IJoFCS (2013) 1, 20-26

e-forensic PRESS

The International Journal of FORENSIC COMPUTER SCIENCE

www.IJoFCS.org

DOI: 10.5769/J201301003 or http://dx.doi.org/10.5769/J201301003

Preventive Actions to Emerging Threats in Smart Devices Security

Nilay R. Mistry(1), M S Dahiya(2), Hitesh P. Sanghvi(3)

(1) Institute of Forensic Science, Gujarat Forensic Sciences University, Gandhinagar, E-Mail: nilaymistry30@gmail.com

(2) Institute of Forensic Science, Gujarat Forensic Sciences University, Gandhinagar, E-Mail: dir_fs@gfsu.edu.in

(3) Cyber Crime Division, Directorate of Forensic Science, Gandhinagar, E-Mail: hpsanghvi@gmail.com

Abstract - Smart devices have become indispensable tools for today's highly mobile workforce. Smart devices can be used for different type of operations, including email service, office stuff and remotely accessing data etc. As these devices deliver productive benefits, they pose new risks like malicious attacks to users. Viruses, worms and Trojans, under whatever category they are classified, can cause anywhere from minor irritation to total system failure. The study revealed that the only type of phone, vulnerable to a virus attack is one that runs an operating system - a Smartphone. There are emerging threats like Smishing, Blue Jacking, Sim Card duplication, Data theft, Mobile Spamming, IMEI change and many more. In this research paper, all such emerging threats have been discussed and solution has been provided to recover from those threats and attacks.

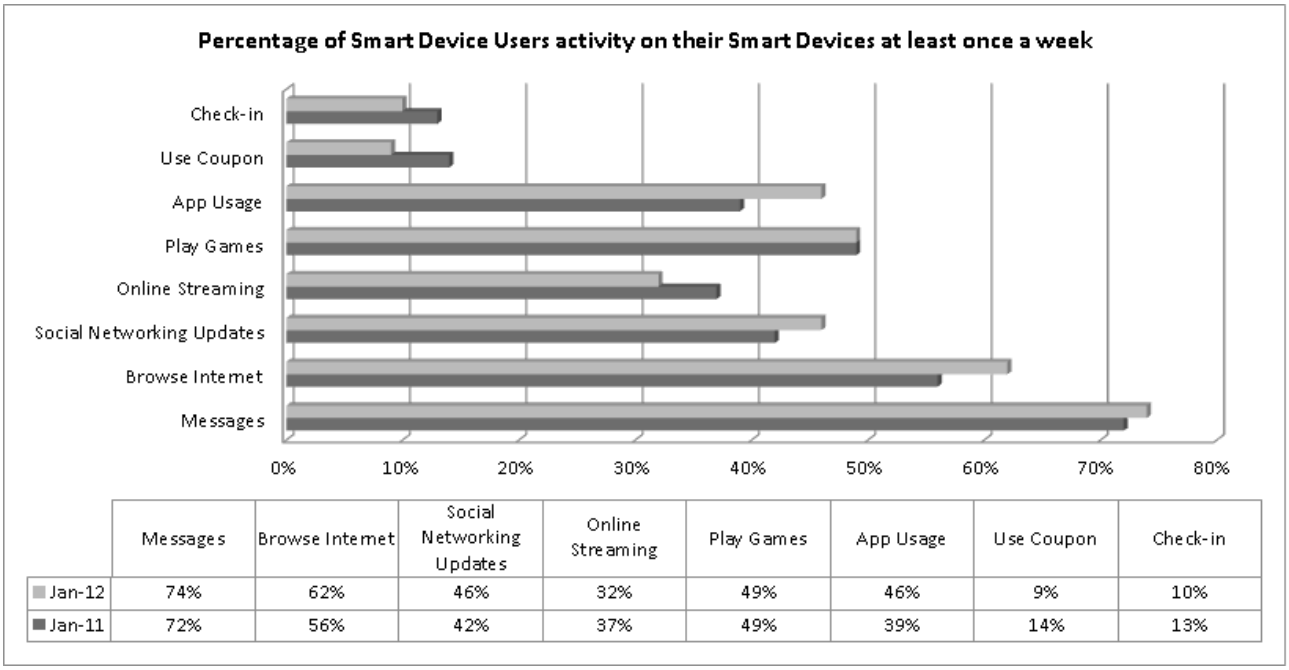
Key words: Threats, Virus, Mobile Crime, Mobile Forensics

1. Introduction

The smart phone and smart phone industry has rapidly developed across the world. The days of the phone being used as simply a voice device have gone. Today each smart phone has become a small PC in the pocket of each person.

Year 2011/12 is an era of embedded systems – Smart Devices and Tablets are enormously common in use. Most of the smart devices have the facilities like sending and receiveing emails and multimedia messages, internet connectivity, wireless file transfer, video calling, image and video capturing, one touch social networking etc. [2] Although these are features that user might find useful and convenient, attackers may try to take advantage of these services. As a result, an attacker infect smart phone with potential virus, steals important information, spoof the incoming/outgoing calls and sms, smishing, hack or access phone through Bluetooth. In this smart devices world professionals make their bank transactions, online payment, secure emailing on internet

Paper submitted on April 11th, 2013.



	Messages	Browse Internet	Social Networking Updates	Online Streaming	Play Games	App Usage	Use Coupon	Check-in
Jan-12	74%	62%	46%	32%	49%	46%	9%	10%
Jan-11	72%	56%	42%	37%	49%	39%	14%	13%

Figure 1 : Percentage of Smartphone owners activity [Source http://www.adage.com/]

connectivity based smart phone. Here shown the Smart devices users activity and which kind of facilities are used most by them.

Smart devices security attacks are easy to commit due to application download support from device itself. For an example, FakeToken – an Android based application contains man-in-the-middle functionality to hijack two-factor authentication tokens and could be remotely controlled to grab the initial banking password from the infected mobile device [1]. Offender can listen calls through call eavesdropping technique, grasp all incoming and outgoing e-mails, see all the websites being surfed by the smart phone user through Global Positioning System, at any time, can know where the victim is [4].

2. Mobile Threats and some prior terminology

Smart device user may recall the basic rules of security while using PC; forget that the similar risks apply to smart phone as well. At Present some of the most prolific transport methods for malware (instant messaging, IP network traffic, web browsers, and email attachments) have made their way to the common user on a smart device platform. Android based smart devices consists its own Market place from where user can download the application. There are various free applications or cracked version, untrusted applications reside on internet which spreads risky kind of malware in to the smart device. A study says "*71% expect a serious incident arising from attacks on, or problems with, connected smart devices within the next 24 months*" [6]

2.1. Prior terminology

To get acquainted with various mobile threats, some prior terminology like threats, attacks and mobile crime is need to refer.

Threats: To breach a security of the device or system, resulting into a constant danger to the information.

Attacks: Act or action that exploits vulnerability (i.e., an identified weakness) in controlled system.

Intelligent Crime: Every technology has its own loopholes. By using these loopholes adversely to exploit the security of the system and theft or spoof the informa-

tion from system or device is referred as an Intelligent Crime.

Mobile Security Threats: To breach a device security via infect device with a malwares, theft of important and personal data, spoofing call or sms, is referred as a Mobile Security Threats.

2.2. Classification of Emerging Threats

This section addresses all potential threats related with smart phones and provides its solutions. The threats categorization is as follows.

- Physical Threats
- Intelligent Threats
- Non detectable Threats

To understand the risks behind various types of threats and provide better solutions, categorization of threats is needed.

2.2.1. Physical Threats

Use of smart device by an offender for any illegal work, after stealing the device from actual user. Physical act of stealing smart device falls under this category. A smart device is stolen from the actual user. The offender then can access all information stored in. The information is either erased or discarded from the device. Even by using special software program, the erased information can be retrieved. So, there is no guarantee of information that will remain intact. Also the privacy of information is not there.

2.2.1.1. Smart Device Theft:

Physically theft the smart phone device and make a use of that device to do a crime. So the crime refers to the actual user but it is done by other.

Solution:

- Use Mobile tracker system into the smart phone device.
- Use start-up password, so without entering password other cannot use that device.
- If device is GPS enabled then start GPS facility into device. By this the location of the device can be detected.

2.2.1.2. SIM Duplication

SIM duplication refers to make a duplication of SIM card which have same number. So the two cards have a same identity number.

Solution:

- SIM card duplication is easily track from the registration details of that particular SIM identity number.

2.2.2. Video Pornography

Capture undressed photos or videos using mobile phone camera. Today almost all mobile phone have 2.0 to 15 megapixel camera support. Using this camera mobile user can captures undressed images and pornographic video to harass the person.

Solution:

- Make a utility into the mobile phone camera module which can trace the source and identify it. For that Multimedia Steganography can be used.

2.2.3. Intelligent Threats

Logical threats refer to infect the smart phone with various malwares, call/sms forging, bluejacking, Exploitation and Misconduct, Signal Interception, wireless hacking etc, unlawful activities. The most expectant threats to mobile phones in these areas:

Text messages	Call history
Contacts Video	Documentation
Phone transcriptions	Buffer overflows

Now the threats to those areas are as described:

2.2.3.1. Infecting Device through Malware

Financial gain is perhaps the principal driving force behind mobile malicious code. Viruses can let intruder access passwords or corporate data stored on a smart phone. Various scripting languages are used to write a malicious code, and it could affect devices that support that scripting language. As in example if malicious code made in Java then it could affect all java supported smart phones. Several

recent mobile viruses have been particularly noteworthy.

2.2.3.2. Cabir worm

The well-known 29A Eastern European hacker group creating proof-of-concept viruses sent the first version of the Cabir worm, known as Cabir.A. [5]. Cabir runs on smart phones like Motorola, Nokia, Panasonic, and Sony Ericsson. Cabir can be acquired through a shared infected application or it can replicate through Bluetooth, a short-range, radio based, wireless connectivity technology. The worm arrives on victims' devices as Symbian installation system application-installation file. Target devices display a message asking users if they want to receive a message via Bluetooth and then ask for further confirmation if the application is not digitally signed by an authorized Symbian authority. If the user chooses to receive the file, it installs and then sends itself to other Bluetooth-enabled devices within the technology's 10- meter range. [3]

Solution:

- Use good mobile phone antivirus software. And update with particular time.
- Not receive any unauthorised applications from Bluetooth or internet.
- Malwares which have ability to format or delete the data, to save data from that, make a phone data backup.

2.2.3.3. Bluejacking

Bluejacking - the distribution of unwanted messages over Bluetooth to Bluetooth-enabled devices such as cell phones, smart devices and PDAs sending a contact number information which typically contains a message in the name field (i.e. for bluedating or bluechat) to another bluetooth enabled device via the OBEX protocol. Which also known as Bluetooth Hacking. Most commonly people would change a contact in their phone to something like "I can hack you" and send it as a Vcard to nearby phones. BlueSnarfing on the other hand has a more malicious intent. It is a technique that could be used to copy sensitive data from a victim's phone as well as take complete control of their devices to make calls. This was done by exploiting a security flaw in the Bluetooth standard of earlier phones that has since been corrected.

Solution:

- Switch off Bluetooth if it is not needed.
- Turn the visibility off while Bluetooth is not actively transfer the file.
- Protect your Bluetooth with allowing paring permission, so without pairing no other device can send or receive the files.

2.2.3.4. Call/SMS Forging

SMS Forging is the trick by which intruder can steal the identity of the sender. The working of SMS is explained here. First of all the sender sends the SMS via SMS gateway. The identity of the sender is attached to the SCCP the packer of the SMS. The SMS once reaches the SMS gateway is routed to the destination Gateway and then to the receiver's handset. There are many ways by which we can send SMS to the SMS gateway. One of them is to use internet.

Now the concept of SMS forging lies in changing the SCCP packer which contains the sender information prior delivering to the SMS gateway. The intruder can change the SCCP packet and can send that packet to any of the receiver as a spoofed SMS.

Caller ID Forging the practice of causing the telephone network to display a number on the recipient's caller ID display which is not that of the actual originating station; the term is commonly used to describe situations in which the motivation is considered nefarious by the speaker. Just as e-mail spoofing can make it appear that a message came from any e-mail address the sender chooses, caller ID forging can make a call appear to have come from any phone number the caller wishes. Because people are prone to assume a call is coming from the number (and hence, the associated person, or persons), this can call the service's value into question.

To use a typical service, a customer pays in advance for a PIN allowing them to make a call for a certain amount of minutes. To begin, the customer dials from any phone the toll free number given to them by the company and enters their PIN. They are then asked to enter the number they wish to call and the number they wish to appear on the caller ID. Once the "customer" selects the options, the call is then bridged and the person on the other end assumes someone else is calling them.

Many Caller ID forging service providers also allow customers to initiate spoofed calls from a web-based interface in addition to calling a toll free number and entering the ten digit number you want to display followed by the ten digit number you want to call. Some providers allow you to enter the name you would like to display along with the spoofed Caller ID number but in most parts of the United States for example, whatever name the local phone company has associated with the spoofed Caller ID number is the name that shows up on the Caller ID display.

Using a web-based spoofing form involves creating an account with a provider, logging in to their website and completing a form. Most companies require the following basic fields:

1: Source number 2: Destination number 3: Caller ID number

Once the user completes this form and clicks a button to initiate the call, the source number is first called. Once the source number line is picked up, the destination is then called and bridged together. Some providers also offer the ability to record calls, change your voice and send SMS text messages.

Solution:

- Not publish the phone number at any web site or unknown person
- Change phone's security settings to allow incoming calls from contacts only. Methods for limiting incoming calls vary widely by phone model.
- Turn off the browser or internet connection when it is not in use.

2.2.3.5. Smishing

SMiShing basically takes a "social engineering" tactic to spam, in that it attempts to take advantage of a subscribers' lack of awareness. This variation of spam does not directly attack handsets like a virus would. The hackers liable for it are financially driven to exploit legal loopholes and the cutting-edge technologies to get grasp of personal data. Recent attacks have included false online dating subscriptions and job offers via SMS, asking users to go to websites to unsubscribe the service.

This is an example of a smishing message in current circulation: "Notice - this is an automated message from (a local credit union), your Debit card has been suspended. To reactivate call urgent at 500-###-####."

Solution:

- Don’t provide any personal information to any website or any phone number.
- SMS Phishing asks for bank account to transfer gifted amount, then don’t provide any account related information to it.
- Don’t even call to given number in that sms, which may track your location.

2.2.3.6. SMS Spamming

Attackers can manipulate smart-phone zombies to send junk or marketing messages through SMS. In the case that the charging model is flat, a compromised smart-phone can spam for “free”; and therefore its owner may not even notice its bad behaviour. Free SMS spamming gives attackers good incentives to compromise smart-phones.

Solution:

- To guard one's smart phone number. One of the biggest sources of SMS spam is number harvesting carried out by Internet sites offering "free" ring tone downloads. In order to facilitate the download, users must provide their phones' numbers; which in

turn are used to send frequent advertising messages to the phone.

- To reduce SMS spamming from unused advertisement, off the advertisement service at telecommunications providers. To off the services ask the customer care.

2.2.4. Non Detectable threats:

Some of the threats shown here are undetectable. Take a look on it.

2.2.4.1. Smart Phone Spy

Smart Phone Spy is undetectable spy software which allows you to secretly record all activities of your Windows Mobile, Symbian OS, Apple iPhone, Apple iPad, Android or Blackberry smart phone. Smart Phone Spy records every SMS and logs every call including phone numbers with durations. All the calls and SMS logs are uploaded to your online account. Smart Phone Spy starts at every boot of your phone, in complete stealth mode.

2.2.4.2. Messaging through Multiple SIM Cards

With the multiple SIM cards send messages in a chunk of sentences or word. As an example if the message like "The terrorist team will reach at location 204 on Thursday 11:00 am." Then send/receive message from various sim card is as like,

SIM 1: The intruder team
SIM 3: Location 204 on Thursday
SIM 2: Will reach at
SIM 4: 11:00 am

If the two from the four SIM cards are traced, then the information traced from that SIM cards is not fruitful. And no idea can make out of it.

3. Communication over call/chatting

If the message passing or question/answer communication happen over call then detect it using call trace and if over chatting then trace its IP and sniff all that packets. But threats are gone worse to detect if the communication happen over both at a time. As in example, Question asked through smart phone and answer is given through chat box. After then Question asked through chat box and answer is given through a talk on smart phone or SMS it.

4. Future scope

To develop a concept which can detect the undetectable mobile phone threats? Make a general awareness to the public related with this crime. Antivirus solution should make up to that extent so dangerous Malware can be detected. Other advance security threats related solution will be developed.

5. Conclusion:

The number of smartphone attacks is raised due to lack of awareness. To reduce that kind of threats general awareness is a basic need. Try to provide anti threats solutions to the users. Make a device which contains various security features. Security standards for smart device should be evaluated.

References:

[1] Neal Leavitt, "Mobile Phones: The Next Frontier for Hackers?"; In: IEEE Computer Society, April 2005 (Vol. 38, No. 4) pp. 20-23.

[2] Kurt Stammberger, "Concern Grows as Vulnerable Devices Proliferate, Smartphones are the Tip of the Iceberg", CISSP, Summer 2010 Device Security Report, Mobile & Smart Device Security 2010; 2010, San Francisco, CA.

[3] Thakur, Roshan; Chourasia, Khyati; and Thakur, Bhupendra; "Data Base Forensics of Mobile Phone", In: The International Journal of Forensic Computer Science – IJoFCS, Volume 7, Number 1, pages: 42-50, ISSN: **1809-9807,** DOI: 10.5769/J201201004.

[4] Simão, André; Sícoli, Fábio; Melo, Laerte; Deus, Flávio; and Sousa Júnior, Rafael; "Acquisition and Analysis of Digital Evidence in Android Smartphones"; In: The International Journal of Forensic Computer Science – IJoFCS, Volume 6, Number 1, pages: 28-43, ISSN: **1809-9807,** DOI: 10.5769/J201101002.

[5] Lallie, Harjinder; and Benford, David; "Challenging the Reliability of iPhone - Geo-tags"; In: The International Journal of Forensic Computer Science – IJoFCS, Volume 6, Number 1, pages: 59-67, ISSN: **1809-9807,** DOI: 10.5769/J201101004.

[6] Kathirvel, Ayyaswamy, and R. Srinivasan; "Double Umpiring System for Ad Hoc Wireless Mobile Network Security"; In: The International Journal of Forensic Computer Science – IJoFCS, Volume 5, Number 1, pages: 22-29, ISSN: **1809-9807,** DOI: 10.5769/J201001003.

[7] Rosa, Antonio; Barboni, Daniel; and Quintiliano, Paulo; "Mobile Positioning Methods used in Location-Based Services in GSM, WCDMA and WLAN Networks"; In: The International Journal of Forensic Computer Science – IJoFCS, Volume 5, Number 1, pages: 51-59; ISSN: **1809-9807,** DOI: 10.5769/J200801005.