ISSN 2278-7763

# DETECTING AND AUTOMATED REPORTING OF CHANGE IN IMEI NUMBER

**Mayank Sahni, Guru Gobind Singh Indraprastha University**

**Guru Gobind Singh Indraprastha University Sector - 16C Dwarka Delhi - 110078, India**.
Email: info@mayanksahni.com

## ABSTRACT

With the rapid growth of GSM telecommunication, special requirements arise in digital forensics to identify mobile phones operating in a GSM network. The International Mobile Equipment Identity number uniquely identifies an individual mobile station. Though IMEI number was designed to uniquely identify mobile device, hackers have invented methods to change IMEI number.This has increased IMEI scams bringing loss to data and property .Thus it is important to stop such thefts. This paper presents brief about IMEI number and GSM networks for which it is designed. Paper also list various methods of changing IMEI number. At the end it also states a solution which can avoid changing IMEI number.

**Keywords :** GSM, IMEI, IMEI database, user agent

## 1 INTRODUCTION

While smartphones has provided us convenience to do tasks we normally would do on our computers like email, shopping, and banking, but on the other side, it has also brought another way for criminals to try and target us. The International Mobile Equipment Identity number uniquely identifies an individual mobile station. The IMEI is unique to every ME (Mobile Equipment) and thereby provides a means for controlling access to GSM networks based on ME types or individual units. As IMEI number is a unique number allocated to every mobile equipment, so it comprises of various security concerns too. Various illegal activities that are carried out involves mobile equipment devices too. And mobile devices plays the most important role in tracking down such culprits. So in these cases culprits change the IMEI number of the mobile devices and make them untraceable to the security agencies.

One of such most comman crime is the IMEI and SIM scams that are designed to steal money. IMEI scams happen when one use there mobile browser to bank online. The malicious site asks to enter IMEI number. Once the IMEI number is obtained by the hacker, they call respective carrier and report the phone missing and then have a new SIM card sent to them. Now the hacker is armed with what equates to a cloned phone, and when bank sends a text verification, the cloned phone gets the text and now the hacker can get into bank account. . Hence, attackers can exploit IMEI and other identifier's information to perform any malicious behaviour in smartphone which seriously affect the valid mobile owners.
There are other ways also to execute such crimes, Four smartphone identifiers are individually phone number, International Mobile Equipment Identity number (lMEI) , International Mobile Subscriber Identity (IMSI) and SIM Card Serial Number (lCCID). In addition, the black market has recorded the consumer's IMEI. When consumer's smartphone was stolen, its IMEI is putted into blacklist. In practice, thieves can alter phone IMEIs to replace blacklisted IMEIs with valid IMEIs. The serious situations on IMEI misuse are track and identify. First, several apps bind the IMEIs as individual request to access network. Otherwise, apps often contain not only IMEls but also phone numbers or other identified information. These behaviors indicate that the IMEI is used as a form of "tracking cookie" which can be tracked by thieves.

## 2 GSM FUNDAMENTALS

A GSM network as opposed to satellite based communication provide land based communication. In GSM there is a base station on ground at a fixed position. The network is run by an operator and can be connected to other networks like public switched networks or other mobile networks using gateways. Figure 1 shows in a GSM network [1].

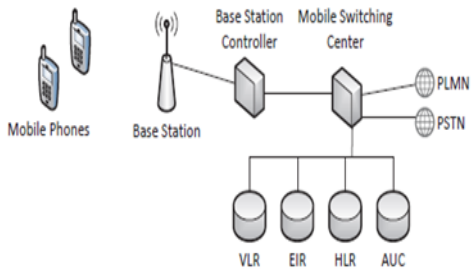


Figure 1: GSM Network Architecture



 

ISSN 2278-7763

Communication of mobile phones to base station is through air interface.geographical locations are divided into fixed cells. For uninterrupted operation, databases like the visitor or home location register store data of subscribers currently using the network. This includes authentication data and identifiers like the IMSI or IMEI. While the IMSI identifies a SIM module with the corresponding contract between a subscriber and the network operator, the IMEI identifies the mobile phone or a similar device which is able to gain access to a GSM network. The handling of the IMEI depends on the network [3].

## 3 INTERNATIONAL MOBILE EQUIPMENT IDENTITY (IMEI)

Having cell phone or tablet stolen is a serious problem, as it compromises safety and security of individuals. Thanks to the FCC (early '80s), Electronic Serial Numbers were created to give a unique identifiers to mobile devices. Since then, usage of mobile devices has exploded, and the Electronic Serial Number of became the IMEI (International Mobile Equipment Identity) and the MEID (Mobile Equipment ID—a super set of IMEI) of today [2].

The International Mobile Equipment Identity number uniquely identifies an individual mobile station. The IMEI is unique to every ME (Mobile Equipment) and thereby provides a means for controlling access to GSM networks based on ME types or individual units. The IMEI format is being originated by the Mobile Telecommunication Standardisation Authorities. The IMEI is of 15 digits each in the range of 0 to 9 coded as binary coded decimal. Many countries have acknowledged the use of the IMEI in reducing the effect of mobile phone theft. For example, in the United Kingdom, under the Mobile Telephones (Re-programming) Act, changing the IMEI of a phone, or possessing equipment that can change it, is considered an offence under some circumstance [4].

IMEI number is structured by the BABT. It has 15 decimal digits. Actualy it has 14 digits plus a check digit. The structure of the IMEI is specified in 3GPP TS 23.003. First 8 digits of IMEI number are TAC (Type Allocation Code) which will give you the mobile phone brand and model. Other 7 digits are defined by manufacturer (6 are serial number and 1 is check digit). From 2004, the format of the IMEI is

AA BBBBBB CCCCCC D [5].

**TAC SERIAL CHECK DIGIT**

AA BBBBBB CCCCCC D

The motto behind this was if a phone, iPad, or other mobile device is stolen, carriers in some countries can blacklist the IMEI or MEID so that the thief cannot use the phone in any capacity, also, if a police complaint is filed some police forces will require the IMEI number in addition to the phone model for the complaint. Some police forces will add the IMEI number to a stolen devices database and, if recovered from stolen property, they could be able to return it to owner [6] [7].

## 4 CITATIONS

IJOART style is to not citations in individual brackets, followed by a comma, e.g. "[1], [5]" (as opposed to the more common "[1, 5]" form.) Citation ranges should be formatted as follows: [1], [2], [3], [4] (as opposed to [1]-[4], which is not IJOART style). When citing a section in a book, please give the relevant page numbers [2]. In sentences, refer simply to the reference number, as in [3]. Do not use "Ref. [3]" or "reference [3]" At the beginning of a sentence use the author names instead of "Reference [3]," e.g., "Smith and Smith [3] show ...." Please note that references will be formatted by IJOART production staff in the same order provided by the author.

### 3.1 HOW TO FIND IMEI NUMBER ON MOBILE DEVICE

There are various methods to find IMEI number of a particular mobile device, these method depends on phone to phone but some standard methods are

1. Most phones have a very simple key-in method to retrieve IMEI/MEID numbers, enter a 5-digit string—*#06#—and the number will be displayed on phone.
2. Remove the back cover Look in the empty battery slot for a white label noting the IMEI
3. For Androids From the home screen, press menu, then Settings, then about phone, and then Status. Your IMEI (or IMSI) will be located on the resulting screen.
4. IMEI is also printed on mobile phone bill.

Width.

### 3.2 CHANGING IMEI

There are different unethical reasons for IMEI changing:

1. To delete tracks about stolen or lost phone (this reason is used mostly)
2. To delete tracks about phone manufacturer and model
3. For researching
4. Other reasons

Changing IMEI number is problematic in most countries, because it is in conflict with the law. With older phones it was easier than with new phones because new phones have better security and also one time programmable chips.

One method is just enter this code in dialler: - *#7465625# or * # * # 3646633 # * # *. Now Tap on Call pad or connectivity option or you have to slide the screen. Just Look for CDS information option radio information can be seen there and after tapping on it. If phone is dual sim android then one can see TWO option select any one. Now put IMEI no in this manner: -"AT +EGMR=1,7,"IMEI_1" and "AT +EGMR=1,10,"IMEI_2" (replace IMEI_1 and IMEI_2 with your IMEI no) and tap on send command button. *For Example: - "AT =EGMR=1, 7"9100XXXXXXXXXXX".*

Also there are now software available that can change IMEI number.

A hardware approach to changing IMEI number is connecting resistors to terminals of mobile PCB to bypass the circuit protecting the write access of IMEI number.

## 4 SOLUTION TO STOP CHANGE IN IMEI

Solution for all kind of IMEI theft have two requirements:

 

ISSN 2278-7763

1. Database at manufacturer side that records IMEI number with corresponding fingerprint
2. Fingerprints are a way to uniquely identify individual eg. $(BRAND)/$(PRODUCT)/$(DEVICE)/$(BOARD):$(VERSION.RELEASE)/$(ID)/$(VERSION.INCREMENTAL):$(TYPE)/$(TAGS)

Now what happens is when phone is booted IMEI number goes to network process and it register this with simid, so if a phone is stolen and someone changes its sim card it can never be tracked. Solution is when phone is booted IMEI no goes also to manufacturer and manufacturer checks in its database whether or not this IMEI belongs to its database if yes it returns a true otherwise false, at same time with IMEI database also stores fingerprint .Next step is manufacturer request for fingerprint of use and if finger print matches phone is successfully booted otherwise not. Longer the fingerprints are better the security is.

## 4 Conclusion

Though this solution is not able to stop IMEI theft hundred percent but it is able do do so to a great extent. It could be understand in this way that suppose attacker is abel to get "Brand" correct,then he need to guess matching "product", if he is abel to get both correct then he needs to guess "device" correct and so on. Thus security of this method depends on length of fingerprint.



## References

[1] Forensic identification of GSM mobile phones by Jakob Hasse, Thomas Gloe and Martin Beck. (http://dl.acm.org/citation.cfm?id=2482529)
[2] A survey of mobile malware in the wild by Adrienne Porter Felt, Matthew Finifter, Erika Chin, Steven Hanna, and David Wagner. (http://dl.acm.org/citation.cfm?doid=2046614.2046618)
[3] iClarified. How to change your iPhone IMEI with ZiPhone (Windows). (http://www.iClarified.com/entry/index.php?enid=657)
[4] W. Enck, P. Gilbert, B. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth. TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones. In OSDI, 2010.
[5] ANDROID PRIVACY by Te-En Wei, Albert B. Jeng, Hahn-Ming Lee, Chih-How Chen andChin-Wei-Tien.(https://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6359654&pageNumber%3D137050)
[6] http://www.berryreview.com/wp-content/uploads/2009/02/blackberrytool.jpg
[7]http://www.zopomobileshop.com/zopo-rom/wp-content/uploads/2012/06/how_to_change_zopo_imei_number.png
[8] http://i-cdn.phonearena.com/images/articles/68386-image/verizon-samsung--galaxy-s-iii-I535VRALHD-ROM-ODIN.jpg

 