International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 9, September- 2014

Safeguarding Against Cyber Crimes Spreading Through Mobile Devices

Samir Thakkar
Assistant Professor
Dept. of Computer Applications, Faculty of Science
The MS University of Baroda
Vadodara, India

Mahesh Mulani
Assistant Professor
Dept. of Computer Science
KSKV Kachchh University
Bhuj - Kachchh, India

***Abstract*— The use of mobile devices has increased tremendously recently. These mobile devices are no longer tools only for voice calls and messaging services. These devices now come with internet access capability at much higher data transmission rates and other smart features. As more and more people have started using Internet on mobile devices, the number of cyber crimes and cyber attacks has also increased. Cyber attacks by hackers and intruders are significantly increasing in India as the penetration of mobile devices is increasing. Moreover Internet capability on such devices makes them easy targets for attackers. The users of such mobile devices are either attackers or victims of cyber crime world. Mobile devices provide flexibility to attackers as well, as they use such devices to plan and commit cyber crimes from anywhere.**

In addition to that, most of the mobile device users are not aware about the security issues related to such devices. This fact makes them soft target for cyber attackers. Attackers use various techniques to reach to these target mobile devices.

Lack of awareness about cyber attacks and preventive measures among people is a major concern. This paper highlights different cyber attacks possible on or through mobile devices. Critical factors which make attackers showing interest in mobile devices are identified. This paper also suggests the guidelines for safeguarding mobile devices against various cyber attacks.

Keywords*— *Cybercrime, Cyber Security, Mobile Device Threats, Cyber Attacks, Safeguarding Mobile Devices

I. INTRODUCTION

Mobile devices are much common today. It includes mobile phones, tablets, PDAs, Ultramobile PC, Carputer etc. and provides to its user ubiquitous processing of information. Mobile devices with smart features are available at very low cost in the market, which have increased the number of users of such devices significantly within short period of time. People use these devices to perform financial transactions, information processing, rapid communication through emails or social networking sites and many more. These devices have affected our lives at such an extent that our morning alarm clocks have been replaced by mobile phones. Today, incredible advancements are being made to mobile devices. Even simple handheld devices provide enough computing power to run small applications, play games, music and to do many other tasks.

But one of the major problems with such devices is security. The way use of these devices is increasing, security standards have not been strengthened with the same pace. As mobile devices have increased their processing capabilities, they have become more prone to malicious softwares like viruses, worms, Trojans etc. Malicious softwares are one of the attack vectors used by hackers and intruders to commit cyber crime on mobile devices. E. Kritzinger and S.H. von Solms have classified personal internet users into Home users and Non-home users, large number of which are novice users, means they do not possess the information security knowledge to understand and protect their personal information [1].

Cyber crime also known as computer crime can be defined as a criminal activity performed using computer or any other electronic media [2]. In cyber crime computer is either target or used as a tool. As mobile devices now come with computing capabilities, these criminal activities are largely targeted to mobile devices as well. Apart from regular mobile devices, large numbers of everyday objects are also often connected to a network or Internet, such as payment cards, car stereo system, smart televisions, RFID tag embedded devices, home appliances, etc. making them vulnerable to security threats.

II. MOBILE DEVICES – ATTRACTIVE TARGET FOR ATTACKERS

According to Norton report, a global survey of end users showed that 38 percent of mobile users had already experienced mobile cybercrime. 52 percent of the mobile phone users are storing sensitive information on their mobile devices, putting their data on risk [3]. Attackers are therefore exploiting vulnerabilities of mobile devices using old techniques along with new ones. In addition to that following factors are making mobile devices an attractive target for attackers.

A. Enough Number of Terminals

Hackers and intruders are gaining interest in targeting mobile devices for committing cyber criminal activities due to excessive amount of its usage. It is expected that number of mobile subscriptions will reach to 6,915 million till the end of 2014 worldwide. Mobile broadband subscription is going to reach to penetration of 32% in 2014, compare to 26.7% in 2013. About 40% of households were connected to Internet in 2013 [4]. These usage figures are rapidly increasing in

developing countries. Thus there are sufficient numbers of terminals for attackers to commit criminal activities.

B. *Enough Connectivity*

Mobile devices offer multiple communication options such as infrared, Bluetooth, WLAN connections, USB connections and synchronization. In addition to that technological advancements like HSDPA, 3G, EV-DO, EDGE, and GPRS make these devices able to connect to Internet anywhere. This offers more choices for attackers to breach into the device.

C. *Security Vulnerabilities*

A large number of mobile devices, especially smartphones are running operating systems like iOS, Android, Symbian and others. Each of these operating systems allows third party applications to be installed, which may contain malicious code. Even the softwares installed in mobile devices may have its own loopholes. Thus these softwares vulnerabilities can be easily exploited by attackers. Android's Linux kernel, iOS, and the Windows operating system each consists of a large number of lines of code that contain numerous known and unknown vulnerabilities [5].

D. *Often Unprotected*

A large number of mobile devices are not password protected and hence easily accessible. Portability of mobile devices makes them easy to steal, which may result in lost of personal and financial data. Sophisticated attackers may use various techniques to break into stolen mobile devices and gain access to data stored within it [6].

E. *Lack of awareness*

Users of mobile devices posses very little knowledge of security issues related to such devices. Users sometimes do not even realize that they have become victim of a cyber attack. It is easy to get infected with malicious programs when receiving SMS, MMS, downloading or installing applications, clicking on untrusted links or browsing unsafe websites, resulting in revealing personal information, contact list, calendar schedules, notes or location information. It may also result in equipment damage and financial loses. A large number of users are not even aware about the existence of laws against cyber criminal activities.

III. THREATS TO MOBILE DEVICES

Incredible advancements are being made for mobile devices today. These advancements have made it easy to steal or gain information from these devices. A numerous type of cyber attacks are possible on mobile devices. Following are highlighted concerned threats.

A. *Malwares, Viruses and Worms*

Processing capability of mobile devices have made them prone to malicious programs. Skull and mosquito Trojans, Cabir and Lasco worms are examples of such programs targeting symbian operating system. Brador Trojan was designed to affect Windows CE. Other software platforms like Android and iOS are also prone to malicious programs. These programs may access or change information available on such devices or may be designed to commit certain cyber criminal activity. Some malwares silently send premium rate SMS or force the device to call premium rate numbers, resulting in overbilling and financial loss.

B. *DoS (Denial of Service) Attack*

The main objective of this attack is to make a system/device unavailable to the intended users. A piece of malicious code can be spreaded to numerous mobile devices and/or computer networks to send large number of packets simultaneously targeting a single system to make its services unavailable. Such attacks are known as push attack through DDoS. If it is targeted to a mobile device to hang up, is called crash attack [7].

C. *Mishing*

Mishing is a combination of mobile phone and phishing. In this technique, attacker tries to get personal information from victim by sending luring messages like winning large amount in a lottery draw or any other such creative method. In another technique attacker pretend to be a bank authority and notifies victim that his bank account security has been compromised and need to be updated. Then attacker tries to get financial information from the victim. Varieties of creative methods are used by attackers to convince victim to reveal its private information. If this communication is done through voice call, it is called Vishing (Voice + Phishing) and if it is done through SMS, it is called Smishing (SMS + Phishing).

D. *Hacking Bluetooth*

Bluetooth is an open wireless technology used for short range communication. It is one of the common technology found different types of mobile devices. Attackers are using various tools to exploit vulnerabilities of Bluetooth technology and access information available on device.

1. *Bluejacking*

Bluejacking is sending unsolicited messages over Bluetooth to Bluetooth enabled devices. Attacker searches for nearby Bluetooth devices and sends a visiting card which contains a message in the name field. If user does not recognize what the message is and allow it to the contact to be added in the address book, the attacker send him unsolicited messages that might be automatically opened as they are coming from known contact.

2. *Bluesnarfing*

Bluesnarfing is the theft of information from a wireless device through Bluetooth technology. This enables the attacker to access calendar, contact list, E-mails or to copy pictures and videos.

3. *Bluebugging*

Bluebug programs allow the attacker to take control of victim's phone. The attacker may conduct many activities such as initiate phone calls, read and send SMS, read and write phonebook contacts, listen to phone conversations and connect to the Internet.

E. Botnet

Botnet is a network of computers infected by specific bot virus which gives an attacker the ability to remotely control those computers. The connection between the traditional Internet and the mobile network may act as a gateway for malware to move freely between these networks. Thus mobile devices connected to Internet may be a part of botnet. Such botnets are used by attackers to commit organized crimes like sending spam, DoS attack or collecting and sale of information that can be exploited for illegal purposes [8].

F. Mobile Device Theft

Theft of mobile devices, especially mobile phones has drastically increased in recent years. According to Lookout's Phone Theft in America report, 1 in 10 U.S. smartphone owners are victims of phone theft. 3.1 million American consumers were victim of smartphone theft [9]. When anyone loses his/her mobile phone, more than anything "Contact List" and "Personally Identifiable Information", that really matter, are lost. Financial information and other credential data may also be lost.

IV. GUIDELINES FOR SECURING MOBILE DEVICES

- Use modern Internet security solution for your mobile device. Use antivirus and antimalware softwares.
- Updating these security applications regularly is necessary.
- Download or accept programs and contents only from a trusted source.
- Blocking premium calls or messages is one way to minimize financial losses, even if malware does get installed
- Be aware and ask questions, in case someone is asking your personal or financial information through voice call.
- Do not answer to text messages asking for your personal information.
- Avoid calling any phone numbers, as mentioned in received message, to cancel membership and/or confirming a transaction which you have not initiated but mentioned in the message.
- Never click on hot link received through message on your mobile device.
- Turn off Wi-Fi and Bluetooth when not in use.
- Disconnect Internet connection when not in use.
- Add a security mark on your mobile device. Mark your alternate number and short address on device as well as on battery to safeguard against lost incidents.
- Set a strong password to your mobile device.
- In case of loss of cell phone, immediately register a complaint to cell phone service provider with your IMEI number to help them block your phone. Also register a complaint at the police station and obtain and preserve a copy of FIR.
- Take periodic backup of information stored on mobile device.
- Use cables and hardwired locks when using devices like laptops in public places.
- Use of motion sensors and alarms may be very effective for securing laptops.
- Keep mobile devices close to yourself whenever possible to safeguard against potential thieves.
- Use encryption software to protect critical data on mobile devices.
- For laptop and portable computers, disable guest accounts and rename Administrator account.
- Immediately report cyber criminal activity to nearby police station as soon as it is realized.

V. CONCLUSION

Mobile devices are increasing their computational and storage capabilities day by day. Internet connectivity options have made them more vulnerable to various cyber attacks. One of the major problems is the lack of awareness about cyber crime among mobile device users. Some users do not even realize if they have become victim of a cyber attack. Attackers largely take advantage of this fact to breach into user's mobile devices. Awareness is a strong tool to defeat cyber crime. Spreading knowledge of cyber criminal activities will definitely help reducing such attacks.

Resistance to complaint against cyber criminal activities is another factor which encourages attackers to commit crime. A large number of victims do not register complaints because they may don't want to put themselves in such hassles or they are not aware about laws against such crimes. Following the security guidelines may prevent being victim of cyber criminal activities.

REFERENCES

[1] E. Kritzinger. and S.H. von Solms, "Cyber security for home users: A new way of protection." Computers & Security, pp 840-847, 2010.

[2] G. Nina, and S. Belapur, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives. Wiley India Publications, 2011.

[3] Internet Security Threat Report 2014. Symantec Corporation.

[4] "ICT Statistics: International Telecommunication Union." International Telecommunication Union. http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (accessed May 6, 2014).

[5] S. Hassen and A. Gehani, "Mobile Security: Challenges, Lessons, and Future Directions." Information Systems Security Association Journal, pp 10-16, 2013.

[6] R. Paul, and J. Foote, "Cyber Threats to Mobile Phones." US-CERT. February 2013. http://www.us-cert.gov/sites/default/files/publications/cyber_threats_to_mobile_phones.pdf (accessed May 2014).

[7] G. Nina, Information Systems Security: Security Management, Metrics, Frameworks and Best Practices. Wiley India Publications, 2009.

[8] F. Anne Ruste and A. Jøsang, "Consequences of Botnets Spreading to Mobile." 14th Nordic Conference on Secure IT Systems. Oslo, pp 37-43, 2009.

[9] Lookout Reports – 2013, https://www.lookout.com/resources/reports/phone-theft-in-america (accessed May 2014).