Mobile Phone Cloning

Sonal[1], Upasna[2]
[1,2]Department of Computer Science & Engineering,
Ganga Institute of Technology and Management,
Kablana, Jhajjar, Haryana, India

***Abstract*— Mobile communication has been most popular from many years, and is major need of todays business and life. It provides most valuable service to its users who are willing to pay a considerable premium over fixed line phone such as landline, to be able to walk and talk freely. Because of its usefulness and importance in business and other normal lifestyle, it is subject to fraud.**

Mobile phone cloning is a technique where the data from one cell phone is transferred into another phone. The other cell phone becomes the exact replicate copy of the original mobile phone like a clone. As a result, while calls can be made from both phones, only the original is billed. Though communication channels are equipped with security algorithms, yet cloners get away with the help of loop holes in systems. So when one gets huge bills, the chances are that the phone is being cloned.

This paper describes about the cell phone cloning with implementation in GSM and CDMA technology phones. It gives an insight into the security mechanism in CDMA and GSM phones along with the loop holes in the systems and discusses on the different ways of preventing this cloning.

Keywords*— *Mobile phone cloning, GSM, CDMA, IMEI, SIM, ESN and MIN, Patagonia.

I. INTRODUCTION

When we look up the dictionary meaning of cloning it states, to create the exact replica or a mirror image of an subject understudy. The idea behind the cloning of mobile communications is simple. Here the object of the exercise is to make calls free of charge. Unfortunately, while such calls might well be free to the caller, no such luck for the genuine renter/end-user. To make a mobilephone call (analogue) the system requires two pieces of information, mobile identification number (MIN) and electronic serial number (ESN), commonly referred to as the 'handshake'. Once the mobilephone network validates these pieces of information, service is allowed. There are a number of ways for fraudsters to obtain such information; for example an unsuspecting mobile-phone user may be called and informed that the engineers are carrying out diagnostic checks of the network[1]. Customer cooperation is then sought, with the customer being directed to the ESN written on a label under the battery compartment. Here obviously the culprit must make a second call to retrieve the information, as the battery must be removed.This information is then input into another mobile, with the result that all calls made by the clone are charged to the original user's account. Unfortunately, here the fraud is aided unwittingly by the carrier who fails to produce an itemized account free of charge.The fraudster may well find himself in clover, should the cloned number belong to a company or a person who fails to check usage. Such a methodology for obtaining handshake information is extremely slow and time consuming. Therefore other resources must be utilized. Here, to speed matters up, scanning devices are deployed.The idea here is to place the scanner near to an underpass or bridge near a motorway.Then as the vehicles pass, those who have established mobile calls in progress, to maintain communication have to re-establish the network connection.This means that the MIN and ESN is forwarded to the network, and as the link is not encrypted, the scanner grabs the salient information. Another alternative is to seek out and to corrupt an employee of a service provider or to steal the customer database containing the handshake information. This information can then be inputted into analogue mobiles and fraudulent calls made.There are parts of the UK where 'dial a clone' is more lucrative than 'dial a pizza' service. Here the cloner rents out the clones for a set fee.

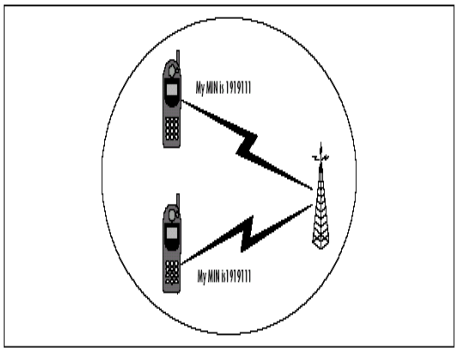

Fig. 1 Mobile Phone Cloning

II. HISTORY OF MOBILE PHONE CLONING

The early 1990s were boom times for eavesdroppers. Any curious teenager with a £100 Tandy Scanner could listen in to nearly any analogue mobile phone call. As a result, Cabinet Ministers, company chiefs and celebrities routinely found their most intimate conversations published in the next day's tabloids Cell phone cloning[1] started with Motorola "bag" phones and reached its peak in the mid 90's with a commonly And Dolly the lamb, cloned from a six-year-old ewe in 1997, available modification for the Motorola "brick" phones, such as the Classic, the Ultra Classic, and the Model 8000.

by a group of researchers at the Roslin Institute in Scotland. While the debate on the ethics of cloning continues, human race, for the first time, are faced with a more tangible and harmful version of cloning and this time it is your cell phone that is the target.

According to media reports, recently the Delhi (India) police arrested a person with 20 cell- phones, a laptop, a SIM scanner, and a writer. The accused was running an exchange illegally wherein he cloned CDMA based cell phones. He used software named Patagonia for the cloning and provided cheap international calls to Indian immigrants in West Asia.

III. TYPES OF MOBILE PHONES

A. GSM Mobile Phones

Global System for Mobile Communications. A digital cellular phone technology based on TDMA GSM phones[2] use a Subscriber Identity Module (SIM) card that contains user account information. Any GSM phone becomes immediately programmed after plugging in the SIM card, thus allowing GSM phones to be easily rented or borrowed. Operators who provide GSM service are Airtel, Reliance, Vodafone, Idea etc.

B. CDMA Mobile Phones

Code Division Multiple Access. A method for transmitting simultaneous signals over a shared portion of the spectrum. There is no Subscriber Identity Module (SIM) card unlike in GSM Operators who provides CDMA service in India are Reliance and Tata Indicom[2].

Both GSM and CDMA handsets are prone to cloning. Technically, it is easier to clone a CDMA handset over a GSM one, though cloning a GSM cell phone is not impossible. There are also Internet sites that provide information on how one could go about hacking into cell-phones.

IV. HOW MOBILE PHONES ARE CLONED

A. Cloning GSM Mobile Phones

GSM handsets, on the contrary, are safer, according to experts. Every GSM phone has a 15 digit electronic serial number (referred to as the IMEI)[3][4]. It is not a particularly secret bit of information and you don't need to take any care to keep it private. The important information is the IMSI, which is stored on the removable SIM card that carries all your subscriber information, roaming database and so on. GSM employs a fairly sophisticated asymmetric-key cryptosystem for over-the-air transmission of subscriber information. Cloning a SIM using information captured over-the-air is therefore difficult, though not impossible. As long as you don't lose your SIM card, you're safe with GSM. GSM carriers use the COMP128 authentication algorithm for the SIM, authentication center and network which make GSM a far secure technology.

GSM networks which are considered to be impregnable can also be hacked. The process is simple: a SIM card is inserted into a reader. After connecting it to the computer using data cables, the card details were transferred into the PC. Then, using freely available encryption software on the Net, the card details can be encrypted on to a blank smart card. The result: A cloned cell phone is ready for misuse.

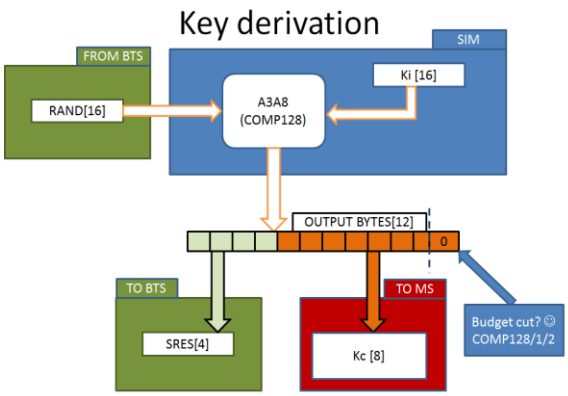

Fig. 2 GSM Cloning

B. Cloning CDMA Mobile Phones

Cellular telephone thieves monitor the radio frequency spectrum and steal the cell phone pair as it is being anonymously registered with a cell site. The technology uses spread-spectrum techniques to share bands with multiple conversations. Subscriber information is also encrypted and transmitted digitally. CDMA[3] handsets are particularly vulnerable to cloning, according to experts. First generation mobile cellular networks allowed fraudsters to pull subscription data (such as ESN and MIN) from the analog air interface and use this data to clone phones. A device called as DDI, Digital Data Interface (which comes in various formats from the more expensive stand-alone box, to a device which interfaces with your 800 MHz capable scanner and a PC) can be used to get pairs by simply making the device mobile and sitting in a busy traffic area (freeway overpass) and collect all the data you need. The stolen ESN and EMIN[5] were then fed into a new CDMA handset, whose existing program was erased with the help of downloaded software. The buyer then programs them into new phones which will have the same number as that of the original subscriber.

But Looking at the recent case, it is quite possible to clone both GSM and CDMA sets. The accused in the Delhi case used software called Patagonia to clone only CDMA phones (Reliance and Tata Indicom). However, there are software packages that can be used to clone even GSM phones (e.g. Airtel, BSNL, Hutch, Idea). In order to clone a GSM phone, knowledge of the International Mobile Equipment Identity (IMEI) or instrument number is sufficient.

V. SOFTWARE FOR MOBILE PHONES CLONING

A Software tool is used for modifying the and configuring the cell phone. The EEPROM chip is replaced of modified with a new chip which will reconfigure ESN (Electronic Serial Number) or IMEI (International Mobile Equipment Identity) and via MIN (Mobile Identification Number) software. When the ESN/MIN pair had changed successfully then an effective clone of the original phone has created.

A. Patagonia

Patagonia is a software available in the market which is used to clone CDMA phone.Using this software a cloner can take over the control of a CDMA[6] phone i.e. cloning of phone. There are other Software's avai;able in the market to clone GSM phone.This software's are easily available in the market.A SIM can be cloned again and again and they can be used at different places.Messages and calls sent by cloned phones can be tracked.However,if the accuses manages to also clone the IMEI number of the handset,for which software's are available,there is no way he can be traced.

Fig. 3 Mobile Cloning Device

VI. SYMPTOMS OF MOBILE PHONE CLONING

1) Frequent wrong number phone calls to your phone, or hang-ups.
2) Difficulty in placing outgoing calls.
3) Difficulty in retrieving voice mail messages.
4) Incoming calls constantly receiving busy signals or wrong numbers. Unusual calls appearing on your phone bills

VII. HOW TO DETECT MOBILE PHONE CLONING IN A NETWORK

There are various communication companies do deploy fraud detection/reduction measures. The aims of which are to identify potential fraudulent activity[7]. Some of these measures are simple for example; the systems look for simultaneous or over lapping calls made by the same mobile number, an impossible event.The exception is informed to an operator for investigation. Here access to calling records takes place, and a decision made concerning the activity. In reality, call barring is applied to the number, inessence only local calls are allowed and the genuine renter is contacted concerning the situation. Also the system may well 'tear down' both numbers and prevent them from making calls. This is a very quick way of ensuring customer contact. Because no one wants to be without service. Then there are the exception reports. Here cash limits are set against each mobile, in consultation with the customer, once this level is reached, only local calls are allowed, and contact is made with the customer. In reality it is only the customer who can confirm the true situation. Obviously, here a degree of trust must exist between the customer and service provider, because the customer's word on usage must be accepted. It is amazing how honest the vast majority of customers are. Once a mobile has been cloned, the carrier often offers the customer the prospect of retaining the existing number, but to migrate free of charge to the digital service. Naturally, this is in addition to an account reduction, no one is expected to pay for unmade calls.

Several countermeasures were taken with varying success. Here are various methods to detect cloned phones on the network:

A. Duplicate Detection

The network sees the same phone in several places at the same time. Reactions include shutting them all off so that the real customer will contact the operator because he lost the service he is paying for, or tearing down connections so that the clone users will switch to another clone but the real user will contact the operator.

B. Velocity Trap

The mobile phone seems to be moving at impossible, or most unlikely speeds. For example, if a call is first made in Helsinki, and five minutes later, another call is made but this time in Tampere, there must be two phones with the same identity on the network.

C. RF (Radio Frequency)

Fingerprinting is originally a military technology. Even nominally identical radio equipment has a distinguishing ``fingerprint'', so the network software stores and compares fingerprints for all the phones that it sees. This way, it will spot the clones with the same identity but different fingerprints.

D. Usage Profiling

Profiles of customers' phone usage are kept, and when discrepancies are noticed, the customer is contacted. Credit card companies use the same method. For example, if a customer normally makes only local network calls but is suddenly placing calls to foreign countries for hours of airtime, it indicates a possible clone.

E. Call counting

Both the phone and the network keep track of calls made with the phone, and should they differ more than the usually allowed one call, service is denied.

F. Pin Codes

Prior to placing a call, the caller unlocks the phone by entering a PIN code and then calls as usual. After the call has been completed, the user locks the phone by entering the PIN code again. Operators may share PIN information to enable safer roaming.

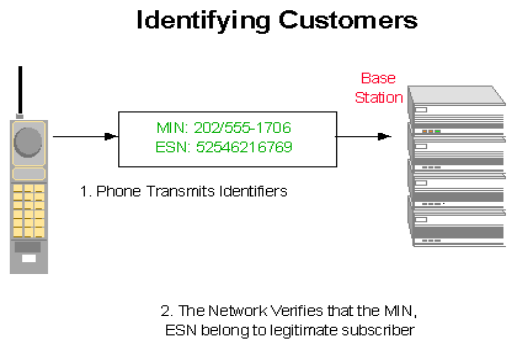

Fig 4:Operators sharing PIN information

VIII. SECURITY FUNDAMENTALS

So far we have considered trust and security in fairly general terms, but at this stage it is necessary to define some trust items that we will examine further in our cellular usag scenarios. Firstly we will introduce some information security fundamentals[7];

A. Call counting

To ensure that entities involved in our trusted solution are legitimate/authentic.

B. Confidentiality

Information, signals, commands or functionality that are restricted to certain authorised entities must be protected from disclosure/discovery by unauthorised entities.

C. Integrity

Critical data and applications code should be protected from modification when in storage, operation or during communications/transactions.

These fundamentals can in turn be underpinned by some practical capabilities;

1) Cryptographic algorithm(s) plus supporting data for authentication/encryption/integrity
2) Secure storage and verification of critical data, with strictaccess controls
3) Secure verification and execution of algorithm(s) and other critical functions
4) Secure communication protocols
5) Controlled operating environment and isolated ‘‘security domains”.

The word ‘‘Secure’’ has been used rather freely in the above points and so we should be clear what it means in this context;

The functionality that embodies our security fundamentals has been correctly designed, implemented and tested to strongly resist the anticipated attacks that may be made against it.

IX. SOME FACTS AND FIGURES

1) Southwestern Bell claims wireless fraud costs the industry $650 million each year in the US. Some federal agents in the US have called phone cloning an especially `popular' crime because it is hard to trace. In one case, more than 1,500 telephone calls were placed in a single day by cellular phone thieves using the number of a single unsuspecting owner[1].
2) A Home Office report in 2002 revealed that in London around 3,000 mobile phones were stolen in one month alone which were used for cell phone cloning.
3) Authorities, in the case, estimated the loss at $3,000 to $4,000 for each number used in cell phone cloning.
4) Ualcomm, which develops CDMA technology globally, says each instance of mobile hacking is different and therefore there is very little an operator can do to prevent hacking[1]. "It's like a virus hitting the computer. The software which is used to hack into the network is different, so operators can only keep upgrading their security firewall as and when the hackers strike," says a Qualcomm executive.

X. FUTURE THREATS

Resolving subscriber fraud can be a long and difficult process for the victim. It may take time to discover that subscriber fraud has occurred and an even longer time to prove that you did not incur the debts. As described in this paper there are many ways to abuse telecommunication system, and to prevent abuse from occurring it is absolutely necessary to check out the weakness and vulnerability of existing telecom systems. If it is planned to invest in new telecom equipment, a security plan should be made and the system tested before being implemented. It is therefore mandatory to keep in mind that a technique which is described as safe today can be the most unsecured technique in the future.

XI. CONCLUSION

To conclude, cell phone communication is one of the most reliable, efficient and widespread. The usage of the system can be changed in either constructive or destructive ways. Unfortunately because of its the security standards it is very easy to break and also takes very less amount of time. Moreover, cloning can be easily increased and also can be implemented easily. Hence, it must be considered that the security which is currently used is not fruitful enough to secure the system in future. So it is very important to verify the working of security system time-to-time and also must change or update it over every month or year once. Preventive steps should be taken by the network provider

and the government the enactment of legislation to prosecute crime related to cellular phones is not viewed as a priority.

Existing cellular system have number of weaknesses, it is not good for us. And it is very harmful of our society, So the security staff must take these cloning kind of problems seriously.

REFERENCES

1. http://www.wikipedia.com
2. IEEE journal for mobile communication
3. http://www.hackinthebox.org/
4. *Security in the GSM network* by Marcin Olawski
5. *CDG Document 138 Version 0.34* CDMA Development Group, 575 Anton Boulevard, Suite 560 Costa Mesa, California 92626
6. http://www.cdmasoftware.com/eng.html
7. Sankaranarayanan ,"Mobile phone cloning", Wireless And Optical Communications Networks (WOCN), 2010 Seventh International Conference in Sept,2010.