Chapter 5

Mobile Phone and Android Forensics

Mobile Hacking – SMS and Call Forging

By using simple mobile handset , hacker hack your cell phone data by using an antenna but condition is that your phone in working mode.

After hacking your phone, they can steal your number and information to misuse by spaying on your call and detect personal information like banking transaction and email username and password.

To avoid this kinds of challenges use strong passwords. If any sensitive activities observed then switch off mobile and time to time upgrade the security software.

Call Spoofing / Forging

Call forging is to spoof caller ID number displayed on the cell phone/landline. It can happen over VoIP(Voice over Internet Protocol). It is a method through which making or forcing telephone network to display incoming call number on the cell phone display with hidden identity. In this case hacker making the victim feel that it is coming from a genuine sources. People attend the call like they are receiving from known user.
After taking advantages of this they says us to enter mobile phone and personal information like bank account number, credit card cvv code etc.
After giving our personal information hacker misuse our information and gain financially and socially.

SMS Forging

In SMS Forging hacker to spoof sender ID from where the message is send over internationally or locally to divert our attention from valid sources of SMS. After this intruder change the content of the SCCP packets and send the same packets to many recipients as a spoofed SMS. Using SMS gateway one user can send bulk SMS to many recipients.

Bluesnarfing

Bluesnarfing refers to the theft of data from mobile phones, PDAs, or similar devices, by making use of the short-range connectivity system called Bluetooth. The new-technology data devices that we use nowadays can get vulnerable to these attacks if certain guidelines are not followed properly.

Unlike olden times, most devices like desktop computers or laptops, cell phones, or PDAs (personal digital assistant) now have a Bluetooth system integrated in them. It helps in interchanging data between multiple devices over shorter distances.

Bluesnarfing can go on to such an extent that the bluesnarfer's device can remain undetected during the course of the fraud. In this case, the culprit's device is included in the trusted devices list (victim's device), and has the rights to access and modify all the data on it.

We may receive connection requests or unsolicited files on our devices at some point or the other and wherein the data of any device is accessed without authority, is called 'BLUESNARFING'.

Majority of the problems arise due to the fact that some devices have a default Bluetooth discoverable mode. Besides this, Bluetooth reachability is within 30 feet or so. Thus, for the attack to happen, the perpetrator must be close to where the victim is.

When a device is bluesnarfed, the perpetrator is able to access all the data. Besides the data, the hacker can make calls, send texts, access the contact list, notes, emails, images, videos, memos, etc. Bluesnarfing is dangerous to a large extent, because the culprit can take complete control over your device, rendering you helpless.

One easy solution to this problem is keeping confidential data on those devices which are not Bluetooth-enabled, because no matter what safety precautions you take, your data is susceptible to threats.Update your device on a regular basis. Make sure your device's Bluetooth is on only when you need it. A constantly running Bluetooth can be one reason for inviting threats to your device.

Mobile Phone Forensics: - The term “mobile devices” encompasses a wide array of gadgets ranging from mobile phones, smartphones, tablets, and GPS units to wearable and PDAs contain a lot of user information. Nowadays, mobile device use is as pervasive as it is helpful, especially in the context of digital forensics, because these small-sized machines amass huge quantities of data on a daily basis, which can be extracted to facilitate the investigation

Evidence that resides on mobile devices

- Incoming, outgoing, missed call history

Phonebook or contact lists

- SMS text, application based, and multimedia messaging content
- Pictures, videos, and audio files and sometimes voicemail messages
- Internet browsing history, content, cookies, search history, analytics information
- To-do lists, notes, calendar entries, ringtones
- Documents, spreadsheets, presentation files and other user-created data
- Passwords, passcodes, swipe codes, user account credentials

- Historical geolocation data, cell phone tower related location data, Wi-Fi connection information
- User dictionary content
- Data from various installed apps
- System files, usage logs, error messages
- Deleted data from all of the above

Forensic Procedures

To get technical and non-technical details of the cell phone evidence analysis and collection, we have to follow guidelines prepared by International Organization on Computer Evidence (IOCE). It includes the procedures/methods for evidence collection, preservation, examination, analysis and report writing on evidence.

Some of the IOCE parameters as follows :

1. Digital Evidence must be handled with all the general forensic and procedural principles.
2. Whatever action or procedures applied on digital evidence, it should not be change evidence irrespective of it's size.

3. Digital Evidence must be handled or access by only trained person with adherence to IOCE guidelines.
4. All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.
5. An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
6. Any agency , which is responsible for seizing, accessing , storing or transferring digital evidence, is responsible for compliance with these principles.

Apart from this, we have to follow guidelines of Association of Chief Police Officers.

a) No action taken by law enforcement agencies or their agents should change data held on a computer or storage media whenever present in court.
b) Whenever necessary, authorised persons can access original data of computer and storage media, in compliance with produce in court and make it more competent.
c) An independent third party should audit trail or other records of all process applied to computer based digital evidence and preserve it properly.
d) The investigator officers have full responsibility for law and guideline adherence to collected evidence.

Files Present in SIM Card Device Data

A SIM card, also known as a subscriber identity module, is a smart card that stores data for GSM cellular telephone subscribers. Such data includes user identity, location and phone number, network authorization data, personal security keys, contact lists and stored text messages.

All of the above data stored in directory structures where Master File(MF) is the root directory and dedicated file(DF) is the subdirectories and elementary file(EF) is the actual files in which the data is stored. Some file can be view without any authentication and important files can be accessed using appropriate ADM code.

SIM Forensics

SIM card Forensics is an essential section of Mobile device forensics. The information that a SIM card can provide the forensic examiner can be crucial to an investigation. Obtaining a SIM card permits a plethora of information, which the suspect has dealt with over the phone to be investigated.

In general, some of this data can help an investigator determine:

- Phone numbers of calls made/received
- Contacts
- SMS details (time/date, recipient, etc.)
- SMS text (the message itself)
- MMS, contacts settings

There are some files which includes the host's network subscriber temporary or permanent identity(i.e. IMSI-TMSI), control channels (i.e. BCCH),subscribers coarse location(i.e. LAI) and the encryption key(i.e. KC)

The File System Organization of a SIM card

The file system of a SIM card is organized in a hierarchical tree structure, as given below:

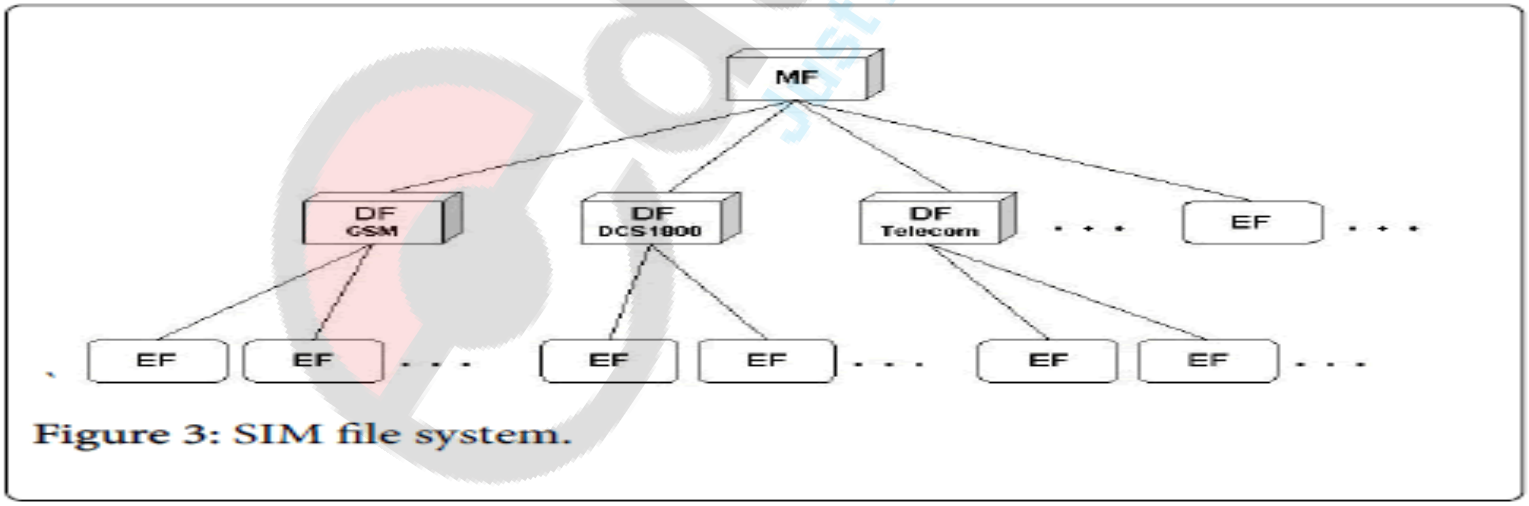

Figure 3: SIM file system.

Master File (MF) – Master file is the root of the file system organization. It contains all the dedicated and elementary files.

Dedicated File (DF) – Dedicated files are subordinate directories to the master file that contain dedicated and elementary files.

Elementary File (EF) – These are files that contain various types of formatted data structures, which can be a sequence of data bytes, a sequence of fixed size records, or a fixed set of fixed size records used cyclically

The Concept of Data Recovery from SIM Cards

SIM cards which are technically smart cards containing an embedded EEPROM memory chip. The EEPROM chip in the smart cards is the same flash memory devices that are the same flash memory devices that are present in pen drives, SSDs, etc. Hence, it is possible to recover data from other electronic **memory chip** devices.

But SIM cards in damaged conditions might become unrecognizable by the SIM extraction device being used. Therefore, the card should be properly cleaned before being subjected to the process of extraction.

Evidential Value of SIM cards

- SIM cards can contain crucial information, for example, messages having login IDs and passwords related to one's bank accounts and social networking sites.
- SIM cards may also contain personal and professional messages, important contact information, call logs, etc.
- Deleted messages can also be recovered from SIM cards.
- Data in SIM cards are not destroyed by heat, flame, dust, soil, moisture, stains or magnetic fields. Hence, environmental conditions have no effect on the data stored in SIM cards.

- Only after going through physical damage a SIM can be rendered unreadable, but scratches and striations do not make the SIM card unreadable
- SIM cards inflicted by stone, hammer or bitten by teeth that create compression marks on the metallic circuit of the card become unreadable.
- Even SIM cards that have become unreadable can be read after replacing the EEPROM chip into a new SIM card or by connecting it to proper probes.
- People should be made aware that SIM cards should not be simply discarded without breaking it into two pieces to make it nearly impossible by a stranger or a criminal to steal private data easily, barely by using a SIM card reader

- SIM cards are vital as forensic evidences as it contains location information and a list of all the network towers it has recently connected to. Call logs of a suspect or a criminal can be of immense value in the proceedings of an investigation.
- In cases of suicide, accidental drowning, road accidents, mass disasters where the mobile device of the unknown victim gets broken or gets switched off due to battery discharge, if the SIM card is taken out and read with a SIM card reader, we can get to know about the victim by extracting information from their SIM card.

Device Data

We identify, preserve and analyze any data in any computer, device or network. Digital device investigations involve the collection, analysis, reporting and presentation of digital evidence stored on hard drives, solid state drives or other storage medium.

Digital forensics is the process that deals with the recovery and investigation of data that is stored on digital devices. It also pertains to the hardware and software tools that experts use to retrieve the data without loss.

Mobile devices can be used to save several types of personal information such as contacts, photos, calendars and notes, SMS and MMS messages. Smartphones may additionally contain video, email, web browsing information, location information, and social networking messages and contacts.

There is growing need for mobile forensics due to several reasons and some of the prominent reasons are:

- Use of mobile phones to store and transmit personal and corporate information
- Use of mobile phones in online transactions
- Law enforcement, criminals and mobile phone devices

There are wide variety of tools exist to extract evidence from mobile devices; no one tool or method can acquire all the evidence from all devices. It is therefore recommended that forensic examiners, especially those wishing to qualify as expert witnesses in court, undergo extensive training in order to understand how each tool and method acquires evidence; how it maintains standards for forensic soundness.

This can be achieved using special software and hardware tools which clone or replicate the contents of memory. In SIM card , the examiner can recover the complete data image in the physical layer.

The entire process in complicated in terms of technical point of view , as data in unstructured format and

They have to be interpreted in some specific file system. Using this tools , we can dump the memory contents is to upload new firmware varities,upgrade,debug and repair the cell phone.

Using Third party unofficial tools, the private entity can change serial number or unlocking the device unethically even mobile in switch off mode or blocked.

The Digital Forensic are exists into Solid State Disk, Magnetic Media, Digital Audio and Video tapes etc.

External Memory Dump

Memory dump primarily identifies a problem or error within the operating system or any installed application within the system. Typically, memory dump provides information about the last state of the programs, applications and system before they were terminated or crashed. This information consists of memory locations, program counters, program state and other related details. It is displayed on-screen and also creates a system log file for viewing/referencing later. After memory dump, the computer is generally unavailable or inaccessible until it's rebooted. Memory dump can also be caused by memory leak, when the system is out of memory and can no longer continue its operations.

Then it is possible to separate and remove the integrated memory circuits by using special precision surface mount device (SMD) soldering/desoldering station. Using right hardware tool, the external memory dump are retrieve from memory of mobile without destructed complete circuit.

Evidence in Memory Card

To enhance the memory storage capacity, the external memory slots are connected to mobile or laptop to store different multimedia files. So user may transfer it's secret information into memory card. Hence investigator must assume the external memory while collecting digital evidences. It also include external network device like Base station and Mobile Network Service Centres database.

Android Device Forensic Fundamental

The concept of Android Forensic consists of technique to extract the most possible data from the device without losing or altering the contents of the device. The data preservation and modification is biggest challenges in Android devices.

There are four primary ways to approach forensics on an Android device. They are:

- SD Card analysis
- Logical acquisition
- Physical acquisition
- Chip-off

1. *SD Card Analysis*

   Nearly every Android device comes with an external SD Card for storing data. Upon receiving and securing an Android device (as you would any other mobile device), an examiner should remove the SD Card and process it in the standard way. The card is formatted with a FAT32 file system.

2. *Logical Analysis*

This technique involves copying a small (~25k) Android Forensics application to the device, running the application, and then removing it from the device. An application, written by via Forensics and distributed for free to law enforcement and government agencies charged with digital forensic responsibilities.

3.Physical Analysis

This technique will provide a forensic image of the various user data partitions. These partitions use the open source file system YAFFS2 (Yet Another Flash File System 2) and is one of the significant challenges with the Android platform.

4.Chip-off

For those with full lab facilities, there is always the option of using chip-off techniques on the NAND memory.

5. RAM memory consists of password,encryption keys,username,application data,data from system process and services.

Procedure for Handling an Android Device

The procedure have five steps:

1. Indentifying
2. Preserving
3. Acquiring
4. Analyzing
5. Reporting.

Above steps description as same as computer digital forensics.

While conducting Android Forensics following points must considered.

1. Chain of custody
2. Detailed notes and final reports
3. Validation of results by different tools or examiners
4. Facts or opinion based testimony

Principle of Android Device Forensics

1. No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
2. Those person collecting original digital forensic, must be competent and well trained.
3. Audit of digital contents should done by third party and preserve in original format.
4. The person in charge of the investigation has overall responsibility for ensuring that law and these principles are adhered to,

Imaging Android USB Mass Storage Devices

1. Attaching the devices by the UMS (USB Mass Storage) interface to the forensic workstation and using appropriate tool.
2. Acquiring the image uses DD on the Android device using ADB port.

Logical Data Acquisition

Data Acquisition is based on the extraction of file system of allocated data over Android Files.

1. ADB pull : This technique relies on the adb pull command which copies parts of the file system to the forensic workstation for further analysis.

2. Backup analysis : This technique relies on examining the backup data found in the SD card or in the cloud.

3. AFLogical : This is a free application developed by viaForensic, which uses Content Providers to extract data.

Physical Data Acquisition

Using this technique physical image of the devices to produces irrespective of if files are deleted.

1. Hardware based :

a) JTAG : This is a technique that uses test access ports of the printed circuit boards for wiring & testing.

b) Chip-off : This is most destructive of all. Once pulled out the chip usually cannot be put back.

2. Software based : AFPhysical : This technqiue was developed by viaForensics