Smartphone Security System

Anas Alarfaj

Introduction

Many years ago mobile phones were used just for calls and sending messages. In the last decade, the usage of mobile phones has increased in a big manner. They have become more sophisticated and more powerful. They have come to be called smartphones. Due to its wide application range the smartphone has been highly popular among the human community. The smartphone is slowly taking the place of laptops and has started competing with computers for performing various user tasks in an efficient way. Apart from communication, smartphone helps user activities by performing many tasks. A smartphone user can carry out personal and important information such as internet banking, online bookings, chatting, emails, using GPS, connectting to social network and many others. While carrying out all these tasks the smartphone user passes authentic information such as passwords, contact details and PIN details. They also store personal information such as SMS message, photographs, passwords and some confidential data. There are chances that some people can pick this information and use them for robbing the users. Therefore, it is required to implement security systems for protecting the user information against fraudulent activities. This paper will discuss some of security problems faced by a smartphone user and also focuses on the methods which can be done to protect the smartphone user information

Smartphone Security System

Smartphones are similar to computers and have many features in common. The extra hardware available in a smartphone is mainly GSM radio and control processor. Before discussing the security systems, it is required to know the basic smartphone architecture. This will help in understanding the sources of security threats and to think about its counter measures.

Smartphones in recent times have the popular Android as open source platform. Other smartphone platforms are symbian, iOS, RIM, Microsoft, and others. Android because of its cross platform capability can run any third party applications and has gained wide acceptability among the users (Wang, Y., Streff, K., & Raman, S,2012; Dorflinger, T., Voth, A., Kramer, J., Fromm, R, 2010; Bhutta, F.K., Ghafoor, A., Sultan, S, 2012). The Android allows any third party to develop applications of user's interest. Users can download and install these applications on their smartphones according to their needs. Android market provides hundreds and thousands of applications for the users to select and use. The presence of a third party to develop user applications in the android platform raises the security concerns in the area of smartphones. Even the best security models may find security loopholes due to the third party presence.

The attacker having the rights to develop applications in android can develop malicious programs to extract user information without the knowledge of the source platform (Delac, G., Silic, M., & Krolo, J, 2011). This may appear as a genuine application and will take a huge time for identification. In such a programming environment it is essential to have sufficient security systems to protect user information against malicious attacks. Some security steps have to be created and automated for easier identification of malicious android application.

The purpose of this study is to find out the possible ways for mobile malware threats, the extent of damage they can cause and also the security systems that can be adopted to get rid of these threats to the maximum possible extent.

In recent times the attackers are targeting more on smartphones rather than personal computers (Bhutta, F.K., Ghafoor, A., Sultan, S, 2012) for following reasons: Computer based systems are more aware, smartphone is slowly but steadily capturing the computer market, users prefer to store vital information in smartphones due to its portability and easy access, presence of possible loopholes in relatively new smartphone architecture and lack of awareness on mobile malwares.

Smartphone Architecture

There are some of available operating systems. Android is the most common open source platforms for smartphones. Android basically consists of an Operating system, middle ware for the third party to develop user desired programs and applications (Muslukhov, I., Boshmaf, Y.; Kuo, C., Lester, J., Beznosov, K, 2012). The android architecture is in the form of layers with Linux kernel as the lowest layer. This layer executes tasks such as memory management and power management. They also contain the hardware drivers. The layer above this contains graphic libraries. This layer also has the ability to run compact and memory efficient executables. This layer has a component called binder, which does the task of carrying out communication between the applications. The next layer is the android application framework layer, which carries out the activity of interactions among the applications. It also aids in establishing the hardware connection with the applications.

Above these three layers is the application layer, which is either developed by google or any third party. These applications are developed by utilizing the application framework layer and the associated graphic libraries (Ugus, O., Landsmann, M., Gessner, D., Westhoff, D, 2012). The developer uses all the features as provided by the android to develop the application. These applications are made available to the user either free of cost or on payment basis. Some of the examples of android applications are: browser, dialer, calculator, calendar, diary and many others.

Android malware history

Android OS had its first release in the year 2008. Since then it has gained big popularity from the smartphone users. Also, the number of malware targeting the android has increased (Delac, G., Silic, M., & Krolo, J. (2011).

The first malware to attack android was SMS Trojan in the year 2010. This malware had a fake widow's media player icon and was spreading to other smartphones as well as infecting the files. SMS Trojan was sending fake SMS's to a few numbers without any consent from the user. This was followed by GPS spy malware. This malware entered the smartphone in the form of a snake game and was efficient enough to provide the smartphone GPS coordinate to a remote server. In December 2010, another Trojan emerged which would collect user information from the smartphone and transmit it to a remote server. In the year 2011 a Trojan call Pjapps which got hidden in the application and did the job of corrupting all the applications already installed in the smartphone. Zitmo appeared in smartphones and mobile devices. It was blocking the SMS messages to the mobile phone and transmitting it to a different server. Zitmo also paired with Zeus banking Trojan to steal the user's bank related information. It steals the internet banking information and provides them to a remote server. NickiBot malware did the job of transmitting the contact information, audio files, video files and the call log details to a remote server. In recent times a malware named RootSmart has emerged to gain the root access of the smartphone. On accessing, it will take the full control and the user will not be able to perform any settings or use any applications. This malware will corrupt all the installed applications (Pieterse, H.,Olivier, M.S, 2013; Dorflinger, T., Voth, A., Kramer, J., Fromm, R, 2010). Table 1 gives the highlights of all the major malware attacks on android until the year 2012. The attacks thereafter are nowhere mentioned explicitly.

Ways for Smartphone Security Threats

Mobile malware accounts for a major amount of security threats in smartphones. They get themselves installed in the smartphone memory through SMSs and emails, for example, SMS Trojan and SMSZombie. Once installed, these malwares gets the administration rights and infect maximum possible files. This makes it difficult for the user to uninstall or remove the infected files. The malware threats are available in many forms (Wang, Y., Streff, K., & Raman, S. 2012; Dorflinger, T., Voth, A., Kramer, J., Fromm, R, 2010). Apart from malware threats GPS system with WiFi access points is also a way for the attackers to access user information in real time. The GPS can provide the user's location and other private details at every instant to the attacker. Another advanced approach as followed by the attackers is through GSM radio control. The GSM software flaws due to its premature nature are utilized to gain access over the smartphones processor. Once in control of the processor, the attacker can control the smartphone at his will. Figure 2 represents the flow chart for the possible ways in which a malware can pose threats to the smartphone (Ugus, O., Landsmann, M., Gessner, D., Westhoff, D.(2012); Pieterse, H., Olivier, M.S, 2012). Some of the ways in which mobile malware attacks the smartphone are as follows

Text Messages

There are applications for connecting the users to social networking sites such as facebook, twitter, watsapp and others. These social networking sites involve chat, SMS, data sharing, photos and other personal information. The attacker targeting through fake android applications can get access of smartphones through text messages (Pieterse, H., Olivier, M.S, 2012). The users not able to differentiate between a good and the fake one will open any SMS received by him/her. Fake SMS, which are actually virus programs, gains way into smartphones and starts their malicious activities such as charging fees through SMS gateways, infecting data files and all other unwanted activities.

Contacts

Malware also targets the contact list of the users. In corporate environment the contact information is an essential thing. There are specialized malware that attacks the contact list of the smartphone, completely destroys them and sends the complete list to a third party thereby passing on the vital information to another person (Delac, G., Silic, M., & Krolo, J, 2011). Such that attacks actually target the specified smartphone users are access their smartphones through GPRS or other internet connectivity.

Slowing down the processing speed

These Malware target the smartphone processing speed. Modern smartphones have operating frequencies of more than 1GHz and 1GB memory. Their performance is at par with the computers. Malware slows down the processing speed by running unnecessary programming multiple times. They create network traffic, infect the file and slow down the speed.

Video. All the smartphones have video and camera facilities. The malware can get access of the smartphone camera, take pictures/video and send it to a third party through WiFi connections. These kinds of attacks are rarely seen because the chances for information extraction are very limited (Delac, G., Silic, M., & Krolo, J, 2011; Dorflinger, T., Voth, A., Kramer, J., Fromm, R, 2010). Apart from accessing the smartphone camera these viruses can also transmit the pictures already available in the smartphones to a third party.

Phone transcriptions

It may happen that the malware or the virus can take control of the audio recording feature of the smartphone to tape the audio at any time and transmit the same to any third party. The audio message transmission can take place through SMS or MMS. The malware can also trigger audio recording through any message services. For getting smartphone access the attacker will send an audio file through SMS or MMS

(Dorflinger, T., Voth, A., Kramer, J., Fromm, R, 2010; Pieterse, H., Olivier, M.S, 2012). The user when opening the SMS will unknowingly trigger the audio recording for a particular duration. The malware will send the audio file to any third party.

Documentation

Malware can target the documents available in the form of pdf, word and excel documents. Users store most of their documents in smartphone memory because of its portability and easy access features. These documents can be targeted by the malwares and transmitted to an third party through SMS or MMS.

GPS tracks

The GPS tracks showing the users movement is normally stored in smartphone memory. These tracks provide information on user's movement particularly to his/her residence. The attacker can trace this information to understand the user movement (Pieterse, H., Olivier, M.S, 2012). This way of stealing the user movement is a major security threat to the smartphone users.

Attack Vectors on Smartphones

The smartphone provides many ways of connecting itself with another device. These interfaces are vital and a smartphone cannot live without them. To list a few: UMTS, Infrared, Bluetooth, W-Lan, WiFi and many others (Wang, Y., Streff, K., & Raman, S, 2012). This makes it more vulnerable to malware and viruses. Malware finds its way through these vectors to transfer its malicious contents. The malware can utilize any of the interface method to find a way inside the smartphone memory and to perform maximum destruction (Pieterse, H.,Olivier, M.S, 2013). Figure 2 describes the attack vectors on a smartphone in a pictorial form. Some the attack vectors as described are

Network services

Inbuilt mobile services like SMS and MMS are a source for the malware to perform its malicious activities. The attacker normally sends an SMS with some URL address. The user when clicking the URL will establish a connection between the smartphone and the remote server. The attacker can make use of this connection to transfer any details from the smartphone or to perform any malicious activity (Bhutta, F.K., Ghafoor, A., Sultan, S, 2012). This kind of attack is called smishing. In another method, the attacker sends a voice call to attain the user's trust and extracts confidential and valuable information. The attacker can then use this information to perform his malicious activity (Bhutta, F.K., Ghafoor, A., Sultan, S, 2012). This kind of attack is called vishing.

Internet connection. Smartphones are continuously connected to internet through WiFi or 3G 4G networks. Most of the smartphone activities are based on the internet services and it is a must for any smartphone to be continuously connected. In such situations the threats due to viruses increase. The attacker passes the URL through any renowned social groups or networking sites. The user when clicking this URL will increase the risk for being attacked (Delac, G., Silic, M., & Krolo, J, 2011). The URL links sometimes appear in such a way that the user has no option but to select the link.

Bluetooth

This can be another method for connecting a smartphone to another device. While connecting a device through Bluetooth, two devices agree to get paired and allow data transfer. Attacker can use this interface to transfer the malicious content to the smartphone. Once the connection is established the data transfer can take place freely. There are limited chances of security threat due to Bluetooth interface because of password protection and file confirmation feature before the file transfer.

USB

This interface is normally used to charge the smartphone and to perform data transfer from personal computers. While connecting a smartphone to a computer there are every chances that malware content is transferred to smartphone memory (Delac, G., Silic, M., & Krolo, J, 2011). A malware available in a computer can access the smartphone information when connected through USB interface.

Apart from the discussed attack vectors there are many other modes such as infrared and W-Lan through which a malware can enter the smartphone memory and perform malicious activity. For example, a malware residing in peripheral device memory can perform the malicious activity when connected to the smartphone.

Smartphone malware types

The smartphone working environment is similar to that of computers. The malwares associated with smartphones highly resembles that of the computers (Pieterse, H., Olivier, M.S., 2012; Delac, G., Silic, M., & Krolo, J, 2011). The malware for computers are normally Trojan, worms, and other kinds of viruses. These malware resides in the computer memory and carries out malicious activities. In the same way, smartphones too have Trojan horse, botnet, worm and rootkit viruses as malwares. Each of these malwares attacks the smartphones in different ways. These malware either attacks the smartphones on individual basis or joins together with others to create disaster. A brief overview on major smartphone malware has been presented.

Trojan Horse

These malware are normally involved in phishing activities. They pretend as if they are performing some useful activities, but carries out malicious activities in the background. They are normally developed to perform some

useful application (Delac, G., Silic, M., & Krolo, J, 2011). The smartphone user while working on the application unknowingly transmits the useful information to the third party. The attacker uses social networking sites to transmit these applications at a fast rate. The applications developed with such malware are often very hard to detect by even educated users.

Botnet. This form of attack involves usage of devices to control the smartphone from a remote location. The devices use their capability and computation power to get control of the smartphone (Delac, G., Silic, M., & Krolo, J, 2011; Dorflinger, T., Voth, A., Kramer, J., Fromm, R., 2010) . On getting the smartphone control they can perform any task of their interest. Botnets are aimed to perform activities such as sending spam mail and performing attacks on the device/operating systems.

Worm

These malware find ways into the smartphone memory through attack vector, resides there and replicate themselves in a very fast manner, thus occupying most of the smartphone memory (Dorflinger, T., Voth, A., Kramer, J., Fromm, R., 2010; Wang, Y., Streff, K., & Raman, S., 2012). They normally work for reducing the smartphone efficiency, reducing operating speed and blocking certain smartphone activities. Worms are common to all operating system irrespective of any specific operating system such as Android. The first of these malware was found with Symbian-OS. It is believed that worms are the first among the available malwares that started attacking smartphones/mobiles.

Rootkit

These are dangerous malware that tries to get the administration privileges and attack the smartphone. They find their way into the smartphone memory through attack vector and mask themselves to avoid identification. They wait for the user to perform any specific activities and gains the control/ administration privileges (Delac, G., Silic, M., & Krolo, J, 2011). These are more common to computers and until recent past no such malware has been seen to be associated with the samrtphone devices. However, these malware can very well be developed for smartphone applications.

Available Security Mechanisms in Smartphones

Until recent times, sufficient security mechanisms have been implemented on the largely used android based smartphones. Developers are working on the premature android by adding security features. The attackers are always in a thrust to find new ways of attack. The security mechanism for any system has a growing curve. The more the security protection, more the attacker will find ways to counter attack (Ugus, O., Landsmann, M., Gessner, D., Westhoff, D, 2012). Security mechanism is a continuous process wherein the developer forecasts the possible attacks and continuously updates his/her system. By doing so the developer ensures that the system is safe from any forthcoming attacks. In present situation there are many ways of security mechanisms available for smartphones. Each of these security mechanisms has their strength areas and weak areas. The attacker always searches for the weak areas to carry out his activities (Pieterse, H.,Olivier, M.S,2013; Ugus, O., Landsmann, M., Gessner, D., Westhoff, D., 2012) . Some of the already available security features with android based smartphones are as listed and explained

Sandboxing mechanism

This mechanism works by providing unique identification to each android application while under installation. This ensures that two different applications cannot make use of the same process (Bhutta, F.K., Ghafoor, A., Sultan, S, 2012; Dorflinger, T., Voth, A., Kramer, J., Fromm, R, 2010). In the case of applications sharing the same process they must share the userid which is possible only upon permission from the user. The sandboxing mechanism basically isolates one application from another. It provides checkpoints at different levels of processing and does not allow an application to share the resource or access any smartphone data.

Permission Mechanism

It is another security mechanism which asks for required permission before installation of the application and also at various stages of processing. It consists of a package manager who is responsible and has the authority to grant permissions while the application is running (Muslukhov, I., Boshmaf, Y.; Kuo, C., Lester, J., Beznosov, K, 2012). Number of checkpoints is created and the applications are forced to sought permission from the package manager at every checkpoint. Some of the checkpoints are INTERNET_permission, WRITE_SMS_ permission and CAMERA_USAGE_ permission.

Application authentication verification

This authentication is done at the application store or the application market. The smartphone users normally download the application from reliable app store or an app market. This way of security mechanism evaluates the application before inducting it in the application market (Ugus, O., Landsmann, M., Gessner, D., Westhoff, D, 2012). It detects for any malicious intent of the application and verifies each action of the application before allowing it in app store. The applications are evaluated in runtime and a certificate named "trusted app" is provided. The application can enter the app store only after getting the certificate.

Antivirus Usage

This is a common method used in personal computers for protection against virus. The same can be used in smartphones for reducing malware threats. These antivirus

software continuously runs to detect any incoming malware or the already existing malware (Bhutta, F.K., Ghafoor, A., Sultan, S, 2012; Muslukhov, I., Boshmaf, Y.; Kuo, C., Lester, J., Beznosov, K, 2012). The antivirus software can be set to carry out periodic scanning of the smartphone memory for determining the presence of any virus.

User authentication method

In this form of security mechanism the users have the rights to authenticate the applications process at different stages. For example, while doing internet access or online money transaction the application will ask for user authentication. The user authentication can be through finger print, gesture recognition, retina scan, voice recognition and face recognition (Ugus, O., Landsmann, M., Gessner, D., Westhoff, D, 2012). This security mechanism not only protects the smartphone against malware activities but also through against thefts.

Proposed security model for Android OS

Based on the carried out studies on android architecture, ways of malware threats, attack vectors and the available security mechanisms a security model is proposed which will minimize the security related threats. It is learnt that the android architecture is built and developed on Linux kernel. The Linux kernel takes care of various activities such as memory access, process management, device interface, managing device divers, networking related activities and system security. On the top of Linux kernel is the Dalvik virtual machine that and some libraries. The main activity of Dalvik VM is to execute android applications. In order to access the system services by a third party for application development, android has provided an application interface through C/C++ system libraries. A framework is also provided to access high level services with calculated restrictions. This helps the third party to develop his/her own application and access all the smartphone services. However, this way of providing service access rights gives a room to the attackers and malwares to steal the data and other confidential information.

The proposed model tries to embed certain security features into the present android architecture. This method provides a resource platform to the third party developer and restricts the smartphone services through permission based security enforcement. In order to access any smartphone service the third party application has to get permission from the in between layer. This security model actually removes any interaction among the application. Each of the application while installation is provided with a unique number and the Linux access control mechanism stores the unique number and grants them certain required permission. Now when the application tries to perform any malicious activity, it has to get control of services other than the one that is granted. While granting other services the smartphone will recognize and deny access. This method of restricting the system service access can bring down the security threat to a large level.

However, this method of permission restriction will have issues when the applications have to interact among themselves or to access a service at the same time. For solving such issues a digital certificate can be provided to both applications. The provided digital certificate must be same for both applications. The smartphone services can be accessed and shared by both applications in the presence of the similar digital certificate.

Another issue present in this model will be assigning of permissions. Each application may require different set of permissions. It is the duty of the operating system to determine the specific permissions as required by a specific application. In certain cases the permission sought by an application may be a subset of another already available application. This model will grant the permission only at the installation time and does not allow any modification henceforth. The permission levels as granted by the operating systems are characterized as normal nature, dangerous nature, with signature and signature/systems.

Each of the permission level has different impacts on the system security threat and the operating system has to check for different conditions before granting of rights. The normal nature has little impact on the system security, dangerous nature can provide information of critical services such as telephony, location information and others. Signature permission is used for sharing and accessing of services among applications. signature/systems permissions are those that does not requires any user approval.

Conclusion

There is a study was carried out in the area of smartphone security systems. The possible ways for security threat were discussed and the attack vectors were also studied. All the malware types found until recently were also overviewed. It was seen that attackers find new way and adapt new methods every now and then. For all security mechanisms, the attacker will find methods for way out. They continuously search for the weak points of any security mechanism to perform attack. For operating system like android with cross platform feature, it is necessary to have a strong security mechanism. All the available methods on smartphone information security where studied and found that each of the method has issues in some or the other way. A new method for improving the security threats was proposed and found to be effective if implemented.

References

Bhutta, F.K., Ghafoor, A., Sultan, S. (2012). Smart phone based authentication and authorization protocol for SPACS . High Capacity Optical Networks and Enabling Technologies.
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6421448&isnumber=642142,

Delac, G., Silic, M., & Krolo, J. (2011). Emerging security threats for mobile platforms. *MIPRO, 2011 Proceedings of the 34th International Convention*.
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5967292&isnumber=5967009

Dorflinger, T., Voth, A., Kramer, J., Fromm, R.(2010).”My smartphone is a safe!” The user's point of view regarding novel authentication methods and gradual security levels on smartphones. *Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on*.
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5741642&isnumber=5741585

Ilyas , M. (2006). *Smartphones*. Chicago: International Engineering Consortium. DOI: www.iec.org

McIntyre, S. (2012). *Which smartphone is the most secure*.
http://www.csoonline.com/article/691219/which-smartphone-is-the-most-secure-

Muslukhov, I., Boshmaf, Y. Kuo, C., Lester, J., Beznosov, K. (2012).Understanding users’ requirements for data protection in smartphones.
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6313685&isnumber=6313630

Nosowitz, D. (2013). *The future of smartphone security*.
http://www.popsci.com/gadgets/article/2013-09/future-smartphone-security

Rose, B. (2011). *Smartphone security: How to keep your handset safe*. Retrieved from
http://www.pcworld.com/article/216420/how_much_smartphone_security_do_you_need.html

Ugus, O., Landsmann, M., Gessner, D., Westhoff, D. (2012). A smartphone security architecture for app verification and process authentication. *computer communications and Networks.*
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6289217&isnumber=628917,

Pieterse, H., Olivier, M.S. (2012). Android botnets on the rise: Trends and characteristics, *Information Security for South Africa (ISSA)*.
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6320432&isnumber=6320423

Pieterse, H., Olivier, M.S. (2013). Security steps for smartphone users, *Information Security for South Africa,* 1-6.
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6641036&isnumber=6641027

Wang, Y., Streff, K., & Raman, S. (2012). Computer. Smartphone Security Challenges, 45(12), 52-58.
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6269870&isnumber=6383143