Mobile Device Security

Fei Yu, feiyu8643@gmail.com, (A survey paper written under the guidance of Prof. Raj Jain)

Download 

Abstract:

Smartphone becomes the most typical and popular mobile device in recent years. It combines the functionality of mobile phone and PDA. Besides, it provides many computer's functionality, such as processing, communication, data storage and etc. It also provides many computer's service, such as web browser, portable media player, video call, GPS, Wi-Fi and etc. This paper analyzes and compares the feature and security issue among three popular brands of smartphones (Google Android, iPhone and BlackBerry) aiming to help customers choose suitable mobile device based on their specific needs.

Keywords: Mobile Device, Smartphone, Security, iPhone, Android, BlackBerry

Table of Contents

1. Introduction

1.1 What is mobile device

Mobile device [MobileDevice] usually is a small, portable size computing device, which allows user to input information through touchscreen or small keyboard on the device. Comparing with conventional computer, mobile device is easily carried out but provides much computer functionality, such as processing, communication, data storage. PDA and smartphone are the two most popular mobile devices. Smartphone combines functionality of mobile phone and PDA. This paper mainly focuses on analysis of security issues on smartphone [Smartphone]. Smartphone usually provides many computer's services, such as web browser, video or audio player, video call, GPS, Wi-Fi, and etc. The top three successful smartphone brands are Google Android, Apple iPhone, and BlackBerry. The following sections will analyze and compare feature and security issue of these three kinds of smartphone.

1.2 Security threats and treads of Smartphone

Smartphone are increasingly becoming a target of security threats [SmarThread]. First, the number of attacker performing browser attack is increasing recent year, whose targets are many different kinds of smartphone's applications [MIB]. There is one kind of Trojan that can infect users' web searching engine and modify web pages or transactions. Some approaches can be used to protect users from this kind of attack, such as transaction validation, site to client authentication, security code evolution and etc. The providers of smartphone's applications should take more responsibility to protect their users from these attacks.

Second, when social network application becomes more and more popular, the importance of security and trust attracts more attention. Security refers to the issue that whether users' private information can be well protected from other illegal accessing. Trust refers to the issue that whether people in the social network provide their real information. To address these issues, a lot of methods, such as strong authentication, account control and protecting application layer attacks, should be added into this kind of applications.

Third, data in form of files are more vulnerable than database records, since files are independent from each other in most of times and hard to be tracked. To perform a high level of accessing control, data safety should be paid more attention.

Fourth, the number of mobile malwares attacking the platform of the device or applications is growing very fast in recent years. Therefore, more sophisticated encryption methods, such as anti-virus software and authentication method should be used. Moreover, application developer should work together to develop more reliable applications.

2. Smartphone Security

This section illustrates the feature and security issue of three kinds of popular smartphone in the market: Android, iPhone and BlackBerry.

2.1 Google Android

The first part will introduce the history of the mobile operating system and main features of the smartphone. The second part will analyze security issues of this sort of smartphone.

2.1.1 Features

Android is a famous operating system for mobile device. Its name is from the first developing company, Android Inc [Android]. In October 2003, Android Inc. was founded, whose focus is on developing software for mobile devices. After two years, Android Inc. was acquired by Google, and became wholly subsidiary of Google. This was the first signal that Google would expand their services to mobile phone market. Figure 1 shows the images of Android Smartphone devices. Android was revealed on November 5, 2007. On the same day, the news that Open Handset Alliance is founded was announced. This alliance includes many large software, hardware and telecommunication companies, such as Intel, HTC, Motorola, T-Mobile and etc, whose aim is to develop open standards for mobile devices. Table 1 shows the history of Android System.

Figure 1 Android Smartphone (source: [Tmobile])

The most attractive part of Google Android is that Google releases most of source code. Google allows the companies within Open Handset Alliance freely install this operating system. This movement leads to significant growth of the mobile market of Android, from 2.8% market share in 2009 to 48% market share in 2011 in smartphone's market. Google Android has became the best selling mobile device platform.

Besides that, third-party application developers can use Java, C, or C++ to develop their applications. Google provides online software store whose named is Market. Users can search and download third party applications from this application. Google also provides applications, such as Goolge Voice, Google Goggles. Google translate, Google shopper and etc. Table 2 shows feature of current Android smartphone.

Table 1 Android version history (Source [AndroidHistroy])

Versions	Time	Description
Android 1.0	September 23, 2008	The first commercial version
Android 1.1	February 9, 2009	Released for T-Mobile G1
1.5 Cupcake	April 30, 2009	Based on Linux kernel 2.6.27
1.6 Donut	September 15, 2009	Based on Linux kernel 2.6.29, 1.6 Software Development Kit (SDK) was released

2.0/2.1 Eclair	October 26, 2009	Based on Linux kernel 2.6.29, 2.0 SDK was released
2.2.x Froyo	May 20, 2010	Based on Linux kernel 2.6.32, 2.2 SDK was released
2.3.x Gingerbread	December 6, 2010	Based on Linux kernel 2.6.35, 2.3 SDK was released
3.0 Honeycomb	February 22, 2011	Based on Linux Kernel 2.6.36, 3.0 SKD was released, table-orientated, support large screen, multi-core processors.
3.1 Honeycomb	May 10, 2011	3.1 SDK was released, support extra input devices, Google Movies, and Books apps
3.2 Honeycomb	July 15, 2011	3.2 SKD was released, support optimization for broader screen size
4.0 Ice Cream Sandwich	October 19, 2011	4.0 SKD was released, support facial recognition, photography enhancement, and other new features

Table 2 Feature of current Android version

Features	**Description**
Video calling	No native video calling in Android, some handset use UMTS or IP network support video call, for example, Google Talk or Skype
Screen capture	Native support screen capture
Handset layouts	2D or 3D graphic library
Messaging	Text messaging and Cloud to Device Messaging Framework
Storage	SQLite database to store data
Connectivity	Support many connectivity method: Bluetooth, Wi-Fi, WiMAX, CDMA, GSM/EDGE, IDEN, EV-DO, UMTS, LTE, and NFC
Language	Support multiple language
Web browser	Provide WebKit engine
Media	Support many audio or video formats
Java	Support Java application, and third-party can use java to develop apps
Streaming media	Support Adobe Flash Streaming, RTP/RTSP streaming, and HTTP Dynamic Streaming, and HTTP Live Streaming
Multi-touch	Native support multi-touch
Bluetooth	Support Bluetooth sending or access stored data
Multitasking	Support multitasking
Voice based feature	Voice control texting, calling, Google search, and navigation
Tethering	Support wired or wireless Wi-Fi hotspot
Hardware support	Support camera, GPS, accelerometer, barometer and other hardware

2.1.2 Security Issues

Android also provides application security through "sandbox" which isolates applications from each other. Without permission, one application can not access to other application's data or private information in the mobile device [Android].

Since Android is an open platform operating system, it provides more freedom to the users to install their desire applications. However, it causes the system easier to be attacked at the same time. There are some types of security issues as below.

Sometimes a flaw of software can cause significant matter. The common method to solve the problem is that the developers recognize the flaws and provide update version of software. For example, Skype once was truly careless to store username, contacts and some other private information. Also in late 2010, a research found that there was a flaw in Android that allowed attacker to download files on Secure Digital (SD) card through JavaScript or HTML. The most recent one was that researchers found out that nearly all Android devices had a security hole in their authentication token. It was possible to man-in-the-middle attack to the Android devices. Now Google has already fixed this flaw.

The second type of security issue is that malicious applications can steal users' private data. Because some of applications may need user's permission to access to SD card, send messages, or access contacts, some malicious applications pretend to be innocent to access and steal data. This may cause a serious damage to users, especially when the device stores lots of confidential information. Although these sorts of malwares shows up occasionally, Google removes them quickly.

The third type of security issue is Root Trojans. Android default setup is to disable of access root, but many users like to root their mobile device. This increases the potential of being attack. Some malwares can steal users' confidential information or even remotely control the users' device. Whenever Google finds out these bad applications, it will remove them quickly. But still, this kind of Trojan does not stop, so it is better for users to ensure root safety by themselves.

Here are some tips for users to improve the level of security for their Android phones [AndroidTips]. First, the most simple and the most effective method is to set password of the device. Before inputting correct the password, attackers can not access stored information. Fingerprint lock is the most secure method. Since some user may concern about leakage of their biometric information, setting up a password still can well protect the device.

Second, user should not change root Android device. Some users want to download applications from unofficial third-party application store, so they choose to root their Android device. This is a dangerous decision, because it will remove many restrictions and security protections from default setting. Root Android phone also means to open their system-level access, which allows many malware applications attack the device. So unless you are a master of Android, it is a bad choice to root Android phone.

Third, although Google Android Market does not ensure that all their applications are free of malwares, Google will remove that application from Market and remotely remove them from devices if many users report a same malicious application. So downloading applications from official Android Market ensures higher degree of security.

Fourth, there are some anti-virus applications available on the Market. Installing one of popular anti-virus can help users scan bad applications and enhance the security.

Fifth, user should ensure the wireless connection is secured and turn off Wi-Fi when they do not use it. Only connecting to familiar wireless network is also a good method to protect the security of device.

2.2 Apple iPhone

The first part will introduce the history of the mobile operating system and main feature of the smartphone. The second part will analyze the security issues of this sort of smartphone.

2.2.1 Features

The iPhone is one of the most popular smartphone in the world marketed by Apple Inc. The first generation iPhone was released on June 29, 2007 [iPhone]. Now it totally released five generations, the 5th generation, iPhone 4S, was released on October 14, 2011. Figure 1 shows the images of iPhone 4S. As a smartphone, iPhone supports video call, text message, media player, email, web browsing through 3G and Wi-Fi connectivity. The users interface is touchscreen, which is designed for one finger or multiple fingers.

Figure 2 iPhone 4S Black and White Version (Source: [AppleiPhone])

The operating system of iPhone is iOS [iOSVersion]. This operating system is also used in other Apple's mobile devices, such as iPad or iPod. Table 3 shows the history of iOS version. Apple users can update their operating system through iTunes. iOS version 5.0 supports wireless data synchronization through iCloud service. This means users do not need USB connection with iTunes to update data. Table 4 shows some special features provided by iPhone.

Any third-party provider who want to develop applications for iPhone needs SDK [SDK]. After paying 99 dollar per year for membership fee, a third-party developer can upload their application to Apple store. Apple store can provide voluntary free download and set a price to their application including 30% revenue which will go to Apple. Developers have to use C, C++, or Objective-C to develop all iPhone applications.

There are also some restrictions of iOS SDK. First, it doesn't allow developers run Java on the iPhone, so developers can not write Java applications and load onto Apple store. Second, it can not install .NET framework. Thus developers can not use their .NET software environment. Third, neither Adobe Flash nor Adobe Flash Lite is supported by iOS.

Table 3: iOS version history

Versions	Time	Description
iOS 1.x	June 29, 2007	First version of iOS, upgrade through 1.1.5
iOS 2.x	July 11, 2008	Upgrade through version 2.2
iOS 2.x	July 11, 2008	Upgrade through version 2.2
iOS 3.x	June 17, 2009	The first generation iPhone use iOS 3.1.3
iOS 4.x	June 21, 2010	Released for iPhone 3G, iPhone 3GS, and iPhone4
iOS 5.x	June 6, 2011	Released for iPhone 3GS, and iPhone 4(GSM and CDMA), iPhone 4S

Table 4: Feature of the fifth generation: iPhone 4S

Features	Description
Phone	Make Facetime calls, enable/disable option for voice dial
iMessage/Message	Send text, video, photo, location or contact information
General	Show general information of phone
Siri	Voice commands, support English, French and German
Notification Center	Display stock or weather

Calendar	View, create calendar
Clock	Display time
Weather	5 day weather forecast, hourly update
Stock	Real time finance information
Newsstand	Show all paper or magazines had been downloaded
Reminders	To-do list
Twitter	Twitter application
Music	Play music or broadcast song
Camera	Take photos, Auto Focus
Maps	Find location, maps, or routes
Mail	Receive or send email
Photos	Create or edit local photo
Safari	Web browsing
iCloud	Selected data or documents can sync with iCloud account
Game Center	Play game with friends
Settings	Basic setting function
Keyboard	Input words or command, support Chinese input method
PC-Free	Start fresh the device, wireless sync to iTunes
YouTube	Video play
FaceTime	Video call via camera
iTunes/App Store	Search, purchase, download, and install apps
Contacts	Edit contact information
VoiceOver	Speak text selection
Bluetooth	AVPCP 1.4 supported
Minor improvements	Bug fixes, delete app data

2.2.2 Security Issues

According to the publication from Apple website, Apple considers the security of iPhone for personal or business use from four aspects: device security, network security, data security and application security [iPhoneSecurity].

For device security, it mainly focuses on preventing unauthorized use of device. It requires each user to have a unique passcode to generate encryption key. This is used to protect the private information stored on the iPhone. Also, company can set some specific settings or restrictions when iPhone used in the business environment. The passcode policy provides some specific requirements, such as passcode reuse history, minimum length and complex of passcode, maximum failure attempts and so on. These polices can be enforced by install in the configuration profiles, which are XML files. All the restrictions and polices, the authentication credentials and other confidential information are written in configuration profiles. In order to prevent anyone from altering the setting and changing the contents of the profiles, these profiles are signed and encrypted by Triple Data Encryption Algorithm (3DES) or Advanced Encryption Standard 128 bits (AES-128). According to different needs of companies, iPhone supports setting restrictions of the device. For example, it can restrict YouTube, camera, voice dialing and etc. Through the above methods, Apple can control the device security.

For network security, Apple considers both authorized use and safe data transmission through Wi-Fi or cellar data connection. IPhone uses standard X.509 digital certificates to authentication which prevent unauthenticated access on confidential resource of the company. IPhone integrates two-factor token, RSA SecurID and CRYPTO Card, to protect company's resource. In addition, iPhone supports many Virtual Private Network (VPN) technologies, such as IPsec, L2TP, Cisco and PPTP. It also supports Secure Sockets Layer (SSL) VPN, which provides a higher level of security to transmit data. In order to provide safe internet usage, iPhone provides web traffic security through two approaches: SSL v3 and Transport Layer Security (TLS) v1.0. It encrypts the internet communication. What's more, iPhone supports Remote Authentication Dial In User Service (RADIUS) and provides its wireless network security though Wireless Application Protocol 2 (WAP). The AES encryption with counter mode provides the highest security of wireless communication.

For data security, there are two kinds of data needed to be encrypted. One is transmitted data and the other is stored data on the device. IPhone uses AES-256 to provide the hardware encryption. Users can not disable this encryption. It also encrypts the data and back it up to the iTunes. Through generating a strong key, iPhone can encrypt the transmission data. Passcode also plays an important role in data protection, thus setting a strong passcode is critical. If users accidentally lose the device, issuing a remote wipe command can deactivate the device and erase all the information. In order to provide brute force passcode attempts, local wipe command can also erase information after many failed attempts. The default attempts setting by Apple are ten times. Of course, users can set different number by themselves.

For application security, a "sandboxed" approach prevents one application access data of other applications. If an application wants to read other

application's data, it needs to use application programming interface (APIs) whose services are supported by iOS. In order to prevent application from being changed, all third-party providers need to use Apple issued certification to sign their applications. The encrypted keychain ensures the security of storing digital information. AES, RS4, or 3DES can be used to encrypt application data. AES encryption and Secure Hash Algorithm 1 (SHA1) hashing can be use in iPhone to protect data too. What is more, the hardware encryption can be also used to protect the application data.

Although Apple claims to provide high security of iPhone, new security holes still open up [SecurityIssue]. Recently German news showed that flaws in software running on the devices can be a serious problem. After clicking an infected PDF file, the attacker can steal all the confidential data stored on the device.

So some researchers give six tips to iPhone users to enhance the security [iPhoneTips]. First, do enable Auto-Lock. Although it is only a default feature which can not specific assigned to a security function, it includes passcode lock which is a good method of protection. Second, do enable passcode lock, the four digit password preventing unauthorized access to the device. This ensures the safety of the stored data. Third, do use safety Wi-Fi. This ensures that personal Wi-Fi network is using wireless security protocol. Enable the feature on asking to join networks function to choose network. This limits the chance that users connect to an unsafe network. In addition, disconnect Wi-Fi when users aren't using it. This also reduces the chance to connect to unknown networks. Fourth, do open mail securely. For corporate users, through Microsoft Exchange Server to open corporate mail is much safer. For personal use, always ensuring open SSL protection which encrypts mail information. Fifth, do use Safari as web browser. Safari has some default security setting. Besides, users can block pop ups on Safari setting. In addition, users can delete the cookies in a regular time base to protect their private information. Sixth, people can use device to set specific restrictions to their employee or their children.

2.3 BlackBerry

The first part will introduce the history of the mobile operating system and main features of the smartphone. The second part will analyze the security issues of this sort of smartphone.

2.3.1 Features

BlackBerry is the name of one kind of smartphone device developed by Research In Motion (RIM), which is an Canadian company [BlackBerry]. The first BlackBerry smartphone was unveiled in 2003. In this first version, it supports web browsing, mobile telephone, text messaging, internet faxing, push emai, and other internet services. Figure 3 shows some images of BlackBerry devices. The most famous feature is that BlackBerry provides high level of security through complex encryption method to push email and instant message.

Figure 3 BlackBerry Device (Source: [BBFeature])

The operating system of BlackBerry is BlackBerry OS [BBOS] written by C++. BlackBerry OS supports multitasking and specialized input device, such as trackball, trackwheel, trackpad and touchscreen. This operating system supports WAP1.2, Mobile Information Device Profile (MIDP) 1.0 and a subset of MIDP2.0. This supports wireless synchronization exchange tasks, email, and other business schedule through BlackBerry Enterprise Server (BES). BES is a software package supporting companies' email system. It can be use in Google Apps, Lotus Domino, Novell GroupWise and Microsoft Exchange. The BlackBerry operating system can be automatically updated through their wireless carriers. The Blackberry OS 6 was

released in late 2010. The most current version-Blackberry OS 7 was released in August 2011. There are many series of device, they have some common features with slightly different in each version. Table 5 shows different series of devices running on Black Berry OS6 and OS7. Table 6 summarizes the most common features provided by BlackBerry.

Like other smartphone devices, third-party application can be ran on BlackBerry devices. All third-party developers should be digitally signed to ensure the safety of the application. One big news is that now android applications can run on unmodified newest BlackBerry smartphone on BlackBerry OS7. This news is announced by RIM on October 20, 2011.

Table 5 Series Devices running on Black Berry OS6 and OS7

Versions	**Name**
OS6	Pearl 3G(Stratus)9100, Curve 3G 9300/9330, Bold(Essex)9650, Style(Oxford)9670, Bold2(Onyx)9700, Bold(r020)9780, Torch(Talledega)9800,
OS7	Curve 9350/9360/9370, Bold(Bellagio) 9790, Torch 9810/9850/9860, Bold 9900/9930

Table 6 Common feature of BlackBerry Device (Source [BBFeature])

Features	**Description**
Camera	Capture picture and video record
Wi-Fi	Wi-Fi access
Video/Audio	Support Video, Audio, or Picture play
Touchcreen/ Trackpad	Recent versions support touchscreen, trackpad or both.
BlackBerry Messenger	Support sending or receiving messages, voices, videos, or pictures through BlackBerry PIN
Web browsing	Web browsing engine, Google Quick Search
Third part application	Other applications provided by third party, user can download and install these applications on their device.
Game	User can download and play games
BlackBerry Maps	Show maps, and search location
BlackBerry News	Users can view recent news
Corporate Data Access	Facilitated to access corporate data
GPS	Navigation
Bluetooth	Support Bluetooth
Social Networking	Support social networking applications

2.3.2 Security Issues

BlackBerry Enterprise Solution provides industry-leading security on both stored data and wireless transmitted data. It also provides some advanced security features for government users.

For stored data, BES makes mandatory password authentication. After ten times of failed attempts, all the memory on the device will be erased. All the messages, contact information, tasks and schedules will be encrypted through AES and Password Keeper. Administrator can remotely change the password. All local information can be locked or deleted by administrator after receiving report of phone lost. Only authenticated command can be execute on the system and only decrypted communication can be permitted. BES never stores users' private data. Only server and the users' mobile device can decrypt data. This prevents unauthorized parties' attack [SecurityFeature].

For wireless data, Blackberry Enterprise Solution uses both AES and 3DES to encrypt the transmitted data. Each smartphone user has a secret key stored both on secure enterprise account and on their device. This secret key can be regenerated by the user. BES and the smartphone device use the secret key to encrypt or decrypt the transmitted data. Through the whole transmission process, data is encrypted. If users want to access corporate intranets, RSA SecurID provides two-factor authentication, both username and token care be request. Both proxy mode and end to end mode of HTTPS communication are supported by BlackBerry. Figure 4 shows wireless data transmission use HTTPS. In proxy mode, BEA and application Server are connected by SSL or TLS. In end to end mode, smartphone and application server are connected by SSL or TLS. Only trusted end points can choose the mode. Also BlackBerry supports IBM Lotus Notes email encryption. All the third party applications are required to have their developer's sign. Corporation uses trusted certificate authority or self-signed certificate to sign, e.g. Public Key Infrastructure X .509 standard.

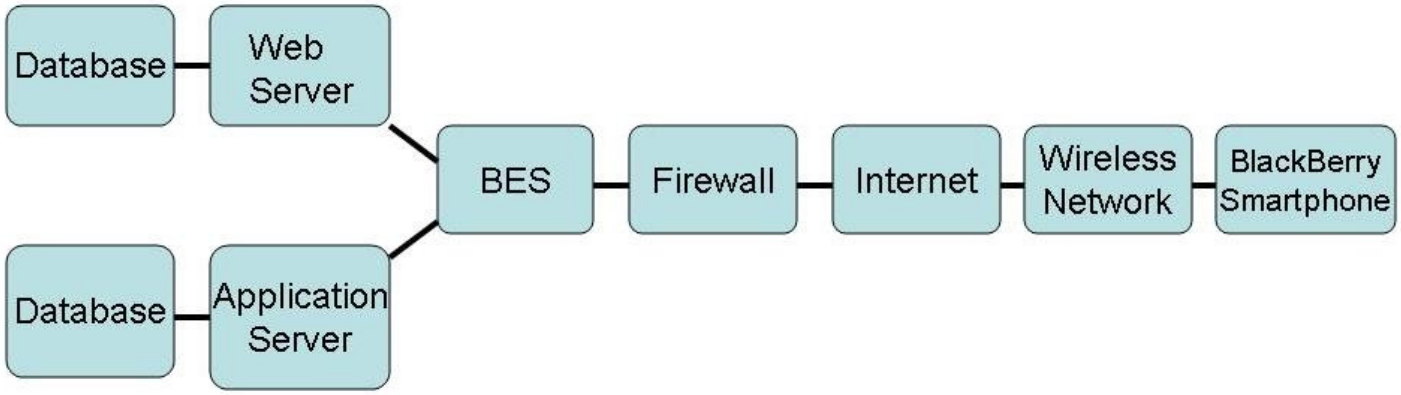

Figure 4 Wireless Data Transmission (Source: [SecurityFeature])

BlackBerry also provides advanced security features for government users [AdvanceSecurity]. BlackBerry provides devices which encrypt Federal Information Processing Standard 140-2 validation and Secure/Multipurpose Internet Mail Extensions (S/MIME) and public key infrastructure. This meets the requirement of Department of Defense. S/MIME provides a high level of smartphone security and use private and public key to encrypt messages. PGP also aims to improve a high level of security. BlackBerry Smart Card Reader allows users add more security feature to existing security architecture. Through all above methods, BlackBerry provides a safety security protection for users.

3. Summary

The purpose of this paper is to give a big picture of recent popular smartphones and help users choose different brands based on their different needs on security. In the first section, this paper introduces the definition of mobile device. In the second section, it compares different features and security issues of three popular smartphones: Google Android, Apple iPhone and BlackBerry.

For Google Android, the most advantage is that it provides open platform which makes the products grab the largest market share quickly. The programming language is Java as well as C/C++. The development of SDK is free. These free platform and free SDK also cause some security problems. The mobile device and applications are vulnerable to be attacked. This requires users to be more responsible and careful to protect their private data when downloading applications.

For iPhone, its interface is very attractive, thus it can entertain users better. The platform is closed and the programming language is only objective C. Third party providers need to pay member fee to upload their applications to Apple store. The security level of iPhone is fairly good because of the control by Apple store and the closed platform.

For BlackBerry, it is a business device instead of a entertaining device. It provides a high level of security on both stored data and wireless transmitted data. To enterprise users, it provides many functions and methods to ensure the safety of business information. In addition, it provides advanced security features for government. Therfore, BlackBerry would be a good choice if users have high requirement on confidentiality and security.

References

1. [MobileDevice] "Mobile Device", http://en.wikipedia.org/wiki/Mobile_device, Description: an introduction of mobile device in wiki webpage.
2. [Smartphone] "Smartphone", http://en.wikipedia.org/wiki/Smartphone, Description: an introduction of smartphone in wiki webpage.
3. [SmarThread] "Smartphone Security Threats and Trends", http://www.fishnetsecurity.com/News-Release/Smartphone-Attacks-and-Hacking-Security-Threats-and-Trends-2011, Description: a webpage to introduce recent security threats trends in 2011.
4. [MIB] "Man in the Browser", http://en.wikipedia.org/wiki/Man_in_the_Browser, Description: an introduction of man in the browser in wiki webpage.
5. [Android] "Google Android", http://en.wikipedia.org/wiki/Google_Android, Description: an introduction of Google Android in wiki webpage.

6. [AndroidHistroy] "Android Version Histor", http://en.wikipedia.org/wiki/Android_version_history, Description: an introduction of Android Version History in wiki webpage.
7. [AndroidTips] "Android Security Tips", http://www.cio.com/article/675129/Android_Security_Six_Tips_to_Protect_Your_Google_Phone?page=3&taxonomyId=3061, Description: a webpage to introduce six tips to protect Google Android smartphone.
8. [iPhone] "iPhone", http://en.wikipedia.org/wiki/Iphone, Description: an introduction of iPhone in wiki webpage.
9. [iOSVersion] "iOS Version Histroy", http://en.wikipedia.org/wiki/IOS_version_history, Description: an introduction of iOS version history in wiki webpage.
10. [SDK] "iPhone SDK", http://en.wikipedia.org/wiki/IPhone_SDK, Description: an introduction of iPhone SDK in wiki webpage.
11. [iPhoneSecurity] "iPhone Security", http://www.apple.com/iphone/business/docs/iPhone_Security.pdf, Description: a webpage of Apple to introduce iPhone security.
12. [SecurityIssue] "iPhone Security Issue", http://www.huffingtonpost.com/2011/07/07/iphone-security-issues-apple-update_n_892203.html, Description: a webpage of Apple to introduce iPhone security issue in 2011.
13. [iPhoneTips] "iPhone Security Tips", http://www.pcworld.com/businesscenter/article/152128/six_essential_apple_iphone_security_tips.html, Description: a webpage to introduce six tips to protect iPhone
14. [BlackBerry] "BlackBerry", http://en.wikipedia.org/wiki/BlackBerry, Description: an introduction of BlackBerry in wiki webpage.
15. [BBOS] "BlackBerry OS", http://en.wikipedia.org/wiki/BlackBerry_OS, Description: an introduction of BlackBerry operating system in wiki webpage.
16. [BBFeature] "BlackBerry Feature", http://us.blackberry.com/smartphones/blackberry-bold-9900-9930/#!phone-specifications, Description: a webpage to introduce BlackBerry features.
17. [SecurityFeature] "BlackBerry Security Feature", http://us.blackberry.com/ataglance/security/features.jsp#tab_tab_stored_data, Description: a webpage to introduce BlackBerry Security features.
18. [AdvanceSecurity] "BlackBerry Advance Security", http://us.blackberry.com/ataglance/security/government.jsp, Description: a webpage to introduce BlackBerry Advance Security Service for government users.
19. [AppleiPhone] "iPhone images", http://www.apple.com/iphone/, Description: official website of apple.
20. [Tmobile] "Android phone images", http://www.t-mobile.com/shop/phones/default.aspx?features=48CC3997-D234-4683-8B5A-F026B9DB5528#HTC-Wildfire-S-Black, Description: official website of Tmobile.

List of Acronyms

SD: Secure Digital
SDK: Software Development Kit
3DES: Triple Data Encryption Algorithm
AES-128: Advanced Encryption Standard 128 bits
VPN: Virtual Private Network
SSL: Secure Sockets Layer
TLS: Transport Layer Security
WAP: Wireless Application Protocol
API: Application Programming Interface
SHA: Secure Hash Algorithm
MIDP: Mobile Information Device Profile
BES: BlackBerry Enterprise Server
S/MIME: Secure/Multipurpose Internet Mail Extensions

Last modified on Dec 8, 2011
This and other papers on latest advances in performance analysis are available on line at http://www1.cse.wustl.edu/~jain/cse571-11/index.html
Back to Raj Jain's Home Page