**Introduction to Computer Network EA2 Android vs iOS**

team：14

team member：許心慈(b06502051,機械三),鐘民憲(b06901017,電機三)

**1. Introduction**

An operating system is the heart of smartphones, since it determines features, performances, security, and availability of applications (Lin and Ye 2009). The two most dominant mobile operating systems are Android and iOS currently. They respectively account for 87% and 13% of market share.

Obviously, Google and Apple have different strategies and policies in development of their mobile OS such as open-source or closed-source, customized or standardized, but due to the page limitation, we will mainly compare two operating systems on two topics : security, and apps.

**2. Comparison of Security in Mobile OS**

In this part we mainly take reference to “Comparison between android and iOS Operating System in terms of security”. However, this paper was published in 2013, 6 years out of date, so we did further research on the topic and updated some information. The security requirements for mobile operating systems(MOS) are partly listed below as: Application Sandboxing, Encryption, and Built-in Antivirus. We would explain them in detail:

**．Application** **sandboxing** improves security by limiting the application's accessibility to the OS in order to prevent outside malware, intruders or other applications.

Android assigns a unique user ID to each application and each application has its own sandbox directory. Therefore, they won't affect each other. In addition, users need to set the permissions of different applications individually. For iOS, the majority of program runs as the non-privileged user (mobile), so as all third-party apps. Besides, the entire OS partition is set to be read-only. And APIs don’t allow apps to upgrade their own privileges to modify other apps or iOS itself.

**．Encryption**

Android has two device encryption methods: file-based encryption and full-disk encryption. File-based encryption allows different files to be encrypted with different keys that can be unlocked independently. As for full-disk encryption, it uses a single key to protect the whole user data in device. As to iOS, every iOS device has a built-in AES-256 crypto engine, making file encryption highly efficient. In addition, Apple uses a technology called *Data Protection* to further protect data stored in flash memory. Data Protection enables a high level of encryption for user data. Key system apps, such as Messages, Mail, Calendar use Data Protection by default.

**．Built-in Antivirus**

For Android, the apps downloaded from outside web source beside Google Play is risky, so extra antivirus needs to be installed to avoid popular malware. By comparison, Apple does not need antivirus program because the only place to get apps download is from the Apps store and checking is done in the Apps store.

**3. Comparison of Apps between Android and iOS**

Nowadays, the number of apps available for Android is approximately 3.5 millions, while for iOS it’s 2.5 millions. Although there are more free Android apps and greater variety, it is undeniable that Apple has the better quality apps, especially games, because only apps qualified by Apple company can be published in App Store. Moreover, the developers must pay a $99 yearly fee for access to Apple's Developer Program. Therefore, Apple is better at weeding out questionable apps than Android.

On the other hands, though the quality of apps in Google Play might not be as uniform as App Store, it is more friendly to program developers. Since Google published the source code for Android through "Android Open Source Project", lots of enthusiasts are able to program and distribute their own apps or even modified versions of operating system. Furthermore, programmers can develop Android applications on any operating systems. The apps can be written in Kotlin, Java and C++ using Android Software Development Kit(SDK). In comparison, the iOS SDK is not available for non-Mac PCs. By the way, the officially supported programming languages of iOS apps are Swift and Objective-C.

**4. Review & Discussion**

When we looked up more information, we were surprised to know that encryption is a new security method introduced in Android and iOS just in 2013. Also, the first encryption technique for Android was released in “Ice Cream Sandwich 4.0”(seems tasty). Perhaps, mobile phones then were just mainly used for communications, yet technology of mobile phones change over time. They’ve become big part of people’s life nowadays. People use smartphones not only to communicate with others, but browse the Internet, play games, or navigate roads by GPS, etc. Most people can't live without their smartphone and rely on their mobile devices to store their sensitive information, so it’s important to have a secure OS.

Beside the secure OS, safety and high quality applications also play a crucial role in smartphone usage. iOS provides more trustable apps because of strict censorship. Nonetheless, Android is more friendly to app developers since it’s open-source and the environments for app developments are not restrict to iOS.

Another interesting thing is that we found another paper[4] says that the network behavior of the devices(categorized into iOS, android and Windows) are in different ways. They make use of passively captured TCP/IP network traffic and ICMP packets to actively force mobile devices to exhibit characteristic network response delays. We think this topic is close to this class, but due to page-limitation, so we just present it briefly in this part for supplementary.

**5.Reference**

[1] Comparison between android and iOS Operating System in terms of security

<https://ieeexplore.ieee.org/abstract/document/6637558>

[2] iOS Security iOS 12.3 May 2019

<https://www.apple.com/business/docs/site/iOS_Security_Guide.pdf>

[3] Android Open Source Project

<https://source.android.com/>

[4] Using network traffic to verify mobile device forensic artifacts

<https://ieeexplore.ieee.org/abstract/document/7983091>