Scientific Journal Impact Factor (SJIF) : 3.518
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

MOBILE PHONE CLONING HISTORY WITH PREVENTION TECHNIQUES

Neha Bapna[1], Imran Raza[2] and Shreyansh Shree[3]
[1,2,3] *IIMT College of Engineering, Greater Noida*

Abstract- This paper describes about the cell phone cloning with implementation in GSM and CDMA technology phones. Mobile communication has been readily available for several years, and is major business today. It provides a valuable service to its users who are willing to pay a considerable premium over a fixed line phone, to be able to walk and talk freely. Because of its usefulness and the money involved in the business, it is subject to fraud. Unfortunately, the advance of security standards has not kept pace with the dissemination of mobile communication. Some of the features of mobile.

Keywords- GSM (Global System for Mobile Communications), CDMA (Code Division Multiple Access), ESN (Electronic Security Number), MIN (Mobile Identification Number), SCN (Station Class Mark), DDI (Digital Data Interface).

I. INTRODUCTION

Cell phone cloning is a technique where in secured data from one cell phone is transferred into another phone. The other cell phone becomes the exact replica of the original cell phone like a clone. As a result, while calls can be made from and received by both phones, only the legitimate subscriber is billed as the service provider network does not have a way to differentiate between the legitimate phones and the "cloned" phone. The cloner can set the options to ring his phone when you make a call and you will have no idea that the cloner is listening from his own mobile .He can read text message, phone book entries, look at pictures etc. Also he can dial phone numbers from their phone and a whole lot more. So when one gets huge bills, the chances are that the phone is being cloned. Millions of cell phones users, be it GSM or CDMA, run at risk of having their phones cloned.

II. PROCESS

Cloning is the process of taking the programmed information that is stored in a legitimate mobile phone and illegally programming the identical information into another mobile phone. The culprits clone and hack into your phone using software's that are easily available, once the software is installed they just need the unique IMEI number of the phone and they can digitally imprint these numbers on any of the phone they want. Once this is done they can send messages, make calls to anyone and the person whose phone has been cloned and hacked will be held responsible.

2.1. **For CDMA:** Cloning involved modifying or replacing the EPROM in the phone with a new chip which would allow you to configure an ESN (Electronic serial number) via software. You would also have to change the MIN (Mobile Identification Number). When you had successfully changed the ESN/MIN pair, your phone was an effective clone of the other phone. Cloning required access to ESN and MIN pairs.

2.2 For GSM: Cloning has been shown to be successful on code division multiple access (CDMA) but rare on the Global System for Mobile communication (GSM), one of the more widely used mobile telephone communication systems. However, cloning GSM phones is achieved by cloning the SIM card contained within, not necessarily any of the phone's internal data. GSM phones do not have ESN or MIN, only an IMEI number. GSM SIM cards are actually copied by removing the SIM card and placing a device between the handset and the SIM card and allowing it to operate for a few days and extracting

the KI, or secret code. Cloning has been successfully demonstrated under GSM, but the process is not easy and it currently remains in the realm of serious hobbyists and researchers.

III. HOW MOBILE PHONE WORKS?

Mobile phones send radio frequency transmissions through the sky on two distinct channels, one for voice communications and the other for control signals. When a mobile phone builds a call, it normally transmits its Electronic Security Number (ESN), Mobile Identification Number (MIN), its Station Class Mark (SCM) and the number called in a tiny burst of data. This burst is the short buzz you hear after you press the SEND button and before the tower catches the data. These four things are the components the cellular supplier uses to ensure that the phone is programmed to be billed and that it also has the identity of both the customer and the phone. MIN and ESN is collectively known as the 'Pair' which is used for the cell phone identification .When the cell site gets the pair signal, it determines if the requester is a valid registered user by comparing the requestor's pair to a cellular subscriber list. Once the cellular telephone's pair has been recognized, the cell site emits a control signal to permit the subscriber to place calls at will. This practice, known as Anonymous Registration, is carried out each time the telephone is turned on or picked up by a new cell site.

IV. HOW TO DETECT THE CLONING?

There are several ways to detect the cloning. One of the most fruitful and mostly used ways are discussed here

4.1 Duplicate Detection:

If the service provider finds out the traces of the same phone in the several places at a time, then the service provider has to shut down the complete network. If the network is down, the legitimate user will respond back to the service provider and the ESN/ MIN can be reprogrammed. The fraudulent user will be automatically bypassed. The only loophole in this system is that it is very much difficult for the service provider to trace out the duplicates.

4.2 Usage Profiling:

The usage patterns of the users are studied. If any discrepancies are noticed, the customer is contacted. For example, if a legitimate user is normally accustomed to the local calls and rarely STD calls, and if a call is traced suddenly to foreign country, then there can be chance of cloning.

4.3 Call Counting:

Each phone records the logs of the service utilized. Each service provider also keeps the same logs. If the logs from the company and subscriber are different, then the only conclusion is that the phone is cloned

4.4 Velocity Trap:

If the location of the phone is continuously changing or the location is too far away from last call in impossible amount of time, then it falls under velocity trap. For example, if first call is made from Mumbai and another is made from Bangalore within 15 minutes, or if the calls are made from Dadar and Vicar within 5 minutes, Velocity Trap is encountered.

4.5 RF (Radio Frequency):

Radio fingerprinting is a process that identifies a cellular phone or any other radio transmitter by the unique "fingerprint" that characterizes its signal transmission. An electronic fingerprint makes it possible to identify a wireless device by its unique radio transmission characteristics. Radio fingerprinting is commonly used by cellular operators to prevent cloning of cell phones. A cloned cell

phone will have a same numeric equipment identity but a different radio fingerprint. [10]1 If the service provider spots the same fingerprint of one existing unit, it temporarily suspends the service.

4.6 PIN Codes*:*

The service provider can assign a smart PIN (Personal Identification Number) code to each user. Before calling, the user will request for service privilege from service provider. After the call user will again ask for temporary suspension of service. This PIN can be shared only by user and company. The security algorithms, encryption standards can be implemented on this PIN rather than ESN/MIN Pair.

Indications that shows the phone is Cloned.
1. Recurrent wrong number phone calls
2. Difficulty in placing outgoing calls.
3. Difficulty in retrieving voice mail messages.
4. Incoming calls constantly receiving busy signals or wrong numbers.
5. Unusual call appearing on your phone bills.

V. MOBILE PHONE SAFETY MEASURE

Cellular operators in many countries have deployed various technologies to deal with this threat. Some of them are as follows:

There's the Duplicate Detection Method where 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 has lost the service he is paying for. Pace Trap is another test to check the situation, whereby the mobile phone seems to be moving at Impossible or most unlikely speeds. For example, if a call is first made in Delhi, and five minutes later, another call is made but this time in Chennai, there must be two phones with the same identity on the network. Some operators also use Radio Frequency Fingerprinting, Originally a military technology. Even the same 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. Custom Profiling is another way wherein profiles of customers' phone usage are kept, and when inconsistency are noticed, the customer is contacted. For example, if a customer normally builds only local network calls but is suddenly placing calls to foreign countries for hours of sky-time, it indicates a possible clone. Call Counting is also a way to check the situation where 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.

VI. SOME FACTS AND FIGURE

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.

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. Authorities, in the case, estimated the loss at $3,000 to $4,000 for each number used in cell phone cloning.

According to a school of thought, the Telecom Regulatory Authority of India (TRAI) should issue a directive, which holds the operators responsible for duplications of mobile phones.

Qualcomm, 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. "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.

VII. 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 the security standards are quite easy to breach and takes very less amount of time. Moreover, cloning methodology is widespread and can be implemented easily. Hence, it must be considered that the security system which was implemented lately must not be fruitful enough to secure the system in future. Therefore it is absolutely important to verify the working of a protection system over a precaution system every once a while and change or update it every once a year.

REFRENCES

[1] Pro-Active Prevention of Clone Node Attacks in Wireless Sensor Networks Anandkumar, K.M, C. Jayakumar Journal of Computer Science 8 (10): 1691-1699, 2012 ISSN 1549-3636.
[2] Security Management against Cloned Cellular Phones: Mirela Sechi Moretti A noni Notre Fernando Augusto da Silva Cruz Bernardo Gonçalves Riso Carlos Becker Westphall Federal University of Santa Catarina (UFSC).
[3] Cellular Telephone Cloning Final Report Economic Crimes Policy Team United States Sentencing Commission, January 25, 2000
[4] http://en.wikipedia.org/wiki/Radio_fingerprinting
[5] http://en.wikipedia.org/wiki/Phone_cloning
[6] Cell Phone Cloning Submitted by: PrateekPatni EmailID:prateekrpatni@yahoo.co.in.
[7] http://seminarproject.com/threat mobile-phone cloning-full-report
[8] http://edutwin.com/t-mobile-phone cloning-full report

