ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 7, October 2015

Comparative Study on Security Issues in Mobile Platforms

C G Thomas[1], Poojitha A[2]

Assistant Professor, Dept. of Computer Applications, AIMIT, St. Aloysius College (Autonomous), Mangalore, Karnataka, India [1]

III Semester M.Sc (Software Technology), AIMIT, St. Aloysius College (Autonomous), Mangalore, Karnataka, India[2]

ABSTRACT: The main purpose of this study is to discuss the different comparative studies on security issues in mobile operating system. From the past few years with the use of mobile, the mobile technology is also increasing at a fast speed. At presentdifferent mobile phone companies are competing in the market each having its own hardware and software. Each mobile phone company has its own interface and they are working to provide new features to their customers. Each company uses different operating systems like, Apple using iOS, Samsung using Android and Microsoft using Windows. In this paper we attempt to perform a comparative study on security issues in mobile platforms done by different authors.

KEYWORDS: iOS,Android, Windows.

I. INTRODUCTION

Mobile technology includes all forms of portable technology like laptops, palmtops, cell phones, personaldigital assistants, wireless card payment terminals, global positioning systems. Mobile security is the protection of smart phones, tablets and other portable computing devices, and the networks they are connected to, from threats and vulnerabilities associated with wireless computing. Mobile security is also known as the wireless security. Securing mobile devices has become increasingly important in the recent years as the number of the devices in operation and the uses to which they are put have expanded significantly. The problem is compounded within the enterprise as the ongoing trend toward IT is resulting in more employee-owned devices connecting to the corporate networks.

II. ANDROID

Android OS is designed on the basis of Linux kernel, which provides advanced computer processing. It is developed by Google Inc .This technology is based on java software, which requires Software Development Kit (SDK) to create applications. The SDK is open source software and Google releases the code under the Apache License which can be easily downloaded from the internet. An android application uses advanced hardware and software, as well as local and served data, exposed through the platform to bring innovation and value to consumers. To protect that value from third person, the platform must offer an application environment that ensures the security of users, data, applications, the device, and the network.

Security Model:

Android is an application execution platform for smart phones comprised out of an operating system, core libraries, development framework and basic applications. Basedon the Linux kernel Android operating system as built. The Linux kernel is responsible for executing core system services such as: memory access, process management, access to physical devices through drivers, network management and security. At top the Linux kernel is the Dalvik Virtual Machine along with basic system libraries. The Dalvik Virtual Machine is a register based execution engine used to run Android applications.

In order to access lower level system services, the Android provides an API through afore mentioned C/C++ system libraries. Along with the basic system libraries, the development framework provides access the top level services, like content providers, location manager or telephony manager. This means that it is possible to develop

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 7, October 2015

applications which use the same system resources as the basic set of applications, like built-in web browser or mail client. However, such a rich development framework presents security issues since it is necessary to prevent applications from stealing private data, maliciously disrupting other applications or the operating system itself. In order to address the security issues, the Android platform implements a permission based security model, as demonstrated in Figure1.

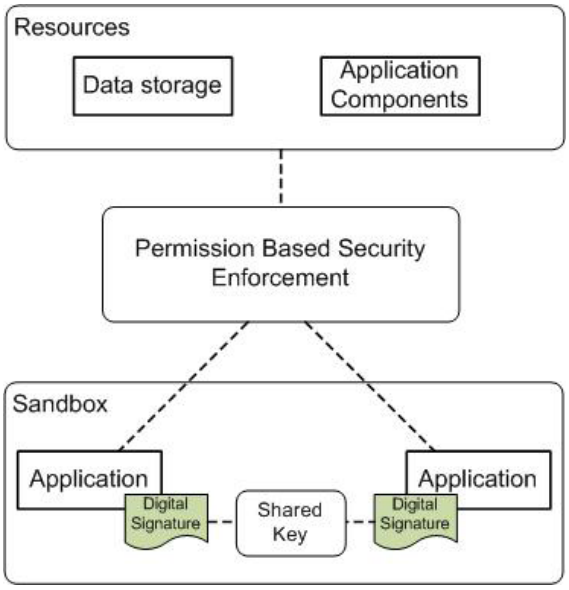

Figure 1. Android Security Model

III. iOS

iOS (originally **iPhone OS**) is a mobile operating system created and developed by Apple Inc. and it is distributed only for Apple hardware. It is the operating system that presently powers many of the company's mobile devices, including the iPhone, iPod andiPad touch.

Security Model:

Compared to Android security architecture, iOS architecture provides different philosophy for achieving mobile device security and user protection. The iOS application platform empowers developers to create new applications and to contribute to the application store. However, each application submitted by a third party developer is sent to the revision process. During the revision process the application code is analyzed by professional developers who make sure that the application is safe before it is released the application store. However, such an application, when installed, gets all the permissions on a mobile device. Application might access local camera, 3G/4G, and Wi-Fi or GPS module without user's knowledge. Whereas Android lets each user handles its own security on their own responsibility. The iOS operating system makes developers to write safe code using iOS secure APIs and prevents malware applications from getting into the app store.

The iOS security APIs are located in the Core Services layer of the operating system and are based on the Core OS layer of the operating system. Application that needs to execute a network task may use secure networking functions through the CFNetwork API, which is also located in the Core Services layer. The iOS security implementation includes a daemon called the Security Server that implements several security protocols, such as access to keychain items and root certificate trust management. Since the Security Server has no public API, applications use the Keychain Services API and the Certificate, Key, and Trust services API, which in turn communicate with the Security Server.

iPhone OS offers various APIs to implement security features for developers. Like desktop counterpart, iPhone platform uses BSD and Common Data Security Architecture (CDSA) to implement the security features. File access permissions a low level features are implemented by the BSD kernel is a form of UNIX operating system.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 7, October 2015

Higher level functionality is given by CDSA for example encryption, security data storage and authentication. With its own API CDSA is an open source standard but it does not follow the standard Macintosh programming convention and due to this reason this not directly accessible.

Like the dialler and browser with base access the iPhone OS runs applications. This indicates that when security vulnerability is exploited in one service or application the entire operating system may be compromised. This is not same as the other operating system in which the applications are shielded from the operating system and other service by running in the virtual machine. Because by introducing the iPhone OS different security features have been founded and with firmware updates fixed by Apple that give permission to a hacker to get full control over the mobile device. However, applications that are running with basic rights by default isa big threat.

IV. WINDOWS PHONE

Windows Phone is from family of mobile operating system developed by Microsoft for smart phones as the replacement successor to Windows mobile and Zune. Windows Phone features a new user interface derived from Metro design language.Compare tothe Windows Mobile, its main aimis consumer market rather than the enterprise market.It was first launched in October 2010 with Windows Phone7.Windows Phone 8.1 is the latest public release of the operating system, released to manufacturing on 14th April, 2014.

Security Model:

The basic Microsoft Windows security model focuses on two areas: authentication and access control. Authentication is usually encountered when a user attempts to log on to a network or call a process on another machine. In such cases, the system wants to be sure that the user is who she claims to be. Access control in Windows enables applications to selectively grant or deny certain users access to specific services. While any executable code presents a potential security risk, Windows mitigates this risk by limiting the access permissions of a given process. Depending on the user account it is running under. To this end, Windows maintains an access token for each user logged on to the system, the access token contains information identifying the user and the user groups to which the user belongs and information about other privileges that might be available. A copy of this access token is later associated with each process launched by that user. The platform selectively grants or denies access to system services by comparing the access token of the running process with the security information attached to the system object that the user wants to access.

In Windows OS each user and user group is identified in the access token by a unique value called a *security identifier* (SID). Every system objects like a thread, a mutex, a semaphore, an event, or a file can contain a *security descriptor* that includes the SID of the object's owner and of the primary user group to which the owner belongs. Also stored in this security descriptor is the *discretionary access control list* (DACL), which controls access permissions, and the *system access control list* (SACL), which specifies operations on the object that should generate audit messages. Both types of *access control lists* (ACLs) are really linked lists of *access control entries* (ACEs). Each ACE in a DACL either grants or denies certain permission to a specific user or user group. The system checks each ACE in the DACL to determine whether permission has been granted or denied for user. Once it makes the determination, it does not examine the remaining ACEs

V. CONCLUSION

Importance of mobile security is increasing day by day, since personal and professional information are stored in mobiles.This comparative study attempted to compare the security features of three different mobile platforms Android, iOS, Windows. In general, there is no perfect OS that is fool proof and fully secure, although we have come to the understanding that as much as the user has privileges to alter and change system level details, the threats towards mobile computing would be at high risk.With that constraint in line, from this comparative study we have come to a conclusion that, the security features available in Windows phone is more reliable than the other devices.

REFERENCES

1. T.N.Sharma, Mahender Kr. Beniwal, Arpita Sharma. Comparative Study of Different Mobile Operating Systems. International Journal of Advancements in Research & Technology, Volume 2, Issue3, March-2013.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 7, October 2015

2. Baluchistan University of Information Technology, Engineering and Management Sciences, Quetta, Pakistan. Research Journal of Applied Sciences, Engineering and Technology 7(12): 2578-2582, 2014.
3. GoranDelac Faculty of Electrical Engineering and Computing, University of Zagreb, Zagreb, Croatia
4. Google Android, "The Developer's Guide", http://developer.android.com/guide/index.html.
5. Apple inc., iOS Reference Library, Security Overview, http://developer.apple.com/library/ios/#documentation/Security/Conceptual/Security_Overview/Introduction/Introduction.html#//apple_ref/doc/uid/TP30000976-CH201-TPXREF101
6. "The Windows Distributed Security Model", http://thrysoee.dk/InsideCOM+/ch18b.htm
7. "Windows Phone", https://en.wikipedia.org/wiki/Windows_Phone