Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.527 – 533

RESEARCH ARTICLE

Vulnerability Detection of International Mobile Equipment Identity Number of Smartphone and Automated Reporting of Changed IMEI Number

Krishan Kumar[1]

Department of Comp. Sci&Engg.

GNDU, Amritsar, Punjab, INDIA

Er.krishankumar4014@gmail.com

Prabhpreet Kaur[2]

Department of Comp. Sci&Engg.

GNDU, Amritsar, Punjab, INDIA

Prabhsince1985@yahoo.co.in

Abstract: ***With the advancement's in the mobile technology and continue reduction in the cost of mobile hardware mobile devices had reached in hand of around 80 % of people on the world. The Unique international mobile equipment identity (IMEI) number uniquely identifies each mobile in world. As IMEI number was designed to uniquely identify an individual mobile device, hackers have designed various methods to change the IMEI number of mobile devices so that lost or stolen mobile devices doesn't located by the securities agencies, causing the IMEI scams which had brought loss of data and property. Various hardware flashers devices and software tools are invented designed by the hackers which are easily available on internet. Thus it is important to stop and prevent such theft. To prevent such attacks some methods are presented in this paper. This paper presents brief about the IMEI number and structure of GSM networks. This paper also list out the various methods of changing the IMEI number, software tools are used for changing the IMEI number of various mobile brands. At the last some methods are proposed which if implemented will help in prevention of Change of IMEI and locating the lost or stolen devices across a country.***

Keywords: GSM, IMEI, IMSI, Smartphone

1. Introduction

A smart phone is a mobile phone with an operating system [1][2][3] capable of doing task which are not feasible in simple mobile phone. It has provided us convenience to do task we normally would do on our computer like email, shopping and banking as well as providing the various way for entertaining like gaming, watching videos and movie and the social media which has brought people near to each other and increased the communication among the people. But contrary, it has brought another way for criminals to try and target the people for their illegal benefits.
The International Mobile Equipment Identity (IMEI) number is used to uniquely identify 3GPP[1] (i.e., GSM, UMTS and LTE) and iDEN[2] mobiles phones, as well as some satellite phones. The IMEI number is used by wireless network operator (GSM network) to identify valid devices over the network and to stop the stolen phone from accessing network IMEI number is put on Blacklist by network operator. The IMEI number of the mobile is used only for identification of the device over the wireless network and subscriber has only semi-permanent relation to the IMEI number. But to identify subscriber, an IMSI number, stored on SIM card is used that can be transferred to any handset. As each mobile has the IMEI number which is unique for every mobile in world, it also comprises of various security concerns too. Lots of illegal activities that are carried out involve mobile equipment devices too and mobile devices play the most important role in tracking down such culprits. So in these cases most of the times culprits change the IMEI number of the mobile devices and make them untraceable to the security agencies.

One of such common crime is the IMEI and SIM scams that are designed to steal money from the subscriber. Most of the times, IMEI scams happen when someone using mobile browser to bank online. The malevolent site asks to enter IMEI number of handset. As the hacker obtained IMEI number, they call respective carrier and report the phone is missing and they have new SIM card sent to them. Now the hacker is armed with that equates to a cloned phone, and when bank sends a text verification code to the owner, then actually it received by the cloned phone and hacker gets the bank account details. Hence, attackers can exploit IMEI and other identifier's information to perform ant malicious behavior in smart phone which seriously affect the valid mobile owners. There are other ways also found to execute such crimes through International mobile equipment identity number (IMEI), international mobile subscriber identity(IMSI) and SIM card serial Number (ICCID) [4]. Whenever the consumer's smartphone was stolen, and the time it reached in the black market, IMEI number of smartphone is changed and software is manipulated with the help of available hardware flashers and software tools. In Consequence, law enforcement agencies focus on monitoring the SIM identifier IMSI, which can be changed easily by switching SIM cards [5]. In practice, thieves can alter phone IMEIs to replace blacklisted IMEIs with valid IMEIs with the help of hardware flasher and software tools available on the internet.

The remainder of the paper is structured as follows. In Section 2, we introduce the details of a GSM network detailing the physical layer air interface. In Section 3 describes about the INTERNATIONALMOBILE EQUIPMENT IDENTITY (IMEI), attacks on IMEIs [1]and techniques/methods used in changing the IMEI. Section 4 describes the tools available on internet for changing the IMEIs. Section 5 represents some method to prevent the change of IMEI number and locating the lost or stolen mobiles. Section 6 Discuss about the studies and section 7 provide the conclusion of the paper.

[1] 3GPPis the 3rd Generation Partnership Project (3GPP) is a collaboration between groups of tele-communications associations.

[2] iDENIntegrated Digital Enhanced Network is a mobile telecommunications technology, developed byMotorola.

[3] The British Approvals Board for Telecommunications (BABT) is a telecommunications certification body

2. GSM Fundamentals

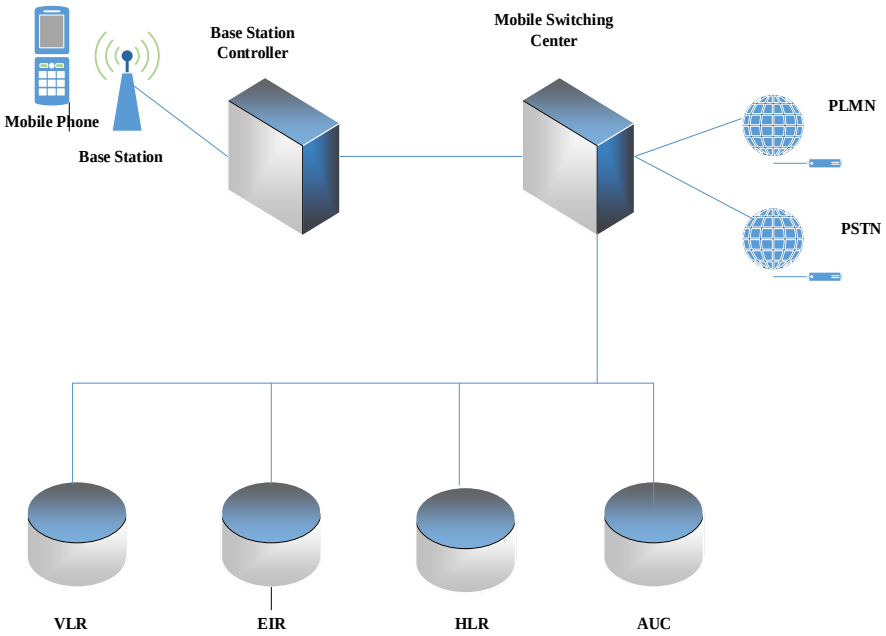

Figure 1: GSM Network structure

A GSM network provides land based communication in contrary to satellite based systems where a base Station relies on ground at 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 the gateways. Figure 1 shows an overview of the entities in a GSM network [5]. The mobiles phones communicate with base station over the air using the Um protocols. The base station provides the RF link in a fixed geographical location, known as the cell [5]. For Uninterrupted operation, database like visitor or home location register store data of subscriber 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 [5]

2. International Mobile Equipment Identity (IMEI)

Having smartphone or tablet stolen is a serious problem, as it compromises to individual privacy and security. So electronic serial numbers were created to give unique identification to mobile devices known as International Mobile equipment Identity (IMEI) and the MEID (Mobile Equipment ID-a super set of IMEI) of today[6]. IMEI is unique to every ME (mobile equipment) and uniquely identifies an individual mobile station. The IMEI format is given by Telecommunication standardization authorities and structured by the BABT[3] and structure of IMEI is specified in 3GPP TS 23.003.

2.1. Structure of IMEI and IMEISV (IMEI Software version): The IMEI (15 decimal digits: 14 digits plus a check digit) or IMEISV (16 digits) includes information on the origin, model and serial number of the device. The model and mobile phone brand is represented by initial 8 digit portion of the IMEI/SV, Known as Type Allocation Code (TAC) and 7 remaining digits are defined by manufacturer (6 are serial number and I is check digit). From 2004, the format of the IMEI is **AA-BBBBBB-CCCCCC-D**[7].

TAC SERIAL CHECK DIGIT
AA BBBBBB CCCCCC D

The format of IMEISV consists of an additional two digits for the Software Version Number (SVN), making the format **AA-BBBBBB-CCCCCC-EE [**7].

TAC SERIAL SVN
AA BBBBBB CCCCCC EE

Now suppose if a phone or other mobile device got stolen by the thief, carriers in some countries can blacklist the IMEI or MEID of the mobile or device so that thief cannot use the phone and if police complaint is filed some police forces will require the IMEI number in addition to the phone model for the compliant. In order to locate the IMEI chip remove the battery and frame of mobile and chip should place in front of the SIM card. This chip is known as RX**12** and it's the only one where's written "RX12".

2.2 Methods of Finding IMEI Number on Mobile Device

To find out the IMEI Number of mobile device various methods are available varies from device to device but some standards methods are

(i).Enter a 5-digit string--*#06# on dial pad and the number will be displayed.
(ii).By removing the battery cover and looking at the empty battery slot for a label noting the IMEI.
(iii).For android from Home screen, press menu, then setting, then about phone and then status. IMEI will be located on the resulting screen.
(iv).IMEI is also printed on mobile phone covering box and bill.

2.3 Reason for Changing IMEI of Mobile Phone

Due to several unethical reasons IMEI of mobile is changed. Some of them are listed below:

(i).To deletes the tracking record of stolen or lost phone. It is one of the most preferable reasons for changing the IMEI of mobile.
(ii).To deletes the tracks about the manufacturer and model.
(iii).For researching.
(iv).When person has bought phone but the IMEI is blacklisted and he/she can't call with the phone.

2.4 Methods of changing the IMEIs of Mobile

Changing IMEI number is illegal in most countries, because it is conflict with the law. But in real government is fighting against anonymity. There is lots of information available on the internet, in the form of blog, tutorials, and videos, who are teaching to change the IMEI but it's against the law in almost in every country and in some countries it is criminal offense. But on contrary part sometimes mobile get started giving error Bad IMEI and this is due to that the device has been flagged as stolen and blacklisted from cell network. In these types of cases mobile companies has to change to IMEI number of mobile phones.

IMEIs of mobile phone are either Hardware based or Software based. So there are two methods found in black market for changing the IMEIs of mobile phones:

(i)**Hardware-based**: by replacing the RX12 chip in mobile with an old phone.
(ii)**Software-Based:** to change IMEIs of mobile various tools and hardware flashers are used in Black market. But generalized method to change IMEIs of most of the android smartphone is as:

A simple method is presented to change IMEI [8] number on **Single-SIM based Android phones** using Terminal Emulator.

(i). Downloading and installing the Terminal Emulator to Android phone.
(ii).To get the Super User access, open it, type SU and press enter key to gain Superuser access.
(iii)Then type this command and press enter key: **echo AT+EGMR=1,7,"IMEI_NUMBER">/dev/pttycmd1** or **echo AT +EGMR=1*7*IMEI_1 >/dev/pttycmd1**For**Dual-SIM Android phones**
Type this command: **echo AT +EGMR=1,10, "IMEI_NUMBER" >/dev/pttycmd1**

3. Mobile Chipset Prone to IMEIs change Attacks and tools used for Changing IMEIs

According to IDC [9] research India is fastest growing market in Asia-Pacific where Samsung leads the smartphone market with 24 % share, followed by Micromax 20%, Lava and Karbonn 8%, Motorola 5%, Apple and Nokia and Worldwide major market share 82.3 % [9] is taken by Android OS. Most of the Androids devices if gets lost or stolen by thieves, when they reached to Black market their IMEIs number is changed with available software tools and hardware fleshers without much problems.
Even some of the Apple iphone [10] is also prone to this attack and IMEIs could be changed with tools (e.g. Ziphone [10]).Almost any mobile belongs to any brand and OS, their IMEIs are changeable with software or Hardware tool support. As a result of this, there is huge loss in terms of money as well as important information and data.

Table 1 below list out the tools used for changing the IMEI's of smartphone based on chipsets of various chipset manufacturer. Most of the tools are available on internet free of cost and some are paid tools. So whenever someone phone gets stolen or lost, IMEIs could be changed by Bad guys as a result it become very difficult for police to trace the thieves. But in some cases, when someone having Bad IMEIs problem with mobile, it is not illegal to change IMEI number of the mobiles.

S. No	Chipset manufacturer	Tools Used In changing the IMEI's	Chipset used by Mobile phone Manufacturer
1	MediaTek (MTK)	MTK Droid Root and Tools,MobileUncletool,SP flash tool,SigmaKey,	Samsung, HTC, LG ,Motorola,Micromax,Lava,Lenavo, Panasonic etc.
2	QualComm Snapdragon	NV-items_Reader_Writer_tool. Sigmakey	Samsung, NOKIA, HTC,LG,Lenavo,Xiomi, Micromax etc.
3	Broadcom	Sigmakey, Repair 3G tool,BrcmFlashTool_V2.0.7.0, MultiFun Tool Setup	Samsung, Lava,Karbonn,Micromax etc.
4	Apple A4,A5,A6	Ziphone	Apple iphone, ipad

Table 1: listing the Software tools used for changing IMEI number of Various Branded Mobiles

4. Solution to prevent the change of IMEI and locating the Lost or Stolen Mobile

In order to prevent the change of IMEI number of mobile and to locate the lost or stolen mobiles some assumptions are made.

i).Mobile handset manufacturer companies allocate IMEI number to each mobile based on the Country. It will help in locating the mobiles easily across the world. To do so first there is need to change the basic structure of IMEI and need to add extra bit for storing the country-wise information.

ii). Today every smartphone is equipped with GPS System on board as IMEI number, if Unique Id number is given to each GPS system embedded on chipset board it will help in locating the lost or stolen device.

iii). On the basis of two above Ideas if a direct mapping is drawn between GPS and IMEI number such that a checksum is calculated based on these two Unique Number and this calculated checksum could be stored on some

register (one time programmable) which having embedded program, who check the integrity of checksum and report an error if either the IMEI number or GPS Id is changed.

iv). Centralized database at each GSM operator having mapped IMEI number and GPS Id in its database and blacklist of IMEI number.

v) Database at manufacturer side that records IMEI number with corresponding fingerprint.

Case-I: Suppose someone mobile has been stolen or lost and other person is using the stolen or lost phone illegally without changing IMEI number.

In this scenario, if the person who will be using the phone with new SIM number then he can be easily traced and located with help of network operator, If any police complaint has been fired. Suppose person is using phone without SIM card then GPS id will be helpful in locating the position of stolen or lost phone.

Case-II Hacker/Cracker has been trying to changed IMEI number.

In this scenario, if Hacker/Cracker have changed the IMEI number, but special register(One time Programmable) when calculate the checksum with newly entered IMEI number found the mismatch of checksum then it will start giving error and mobile will become useless.

Case III Hacker/Cracker will be Successful in Changing the IMEI number and disabling the checking Program.

In this scenario, when someone using the phone with new SIM number and its IMEI number goes to network Operator. As the network operator having the Data Base of IMEI number and GPS id, blacklist of IMEI number and corresponding GPS Id, now when network operator check the IMEI number with corresponding GPS Id and found the mismatch. From this can be concluded that IMEI number of that mobile had been changed. Further if who's mobile is lost or stolen fired a police complaint, then IMEI number of mobile is put on blacklist database which reside at every network operator. when network operator check the new IMEI number in blacklist database and it doesn't matches with IMEI number but the corresponding GPS id got matched then network operator gives the SIM number and all the necessary information to the police so that legal action can be taken against the person.

5. Discussion

As IMEIs number is used by the GSM network for identification of valid devices and helpful in stopping a stolen phone to access the wireless network. The IMEI number is used only for the purpose of identification of the device and subscriber has no permanent relation or semi-permanent relation with the device IMEIs.
In this study, we found that whenever stolen or lost mobile had reached to the black market, important information of mobile related to owner of mobile, is deleted and IMEIs of mobile, which is used to trace the mobiles is replaced by another IMEI number using the hardware as well as software tools. As a result it become impossible or have much little chances to get back the stolen or lost mobile, even if someone have lodged FIR in police. But in some cases when User have bought new mobile phone, after some time due to some reason if mobile started given bad IMEI problem. In this type of cases where IMEIs blacked listed by company it become legal to get replaced the IMEI number with valid new one. It is also found that mobile phone having Software Based IMEIs Number which is true in case of the smart phone, are much prone to this attacks because due to availability of software tools(as listed above in table) on the internet . Many websites and blog are providing information regarding this without any cost. But in case of hardware based IMEIs which involve changing the RX12 chip or Hardware flasher devices for changing the IMEIs number of mobile comparatively difficult. Some countries like United Kingdom having strong enforcement of law, declared under Mobile Telephones(Re-programming) Act, where to change the IMEI number of a phone, or possession of the 0equipment that can change it, is declared an offence under some circumstance [12]. According to iTHEFT news [14] in America lots of people are involved in this and stealing iphones, smuggled to

Hong-Kong, sold at high prices in Hong-Kong and other Asian Countries But in most of the developing countries stolen mobiles are brought from others countries and their IMEI number is replaced by valid one by paying some amount and it is also happening in some developed countries. Hackers and people working in black market are always one step ahead in developing software tools and hardware flashers for changing the IMEI number of mobiles phone.

6. Conclusions

During the study it is found that not much amount of literature is available related to detection and change of IMEI number. Information presented here collected from the black market and people working in black market through self-review. There is need for strict law enforcement in every country and Also there is need for mutual corporations between the countries is required because when Once the stolen phone gets smuggled to the overseas, it become virtually impossible to track a phone back to the person who committed the crime. There is need to conduct advance research and upgrading the structure of IMEIs to Include the new feature, so that protection of mobile is done in better way and it should be provide protection and better security mechanism from mobile theft. The proposed method if implemented greatly help the law enforcement agencies to keep track of lost or stolen mobile device and locating them. So that the hacker or bad guys could not take the benefits of other and legal action can be taken against them by locating with new methods. There is also need to conduct advance research in this field and motivating the researcher in the telecommunication field.

References

[1]"Smartphone". *Phone Scoop*. Last accessed 2015-02-15.
[2]"Feature Phone". *Phone Scoop*. Last accessed 2015-02-15.
[3] Andrew Nusca (20 August 2009). "Smartphone vs. feature phone arms race heats up; which did you buy?".ZDNet.Last accessed2015-02-15.
[4]MayankSahni,"DETECTING AND AUTOMATED REPORTING OF CHANGE IN IMEI NUMBER", International Journal of Advancements in Research & Technology, Volume 3-, Issue 5, May-2014
[5]JakobHasse, Thomas Gloe and Martin Beck"Forensic identification of GSM mobile phones"Pages 131-140,ACM New York, USA 2013
[6] Adrienne Porter Felt, Mat-thewFinifter, Erika Chin, Steven Hanna, and David Wagner. "A survey of mobile malware in the wild"Pages 3-14 ACM New York, NY, USA2011.
[7]Te-En Wei, Albert B. Jeng, Hahn-Ming Lee, Chih-How Chen andChin-Wei-Tien, "ANDROID PRIVACY",International Conference onMachine Learning and Cybernetics (ICMLC), 2012 (Volume:5)Page(s): 1830 – 1837,IEEE.
[8]http://cabnet-onmobile.blogspot.in/2014/09/full-procedures-on-how-to-change.html . Last accessed 01-02-2015.
[9]http://www.idc.com/getdoc.jsp?containerId=prUS25282214 Last Accessed 03-02-2015.
[10]http://www.iclarified.com/entry/comments.php?enid=657Last Accessed 03-02-2015.
[11]www.wikipedia.com.Last Accessed 03-02-2015.
[12] Mobile Telephones (Re-programming) Act 2002. Legislation.gov.uk.
[13]http://www.huffingtonpost.com/2013/07/13/smartphone-black-market_n_3510341.html. Last accessed 17.02.2015.
[14]http://www.huffingtonpost.com/news/iphone-theft. Last accessed 17.02.2015.

