device and information remains safe, the systems architecture, and the encryption method.

Unlike other mobile operating systems in order to create an application and make it available to the public you must register and join Apples developer team. This ensures that all applications come from a known source and are verified before entering the app store. After apps are approved they receive an Apple issued certificate (also known as app code signing) which allows the app to run the iOS kernel on certified Apple devices (iOS Security, 2012). This helps prevent the creation and distribution of malicious software such as malware, spyware and other viruses from entering the app store which consists of more than 800,000 apps (Apple updates iOS to 6.1, 2013). Apple also provides advanced device access security using time delays after

invalid passcodes are entered and an option of completely wiping the memory after ten failed attempts to access the device. A great security advantage that iOS devices have is the ability to locate, lock and wipe your device from anywhere using the Lost my iPhone application. One downside to Apples device access is that you can only either have a four digit pin or a fifty or under character alphanumerical passcode. Other competing devices offer facial recognition, picture identification and other creative ways of unlocking their device. Rumors have it that the next generation iPhone will be equipped with a fingerprint scanner which will make it the first phone to do so.

To understand Apples security you must understand the systems architecture. I have provided a security architecture diagram for a better understanding of the different technologies used by Apple. There are many layers of validation upon booting an apple device and opening applications. Apple iOS uses what they call secure boot chain to help validate and secure the software of their devices. The initial step upon start up is running the Boot ROM code to verify the CA public key which verifies that the Low-level Bootloader is signed by Apple which allows the device to enter the next process known as iBoot. This is stage 2 of the systems bootloader, it verifies that the software has not been changed or tampered with allowing the device to run the iOS kernel (iOS Security, 2012). iOS is only compatible with Apple devices. If you were to put iOS onto a non-Apple product it would fail at stage one of the bootloader.

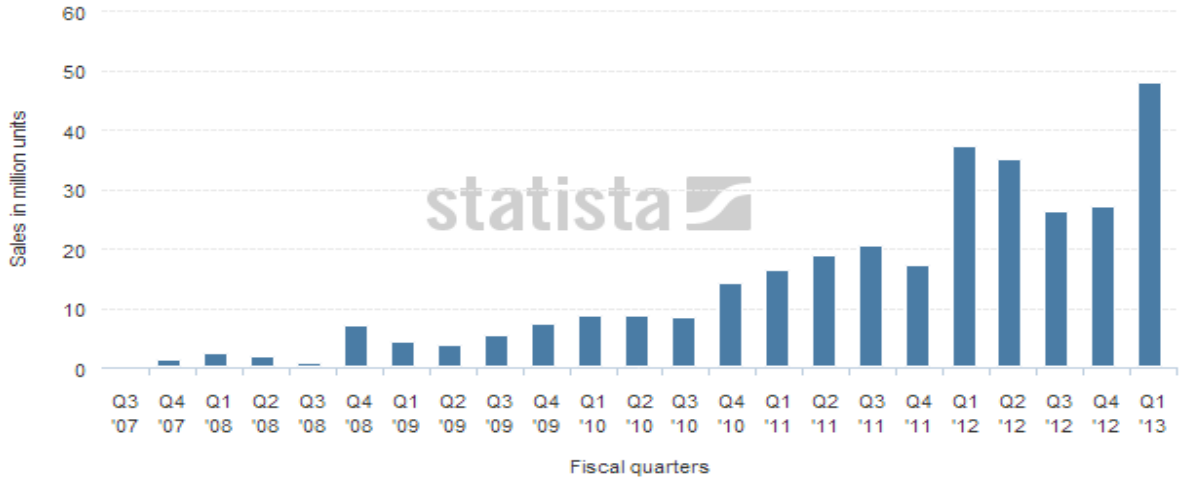


iOS is equipped with a strong encryption algorithm using Advanced Encryption

Standard 256-bit which is one of the top encryption methods used by the U.S government. Each Apple device also contains a unique ID a group ID which is encrypted by AES 256. The unique ID is different on each device and allows the memory to be cryptographically tied to that specific device (iOS Security, 2012). This is a great security measure to ensure all of your personal data is safe even if the memory is taken out of your device and put into another apple device it will not allow that device to recognize that part if the UID's do not match up. The group ID is an ID assigned to the device's processer. For example all iPhone 5's come with an A6 processor so all iPhone 5's will have the same GID. I find this more of a disadvantage then an advantage since it is not a useful security method since all generations have the same GID. It is a disadvantage because this mean you cannot upgrade the processor in your Apple device instead you are forced to purchase the newest generation of that device.

Apple truly goes above and beyond when it comes to securing their devices and protecting their brand name. They continue to innovate and have helped pave the way for smartphones and tablets. As you can see in the chart below Apple is continuing to sell more phones each and every year. As of January 28, 2013 iOS users have uploaded over nine billion photos to Photo Stream, sent over 450 billion iMessages and received over four trillion notifications (Apple updates iOS to 6.1, 2013).

Global Apple iPhone sales from 3rd quarter 2007 to 1st quarter 2013 (in million units)



i Worldwide; Apple

Source: Apple

Global Apple iPhone Sales Q3 2007 – Q1 2013. (2013). [Graph illustration of Apple iPhone sold from Q3 2007 – Q1 2013]. Worldwide Apple iPhone sales by Statista and Apple. Retrieved from http://www.statista.com/statistics/12743/worldwide-apple-iphone-sales-since-3rd-quarter-2007/

*iOS Secuirty. (October 2012). [Technical Proceeding]. Retrieved from http://images.apple.com/iphone/business/docs/iOS_Security_Oct12.pdf

Tero Kuittinen. (March 15, 2013). iPhone Again Shows Surprising Market Share Growth in February. Retrieved from http://bgr.com/2013/03/15/smartphone-market-share-february-2013-380124/

Apple updates iOS to 6.1. (2013, Jan 28). *Business Wire*. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1286674323?accountid=10639

Lemos, R. (2011). Apple iOS: Why it's the most secure OS, period. *InfoWorld.Com,* , n/a. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/870404743?accountid=10639