Vol. 1, Issue IV, May 2013
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

PREVENTIVE ACTIONS TO EMERGING THREATS IN SMART DEVICES SECURITY

Nilay Mistry[1], H. P. Sanghvi[2], Dr. M. S. Dahiya[3], Dr. J. M. Vyas[4]

[1]Gujarat Forensic Sciences University, Institute of Forensic Science,
Sector: 18/A, Gandhinagar, Gujarat – India.
nilaymistry30@gmail.com[1]

[2]Directorate of Forensic Science, Cyber Forensics Division,
Sector: 18/A, Gandhinagar, Gujarat – India.
hpsanghvi@gmail.com[2]

[3]Gujarat Forensic Sciences University, Institute of Forensic Science,
Sector: 18/A, Gandhinagar, Gujarat – India.
msdahiya49@rediffmail.com[3]

[4]Directorate of Forensic Science,
Sector: 18/A, Gandhinagar, Gujarat – India.

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.*

Keywords: *Threats, Virus, Smartphone Crime, Smart Devices*

1. INTRODUCTION

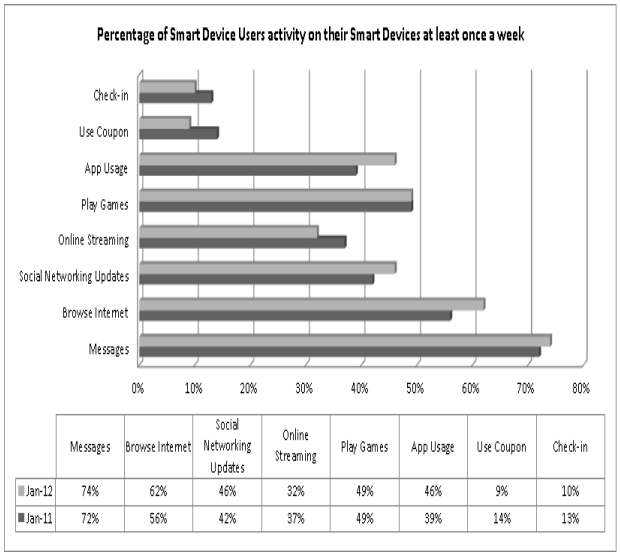
The smart phone and smart phone industry has rapidly developed all across the globe. The days of the phone being used as simply a voice device have outdated. Today each smart phone has become a small PC in the pocket of each person.

Year 2012/13 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 receiving 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, and secure email sending receiving on Internet connectivity based smart phone. Here shown the Smart devices users activity and which kind of facilities are used most by them.

Vol. 1, Issue IV, May 2013
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..



	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 owner's activity [5]

Smart devices security attacks are easy to commit due to application download support from device itself. For an example, Fake Token – 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.[3]

2. SMART DEVICE 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 malwares (infect via messaging services, IP based network traffic, web access, and email links & attachments) have infect in their specific way to the common user on a smart devices. 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]

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 information 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.

3. CLASSIFICATION OF EMERGING THREATS

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

3.1 Physical Threats
3.2 Intelligent Threats
3.3 Non detectable Threats
3.4

To understand the risks behind various types of threats and provide better solutions, categorization of threats is needed [8].

3.1 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. Evan 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.

3.1.1 Smart Device Theft: Physically theft the smart phone device and make a use of that device to do a crime.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS…..

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.

3.1.2 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.

3.1.3 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.

3.2 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:

Table 1: Most expectance threats to mobile devices

Text messages	**Call history**
Contacts Video	**Documentation**
Phone transcriptions	**Buffer overflows**

Now the threats to those areas are as described:

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.[7]

3.2.1 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. [4] 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 and authenticated by an authorized Symbian services. If the user permits that 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 unauthorized 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.

3.2.2 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 blue dating or blue chat) to another blue tooth 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. Blue Snarfing on the other hand has a more malfunctioning intent. That technique could be used to copy sensitive data from a victim's phone as well as take complete control of their devices, like to make calls, change the profiles etc. These kinds of attacks done by exploiting a security loophole in the Bluetooth standard of earlier phones that has since been corrected.

Solution:

- Switch off Bluetooth if it is not needed.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS…..

- 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.

3.2.3 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 send the SMS through SMS gateway.
- The identical information of the sender is attached over SCCP packet builder of the SMS.
- When SMS once reach the SMS gateway is routed to the destination Gateway and then to the receiver's device.
- There are many ways by which one can send SMS to the SMS gateway. In most of the attack internet is used.

Now the concept of SMS forging lies in changing the SCCP packet builder which contains the sender information prior delivering to the SMS gateway. The attacker can change the SCCP packet bulding logic 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. Email Spoofing and Caller ID spoofing is worked on same logic, string maipulation. Caller ID forging is a method through which one can change the caller ID number which appears on the destination phone.

Many Caller ID forging services are web based or and also Over the Air. 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: Who call? 2: To whom call? 3: Manipulated Caller ID
or
*Spoofing Server Number * Caller ID Spoof Number * Destination Number*

(With Area Code and that can happen Over Air i.e. directly from the device no internet connectivity used?)

Once the users filled this form and clicks or call (Over Air) 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 stored contacts only. Use licensed call blocker application.
- Turn off the browser or internet connection when it is not in use.

3.2.4 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 give or publish 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.

3.2.5 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:

- For committing the SMS spamming, number harvesting carried out by Internet sites offering "free" multimedia download. In order to facilitate the download, users must ask to avail all their details like

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS…..

phone number, name, email etc., which are used to send frequent advertising messages to the phone in future. So never ever get "free" things from Internet, it's not actually free.

- SMS spam also gets information from ad wares, which are activate from the smartphone games, which is downloaded and installed via unknown sources.
- To reduce SMS spamming from unused advertisement, off the advertisement service at telecommunications providers. To off the services ask the customer care.

3.3 Non Detectable threats:

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

3.3.1 Smart Phone Spy: Smart Phone Spy is undetectable spy software which allows you to secretly record all activities of your all kinds of smart phones. Smart Phone Spy records every SMS and logs every call including phone numbers with durations. All the call list (Missed Call, Received Calls, Outgoing Calls) and sent, received and drafted SMS log entries, calendar events, notes etc valuable information are uploaded to your online account. Smart Phone Spy start working while device boots. It is hidden process so normally can't be seen at that time, and extremely dangerous factor for privacy.

3.3.2 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.

3.3.3 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] **http://www.ciol.com/Android/Android App/Beware-This-Android-app-steals-bank-passwords/161730/0/**

[2] **http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats#mobile-basics**

[3] **http://defensesystems.com/articles/2012/02/08/cyber-defense-data-in-motion-security.aspx**

[4] **Kaspersky Labs. Viruses move to mobile phones, 2004. http://www.kaspersky.com/news?id=149499226.**

[5] **The user activity on smartphone. http://www.adage.com/**

[6] **Neal Leavitt, "Mobile Phones: The Next Frontier for Hackers?" Published by the IEEE Computer Society, April 2005 (Vol. 38, No. 4) pp. 20-23.**

[7] **Kurt Stammberger, CISSP, summer 2010 Device Security Report, Mobile & Smart Device Security 2010: Concern Grows as Vulnerable Devices Proliferate, Smartphones is the Tip of the Iceberg, 2010, San Francisco, CA.**

[8] **WHITE PAPER, Juniper Networks, Inc. - "Mobile Device Security Emerging Threats, Essential Strategies", 2011.**