Solution for screening the theft handsets and tracking the missing ones

Abdelraheem Mohamed Elkhalifa 1, Abdelrasoul Jabar Alzubaidi 2

1 Transport Network Manager -Sudatel telecom Group Ltd, Sudatel Tower, P.O. Box 11155, Khartoum, Sudan Mobile +249120120087 E-mail Rahimmk@sudatel.sd
2 Electronic Dept- Engineering College –Sudan University for science and Technology Rasoul46@live.com

Abstract : Mobile phone theft has become a growing problem worldwide, with hundreds of thousands of phones reported stolen each year. In many countries, GSM handset theft has become a major factor in rising street crime, particularly among young people. A stolen GSM handset can be reused with a different subscriber's SIM card, possibly in a different mobile network. Upon subscribing to a network and obtaining a legitimate SIM card with subscriber information, the perpetrator will initially buy an inexpensive handset and later steal a better model from another subscriber. The SIM card is then switched and the network operator is unaware that a stolen handset is being used.

The telecommunications industry is working hard to make this crime less attractive to thieves. Screening solutions, along with jointly shared databases of stolen handset numbers, can effectively render a stolen handset useless across all networks. Once the consumer reports the theft to the network operator, it can be cancelled much like a stolen credit card.

The Equipment Identity Register (EIR) is a database employed within mobile networks. The database holds records for 3 types of mobile; namely black, grey and white. Besides, there is also a 4th category i.e. "Unknown". EIR provides an additional level of security which is performed on the mobile equipment itself, as opposed to the mobile subscriber. When a mobile requests services from the network its IMEI (International Mobile Equipment Identity) may be checked against the EIR, to assess which category of mobile it falls under. It is a tool to deny services or track problem equipment.

Keywords : GSM, SIM card, database, EIR, IMEI.

I. INTRODUCTION

Many countries have acknowledged the use of the IMEI in reducing the effect of mobile phone theft. For example, in some countries, 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. IMEI blocking is not the only approach available for combating phone theft. For example, mobile operators in some places are not required by the regulator to implement phone blocking or tracing systems, IMEI-based or other. The regulator has expressed its doubts on the real effectiveness of this kind of system in the context of the
mobile market. Instead, mobile operators are encouraged to take measures such as the immediate suspension of service and the replacement of SIM cards in case of loss or theft.

The existence of a formally allocated IMEI number range for a GSM terminal implies that the terminal is approved or complies with regulatory requirements. When mobile equipment is stolen or lost, the owner can contact their local operator with a request that it should be blocked from the operator's network, and the operator can be expected to do so if required by law in the operator's jurisdiction. If the local operator possesses an Equipment Identity Register (EIR), it then may put the device IMEI into it, and can optionally communicate this to shared registries, such as the Central Equipment Identity Register (CEIR) which blacklists the device. With this blacklisting in place the device becomes unusable on any operator that uses the CEIR, making theft of mobile equipment a useless business proposition, unless for parts. The IMEI number is not supposed to be easy to change, making the CEIR blacklisting effective.

In some countries, such blacklisting is not customary. In 2012, major network companies in the United States, under government pressure, committed to introduce a blacklisting service, but it's not clear whether it will interoperate with the CEIR..It is unclear whether local barring of IMEI has any positive effect as it may result in international smuggling of stolen phones.

II . International Mobile Station Equipment Identity (IMEI)

The IMEI is a number, usually unique, to identify mobile phones, as well as some satellite phones. It is usually found printed inside the battery compartment of the phone, but can also be displayed on-screen on most phones by entering (*#06#) on the dial pad, or alongside other system information in the settings menu on smart phone operating systems.

The IMEI number is used by a GSM network to identify valid devices and therefore can be used for stopping a stolen phone from accessing that network. For example, if a mobile phone is stolen, the owner can call his or her network provider and instruct them to "blacklist" the phone using its IMEI number. This renders the phone useless on that network and sometimes other networks too, whether or not the phone's SIM is changed.

The IMEI is only used for identifying the device and has no permanent or semi-permanent relation to the subscriber. Instead, the subscriber is identified by transmission of an IMSI number, which is stored on a SIM card that can (in theory) be transferred to any handset. However, many network and security features are enabled by knowing the current device being used by a subscriber.
III. Structure of the International Mobile equipment identity (IMEI) and IMEISV(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 origin comprise the initial 8-digit portion of the IMEI/SV, known as the Type Allocation Code (TAC). The remainder of the IMEI is manufacturer-defined, with a Luhn check digit at the end.

As of 2004, the format of the IMEI is AA-BBBBBB-CCCCCC-D, although it may not always be displayed this way. The IMEISV drops the Luhn check digit in favor of an additional two digits for the Software Version Number (SVN), making the format AA-BBBBBB-CCCCCC-EE.

<table>
<thead>
<tr>
<th></th>
<th>AA</th>
<th>BB</th>
<th>BB</th>
<th>BB</th>
<th>CC</th>
<th>CC</th>
<th>CC</th>
<th>D or EE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Old IMEI</td>
<td>TAC</td>
<td>FAC</td>
<td>(Optional) Luhn checksum</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New IMEI</td>
<td>TAC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Old IMEI SV</td>
<td>TAC</td>
<td>FAC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New IMEI SV</td>
<td>TAC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Prior to 2002, the TAC was six digits long and was followed by a two-digit Final Assembly Code (FAC), which was a manufacturer-specific code indicating the location of the device's construction. From January 1, 2003 until that April 1, 2004, the FAC for all phones was 00. After April 1, 2004, the Final Assembly Code ceased to exist and the Type Allocation Code increased to eight digits in length.

In any of the above cases, the first two digits of the TAC are the Reporting Body Identifier, which identifies the GSMA-approved group that allocated the TAC. The RBI numbers are allocated by the Global Decimal Administrator. IMEI numbers being decimal allows them to be distinguished from an MEID, which is hexadecimal and always has (0xA0) or larger as its first two digits.

For example, the old style IMEI code 35-209900-176148-1 or IMEISV code 35-209900-176148-23 tells us the following:

**TAC:** 35-2099 - issued by the BABT (code 35) with the allocation number 2099,

**FAC:** 00 - indicating the phone was made during the transition period when FACs were being removed.

**SNR:** 176148 - uniquely identifying a unit of this model.

**CD:** 1 so it is a GSM Phase 2 or higher.

**SVN:** 23 - The "software version number" identifying the revision of the
software installed on the phone. 99 is reserved.

By contrast, the new style IMEI code 49-015420-323751 has an 8-digit TAC of 49-015420.

The new CDMA Mobile Equipment Identifier (MEID) uses the same basic format as the IMEI.

Check digit computation

The last number of the IMEI is a check digit calculated using the Luhn algorithm. According to the IMEI Allocation and Approval Guidelines, the Check Digit shall be calculated according to Luhn formula (ISO/IEC 7812). The Check Digit is a function of all other digits in the IMEI. The Software Version Number (SVN) of a mobile is not included in the calculation. The purpose of the Check Digit is to help guard against the possibility of incorrect entries to the CEIR and EIR equipment.

The presentation of the Check Digit both electronically and in printed form on the label and packaging is very important. Logistics (using bar-code reader) and EIR/CEIR administration cannot use the Check Digit unless it is printed outside of the packaging, and on the ME IMEI/Type Accreditation label. The check digit is not transmitted over the radio interface, nor is it stored in the EIR database at any point. Therefore, all references to the last three or six digits of an IMEI refer to the actual IMEI number, to which the check digit does not belong.

The check digit is validated in three steps:

1. Starting from the right, double every other digit (e.g., 7 → 14).
2. Sum the digits (e.g., 14 → 1 + 4).
3. Check if the sum is divisible by 10.

Conversely, one can calculate the IMEI by choosing the check digit that would give a sum divisible by 10. For the example IMEI 49015420323751?

| IMEI  | 4 | 9 | 0 | 1 | 5 | 4 | 2 | 0 | 3 | 2 | 3 | 7 | 5 | 1 | ? |
|-------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Double Every Other | 4 | 18 | 0 | 2 | 5 | 8 | 2 | 0 | 3 | 4 | 3 | 14 | 5 | 2 | ? |
| Sum digits | 4 + (8+1) +0+ 2+ 5+ 8 +2 +0+ 3+ 4+ 3+ (1+4) +5 +2 +? =52 |

To make the sum divisible by 10, we set ? = 8, so the IMEI is 490154203237518.
IV. METHODOLOGY

A data base is to be build in the Equipment Identity Register (EIR) so that the 15-digit International Mobile Station Equipment Identity (IMEI) code that is unique to every phone can be blacklisted if the device is reported stolen. Each EIR will be linked to a Central Equipment Identity Register (CEIR), to which the IMEI codes of stolen phones will be forwarded.

All blacklisted IMEI codes would then be stored in the EIRs to render the phones unusable on any network and to block any attempt to reactivate the devices with new SIM cards. Once blocked, the phone cannot ever be reactivated. This can help reduce phone thefts and at the same time, assist the police to identify the thieves or anyone trying to reactivate the device.

CEIR will operate round the clock. It will be responsible for monitoring and generating the IMEI code blacklist. The information will be forwarded to all telcos within 180 minutes of the phones being reported stolen or missing.

V. ALGORITHM

The algorithm in the EIR contains two subroutines for the mobile status. The first subroutine is for blocking the stolen mobiles. The second subroutine is for the missing mobiles. The algorithm is as follows:

Start

Initialization:

… Build a data base in the EIR.

… Insert the IMEI’s for the mobile phones.

… Establish a link with the CEIR.

Mobile stolen or miss report:

… If a mobile stolen is reported then call subroutine mobile blacklist.

… If a mobile miss is reported then call subroutine mobile missing.

Go to mobile stolen or miss report

End

Mobile blacklist:

… Verify the IMEI by checking the check digit.

… If IMEI is incorrect then go to return

… Look up for the IMEI in the data base.

… Put the IMEI in the blacklist.

… Block the mobile set.

Return

Mobile missing:
Verify the IMEI by checking the check digit.

If IMEI is incorrect then go to return

Get the IMEI in the data base.

Put the IMEI in the missing list.

VI. RESULTS

The ultimate result obtained by using the data base in the (EIR) and verifying the (IMEI) includes blocking the activation of the stolen mobile sets and tracking the missing mobile sets.

VII. CONCLUSION

Every mobile phone has a unique serial number. This serial number is the IMEI number. It can normally be found underneath the phones battery. This paper proposes an algorithm for the management of the stolen handsets to render them useless. The algorithm tracks the missed handsets through the missing handsets list. Each time a phone is switched on or attempted to make a call, the network systems check the IMEI number of the handset. At this point the IMEI number of the handset is cross referenced with the Central Equipment Identity Register. If the IMEI number of the handset is on the CEIR then the network will either:
- Refuse to send a signal to the phone (No signal strength at all)
- Or will supply a signal but will not allow any outgoing or incoming calls.

If the IMEI number is on the CEIR then the handset is blacklisted and therefore useless.

References

3. GSM Europe, "GSME proposals regarding mobile theft and IMEI security". 2003-06
5. IMEI Specifications
9. GSM Association, IMEI Allocation and Approval Guidelines, Version 5.0, 2010-09-01, chapter 2.1.5 vs. D.1.6