International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.3, No.6, June 2014 DOI:10.15693/ijaist/2014.v3i6.113-116

Security Threats in the Smartphone's

Kanwal N K*; Janjua, P K**
*Corresponding Author: Assistant Professor, Department of Criminology & Forensic Science, Dr H S Gaur University (Central University), Sagar-MP.

**PDF-UGC, Computer Centre, Panjab University, Chandigarh (UT).

Abstract
Mobiles phones are the one of the most potent and fastest means of communication by the modern society. The first and 2nd generation of the devices was used only for calling and texting but the advancement in the field of Information Technology and communication has provided users 3G & 4G mobiles which are frequently called Smartphone, which enable the user to have many features such as high quality camera, web browsing, up to 64 GB on board memory much higher than the older days PCs hence taking the place as handheld PCs. These mobiles mainly have IOS, Android, Window, Blackberry, Symbian, Java & Bada as one of the operating system. Whenever users start these smartphones they have to login to their server and hence have to provide your information to the server. Similarly when users use other social networking sites on these devices uploads the personal/family information including pictures and videos. Some users also start operating their bank account through them; this important & confidential information can be accessed by the unauthorized persons for commission of crimes. Present work concentrates on studying the vulnerability of Smartphone's of different make and model to the attack of different viruses and malwares.

Keywords: Smartphone, malware, viruses, mobile phones, Security threats

l. Introduction

Smartphone's are the hand held devices capable of having high computing capabilities and bundles of features such as high resolution camera, ability to web browsing, onboard high memory, fast speed and easily operate able operating system.. These

devices have various types of operating systems among them IOS, Android, Window, Blackberry, Symbian, Bada and Java etc. The developers has developed the numerous application compatible to

the different operating system of the Smartphone, these applications includes the categories of social networking, business, games, audio/video and other fun & utilities related activities. The easy availability of these applications and simple installation/operation of these applications are promoting the users to use the Smartphone in their daily lives both personally as well as professionally in various routine activities such checking & sending of e-mails, web browsing, banking transactions, keeping important documents and other relevant information. Hence not only modern generation even old generation is getting dependent on these Smartphone for their all activities and to perform all these activities the users have to keep their secret information on their smartphones, which in turns is a major threat to them. The Smartphone of the individuals even carries the important information such as bank detail, addresses, contact details of the business clients/family members, SMS, Call Logs, personal pictures, videos and documents etc., which can be used by the criminals, if we lost our mobile [8]. Therefore in the present paper an attempt has been made to study various aspects to secure the information on the Smartphone.

ll. Related Work

Schmidt et al. (2008): Worked on enhancing Security of Linux-Based Android Devices [14].

Nicolas Seriot, N. (2010) Despite Apple claim any application downloaded from App Store to standard iphone can access a significant amount of personal data [3]. Data stored is at the risk without the knowledge of the user like phone number, email accounts settings (except passwords), keyboard cache entries, Safari searches and the most recent GPS location.

Jeon et al. (2011): Smartphone and its application are now most popular keywords in mobile technology. However, to provide these customized services, Smartphone needs more private information and this can cause security vulnerabilities. Worked on security of Smartphone based on its environments and described countermeasures [11].

Emigh, J. (2012): According to ESET's survey results, most of the Smartphone's devices are not well protected. Encryption of company data is occurring on only one-third of BYOD phones, tablets, and PCs [9].

Ham,Y.J. and Lee, H.W.(2014): — Worked on problem of the breach of privacy through illegal leakage of personal information and financial information inside mobile devices without users' notices, as the malicious mobile application is relatively increasing In order to reduce the damage caused by the malicious Android applications, the efficient detection mechanism should be developed to determine normal and malicious apps correctly. They aggregated real-time system call events activated from malware samples distributed by Android Malware Genome Project. After extracting the basic difference feature and characteristics of system call events pattern from each normal and malicious

applications, they determined whether any given anonymous mobile application is malicious or normal one [10].

lll. Objective of Proposed study

The present work has been conducted on the handsets of different make and models ranging from apple to java operating system, the study mainly concentrates on studying the susceptibility of these handsets to various security threats. **IPhone, Windows Mobile, Blackberry, Symbian, Android** handsets were selected for present study.

IV. Results and Discussions

iPhone

With the release of IOS 4 the Malware for the iPhone took a different approach. As the multitasking that users take part on their systems easily goes unnoticed, allowing the existence of malware to be easier to miss and less intrusive [7]. Malware is more commonly found on iPhones that have been jail broken."Jail breaking" means freeing a phone from the limitations imposed by the wireless provider and in this case, Apple. Users install a software application on their computer, and then transfer it to their iPhone, where it "breaks open" the iPhone's file system, allowing you to modify it; however, this also opens it up to malware. By jail breaking a phone, users are possibly allowing malicious applications into their device which has access to their personal information including their bank account. These applications are not subjected to the same limitations as Apple and therefore are easier to get from a rogue reference and infect cell phone. Additionally, by not changing the password on a jail broken iPhone, the SSH service, is easy for malicious attackers to create worms used to infect the users operating device. An example of how important this threat is to note was highlighted by Ike, a worm created to raise security awareness when it comes to using these jail broken devices. Apple is slow to pinpoint vulnerabilities, including the SMS (texting) exploit released in the summer of 2010 by Charlie Miller. This also revealed that Apple is so slow to release that third party organizations were able to produce a security patch before Apple [1].

Windows Mobile

Windows Mobiles are much more susceptible to attract malware via SMS. An interesting facet of the Windows Mobile OS is that many of the system calls are shared with its full-featured desktop counterparts. This detail has contributed to many pieces of malware that have originated on the Windows OS being ported to the Windows Mobile OS. A remarkable example of this is the Zeus botnet that in recent years has begun to appear on mobile versions of Windows [8].

Blackberry

Since BlackBerry uses the most closed source of the operating systems and developers has been quite careful in keeping the sensitive inner workings of this smart phone a secret from the public thus making it less prone to exploits. An accepted option to the previous two mobile operating systems, the BlackBerry also suffers from the multitasking concerns that make it easier for malware to run unnoticed. An interesting proof of concept developed for the BlackBerry is the BBProxy application that was presented at DEFCON.

Symbian

It is the oldest of the smartphones and one of the most popular. Symbian OS was originally developed by Symbian Ltd. It was exclusively designed for smartphones and currently maintained by Nokia. Unlike Symbian OS, it requires an additional user interface system, Symbian OS was subject to a variety of viruses, the best known of which is Cabir, which spreaded through Bluetooth. Virus.WinCE.Duts infected executable files in the device's root directory. Another famous program was Backdoor.WinCE.Brador, This malicious program opens a port on the victim device, opening the PDA or smartphone to access by a remote malicious user. Trojan.SymbOS.Mosquit, a type of game which sends SMS messages to telephone numbers coded into the body of the program. Trojan.SymbOS.Skuller, which appeared to offer new wallpaper and icons for Symbian was an SIS file - installer for Symbian platform, it clearly highlighted two flaws of Symbion that is it can be overwritten and lack of stability. Another prominent virus was 'gavno' which freezed the systems when trying to launch the application after reboot.

Android

The Android operating system is the only open source operating system discussed herein. Android is unique in that it is community driven. The Android operating system is not owned by an individual organization, so it is developed in the best interest of the users. However, the applications are not monitored for vulnerabilities in the marketplace, so anyone can submit applications containing malicious functions which are less likely to be caught. Essentially, it is up to the users to determine if it is a safe and reputable source from which they are getting the application. Amazon now has a 3rd party market place, which imposes additional policies and restrictions on applications that are distributed. Android is based on the Linux operating system. On Linux, availability on Android is unlike others and there is not much evidence of ported malware. This is not because there is not any known Linux malware out there, but because it doesn't receive much attention. All operating systems have distinct strengths and weaknesses; however, many are the same and essentially are up to the user and the configuration of the password. Users need to remember that they should not install apps from unreliable and unsecured sources, although it is impossible for the users to know them all; users need to ensure that they are from a reputable source. If not, that is where malware commonly comes from, with backdoor apps veiled as secure applications. Also, jail broken phones are at a huge risk if the user maintains the default password [14-15].

V. Conclusions

The study reveals that the Smartphone has easy connectivity and hence can be connected easily with other devices for

web browsing or data transfer due to this feature these9. Smartphone may get easily attacked by the virus or other malwares from other computers, laptops, mobile & other relevant devices which in turns imposes the intimidation to logs, SMS, MMS, Pictures, Videos, Documents & other confidential information stored in the Smartphone's. This important information can be hacked & used by the criminals. The installation of third party applications from the web also affects your privacy as many of the applications access all your information including your profiles on social networking sites, your location, bank details, web browser history etc. Smartphone users have to put their password, pin code and other confidential information to use it but in many cases we prefer to keep password saved by the websites so that we need not to enter it again and again in this way users themselves are transferring their important information to the unsafe hands [2], So present study proposes some important precautions that must be kept in mind for securing your Smartphone:

1. Use a PIN/Key lock code/Pattern Lock.
2. Protect sensitive data by Encrypting Phone Memory/Memory card & Put Pin lock on SIM Card.
3. Be aware & careful while using Wi-Fi services from unknown and unsecured routers.
4. Set up the default configuration of your Bluetooth non discoverable.
5. Be careful while downloading & installing third party applications.
6. Avoid Rooting of Smartphone by unauthorized persons if required it must be done only by the experts.
7. Back up your data on the server with proper password and encryption.
8. Install genuine Security software's and lock your device remotely, so that if get into the unsafe hands the data on the Smartphone get wiped out.

Bibliography:

1. Mulliner, C.R. (June 2006): Security of Smart Phone, Master's Thesis of University of California
2. Chen, J.V., Yen, D.C., Chen, K. (2009): The acceptance and diffusion of the innovative smart phone use: A case study of a delivery service company in logistics. Information & Management 46(4).
3. http://seriot.ch/resources/talks_papers/iPhonePrivacy.pdf
4. http://www.mt.co.kr/view/mtview.php
5. http://arxiv.org/ftp/arxiv/papers/1201/1201.0945.pdf
6. http://threatcenter.smobilesystems.com
7. http://www.csoonline.com/article/2129760/mobile-security/which-smartphone
8. http://www.sophos.com/en-us/threat-center/security-threat-report.aspx
9. http://www.brighthand.com/default.asp?newsID=18676&news=Smartphone+security+malware+Android+iPhone
10. Ham, Y.J. and Lee, H.W.(2014): Detection of Malicious Android Mobile Applications Based on Aggregated System Call Events, International Journal of Computer and Communication Engineering, Vol. 3, No. 2,149-154.
11. Jeon, W., Kim, J., Lee, Y. and Won, D. (2011): A Practical Analysis of Smartphone Security, M.J. Smith, G. Salvendy (Eds.): Human Interface, Part I, HCII 2011, LNCS 6771, pp. 311–320.
12. Monk, A., Fellas, E., Ley, E. (2004): Hearing only one side of normal and mobile phone conversations, Behaviour & Informaion Technology 23(5) , 301-305.
13. Ni, X., Yang, Z., Bai, X., Champion, A.C., Xuan, D. (2009): DiffUser: Differentiated User Access Control on Smartphones. In: Proc. 5th IEEE Int'l. Workshop on Wireless and Sensor Networks Security, WSNS 2009.
14. Schmidt, A.-D., Schmidt, H.-G., Clausen, J., Camtepe, A., Albayrak, S. (2008): Enhancing Security of Linux-Based Android Devices. In: 15th International Linux Kongress .
15. Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., Dolev, S. (2009): Google Android: A State-of the-Art Review of Security Mechanisms, Cornell University library.
16. Smartphone (2010): Information security risks, opportunities and recommendations for users, *ENISA Report*.
17. Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., Dolev, S. (2009): Google Android: A State of the Art Review of Security Mechanisms, arXiv 2009.

Authors Profile

Dr.Navjot Kaur Kanwal*

Corresponding Author, Assistant Professor, Department of Criminology & Forensic Sc., Dr.HariSingh Gour Central Univ., Sagar, Madhya Pradesh, India. Dr. Navjot Kaur Kanwal , ***M.Sc, PhD (Forensic Sc.), PGDCA, M.Sc-IT & MCA , holds a vast teaching, administrative and research experience in field of Forensic science. Currently serving as Assistant Professor, Department of Criminology & Forensic Sc., Dr.HariSingh Gour Central Univ., Sagar, Madhya Pradesh, India. Her fields of interest are Cyber Forensics and Photo Forensics. She has guided about 25 Master's Research

dissertations and 2 students are taking guidance for their Ph.D. She has also published 1 Book and presented/published more than 15 papers in reputed journals and conferences. She has also organized National and International level Conferences/Symposium for the development of the Subject.

Dr.Parveen Kumar Janjua**
**** Post Doctoral Fellow (UGC), Computer Centre, Panjab University, Chandigarh**

Dr. Parveen K. Janjua, , *M.Sc, PhD (Forensic Sc.), PGDCA, PDF-UGC* worked as founder HOD-Forensic Science & Coordinator, Institute of Forensic Science and Criminology, Bundelkhand University, Jhansi. He was awarded the Doctorate for giving criteria to determine the sex of Individual from fingerprints. Presently working as Post Doctoral Fellow of UGC in Computer Centre, Panjab University and doing full time research in the field of Mobile **Forensics**. Appearing in various Courts Of Law as a Forensic expert for giving opinion on Mobile Forensics and Disputed Documents and giving training and lectures to Police personnel's in Central Detective Training School, BPRD/Ministry of Home Affairs, GOI. Dr. Janjua has been the members of many National level committees for making uniform syllabus of M.Sc (Forensic Science) in Indian Universities & various developmental activities for the subject formulated by the Bureau of Police Research & Development, Ministry of Home Affairs Govt. of India, New Delhi. He has guided many Master's Research dissertations and 2 PhDs. He has already published three books on "*Forensic Science & Crime Investigation*" and *An Interdisciplinary Approach to Forensic Science*. He has presented /published many research papers in various international & National conferences/Journals. He has also organized two National and one International level Conferences/Symposium for the development of the Subject.