# Mobile Cloning: A New Threat of Mobile Phone

Dr. Jyoti Batra Arora*

**Abstract**

Mobile phones are becoming essential part of our life. We cannot expect our life without it. It is involved in every field be it shopping, education, entertainment or money transaction. The security is the main issue with these advance technological devices. Transmission and communication of data, security protocols, and transaction protocols are developed fortnightly to enhance the security of mobile phone software, but to protect the hardware or device is very tough task. The endless possibilities and application in mobile phone allows making misuse of communication. The major threat to mobile phone is from cloning. It makes a loss to individual. This paper describes the mobile cloning, methods of cloning and detection of cloned mobile phones.

**Key words:** Cloning, CDMA, GSM, ESN, MIN, PIN.

## Introduction

Mobile phones are the essential part of our life. Mobile phone works on 3 e's of communication, ease of use, economic and efficient. It is also very much involved in frauds. The mobile phone as a hardware is tough make secure as the different manufacture are involved in their manufacturing. The type of devices breaches the different level of security among themselves. The security methods in CDMA and GSM mobile phones are different and same as the loop hole in security of these mobiles. One of the major security threats is cloning of mobile phones. It is not only a big threat in India but other countries also. This paper will discuss the ill effect of cloning and also different ways to prevent cloning. The future threat of this scam is being elaborated. Cloning is the illegal practice of taking the information from a mobile phone and uses this information for criminal activity. The information is criminally programmed in another mobile. The second phone is known as clone mobile. The cloned mobile is build and get calls and the charges for those calls are billed to the valid subscriber. The service supplier network does not know whether the call is from valid phone or cloned phone.

Mobile phone is the first electronic device which is being cloned after other living being. But unfortunately, it is cloned illegally for illegal and criminal activity. Most of the mobile phone use either of technology be it GSM or CDMA. The mobile phone can be cloned not only for making calls but also to get secret and private information stored on the mobile phone. The first reason or

---

* Assistant Professor, Institute of Information Technology and Management, Delhi

jybatra@gmail.com

identification that one can find that his mobile is being cloned if the user of mobile is getting high bills for calls that was never made by him.

**Working of Mobile Phones**

Mobile phone sends radio frequency signals on two distinct channels one for voice communication and other for control signals. During a call transmission signal or when a mobile phone is making a call it transmits electronic security number, mobile identification number and station class mark and dialed number in a tiny burst of data. This burst is the short buzz that sounds when we press send button or call button and before the tower catches the data. These four attributes are used by cellular to ensure that the phone is now programmed to make bill. MIN and ESN number of mobile phone collectively known as "pair". The pair is used to identify the mobile phone when a mobile phone after getting the pair signal checks for validation of user by comparing it with request or pair to cellular subscriber list. After the recognition of pair the mobile phone site emits a control signal to permit the subscriber to place a call at will. This is known as anonymous registration and this happens every time whenever mobile phones make a call or receive a call.

**Mobile cloning**

It is similar to cloning of living being that acts as the original one. Cloning of mobile phone generate or can make the copy of mobile phone. The other mobile phone becomes the exact replica of mobile original mobile phone such that the calls can be made from both the mobiles but the billed is charged from the original one. It does not only mitigate phone calls but also the services of mobile phones. The mitigate mobile phone acts as twin of original one and for every service used by cloned phone, only the original mobile phone is billed.

Each mobile phone has a specific broadcasting fingerprint in its transmitted information signal. This fingerprint is very unique for a particular number. This print does not get altered even if the user changes MIN or ESN number. The process of Cloning access ESN and MIN pair in following ways to make a success:

a. Sniffing of radio waves sniffing devices.
b. Usage of garbage of mobile phones or hacking of mobile phone service Provider Company.
c. Breach the security to gain unauthorized access in mobile companies.

**History and Methods of Cloning**

It is started in 1990 on Motorola bag phones. It was on its peak during mid of 90's and captured Motorola brick phones such as the classic, the ultra classic and model 8000. Mobile phone cloning is performed in high usage area multiple service providing and fraudulent environments. The loop hole on mobile phone allows the easy cloning of mobile phones.

ESN/MIN pair is not encrypted while using the phone to the MSC mobile switching center for further authentication. Therefore, just by scanning ESN/ MIN pair, the phone can be cloned. If either ESN or MIN is changed, the service provider will accept the call and bill it to the legitimate user or provide the services unaware of the fact that it is not a disconnected receiver. The Station Class Mark (SCM) can also be changed if the cellular tower is provided with a false SCM, the service provider or whoever happens to pursue this fraud is looking for a particular phone in which in reality is not the phone they are looking for.

The System Identification For Home System (SIDH) is also programmed in number assignment module which tells the carrier where to forward the billing information to in case the user is roaming. It takes a few minute to make change in SIDH programming.

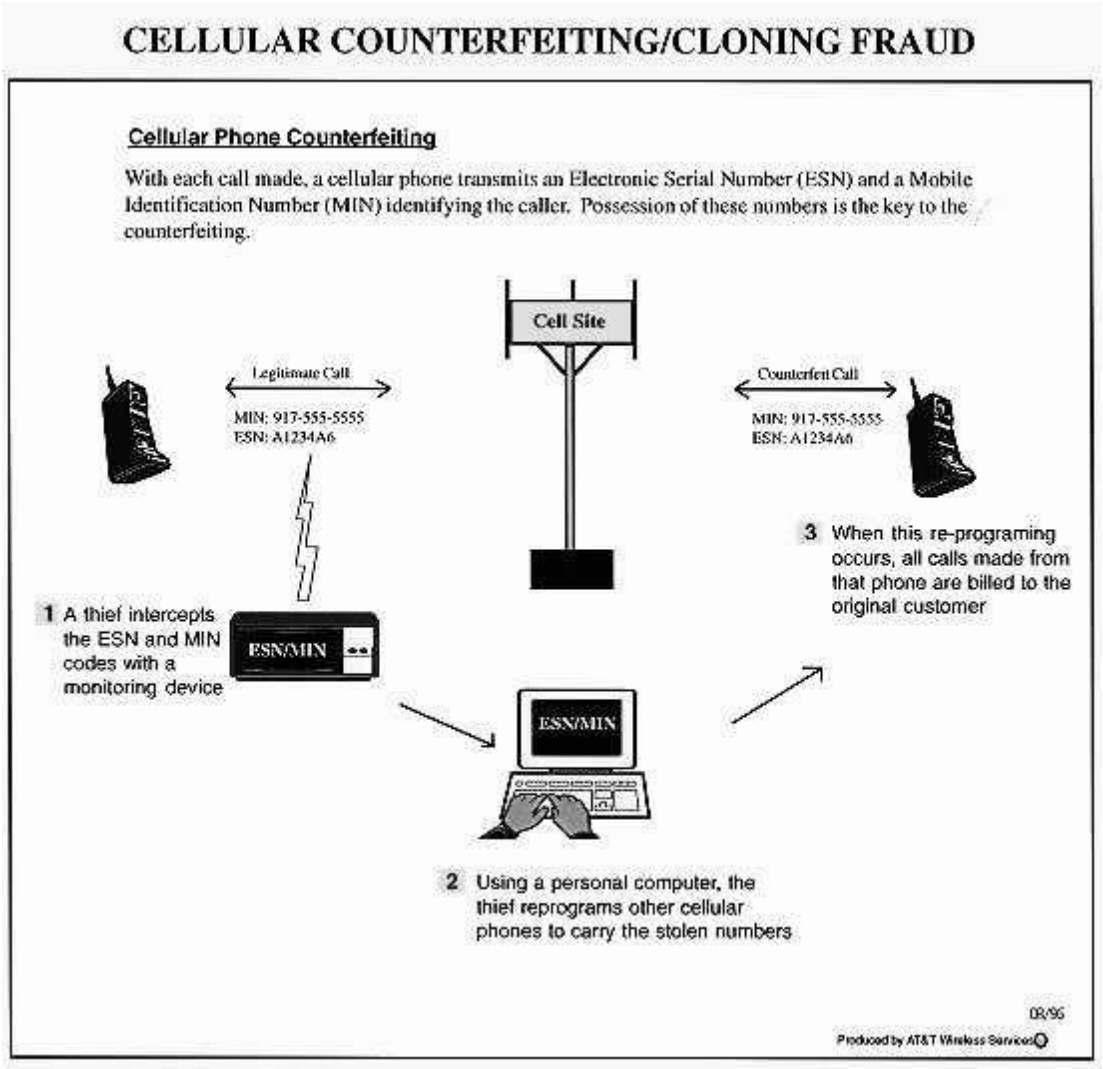
**Methods of cell cloning**

Cloning of mobile phone includes the modification or replacement of EPROM of phone with new chip that allows organizes an ESN by the use of software. Following are the methods described by different researcher that can be used to clone the mobile phone

For CDMA mobile phones : CDMA clone transfers all the user setting and data from original legitimate phone into fraudulent phone that is indistinguishable in make and firmware version.

In CDMA mobile, the EPROM is replaced with a new chip with new configured ESN by the use of software. The second step is to change the MIN and to make a successful ESN/MIN pair. This pair sometimes pronounced as Mobile Equipment Identifier (MEID). The ESN/ MIN is transmitted to cellular company to authenticate device into mobile network. After making this modification the mobile phone PRL and number itself or MIN number can pave the way for fraudulent calls, as the target mobile phone is now the clone of the mobile phone from where the original ESN and MIN numbers are obtained. Cloning in CDMA mobile requires ESN and MIN pair and for GSM mobile, it is a rare process. It is one of the reasons that makes GSM phone more popular as cloning of such mobile is only possible through the cloning of SIM card inserted into it. The main reason for this is that these phones do not have ESN or MIN number they only have IMEI number. SIM can be copied by removing the SIM card and placing a device between handset and SIM card to extract kI or secret code. This process may take a few days. The process of cloning in GSM mobile phone is a tough process so it is being a research area for

researchers.




A few softwares are also available in market to clone the mobile device such as Patagonia is used for CDMA and Bluetooth hack is used to clone GSM phone. Once GSM phone is hacked there is no way that hacker can be traced.

Hackers or mobile phone cloning thieves capture ESN/MIN number of mobile using ESN reader or digital data interpreter (DDI). These are specially designed devices to intercept ESN/MIN number. The hackers or thieves generally attack the area where transmission traffic is high. They monitor the radio wave signals of legitimate user to capture ESN/MIN pair. These numbers are recorded manually and later down load to computer. ESN/MIN readers are used to detect the ESN/MIN pair.

**Detection of the cloning**

Following are the ways to check whether the mobile phone is cloned or not

1. If user receives frequent wrong number phone calls on his phone or mobile phone hangs up usually.
2. When user is facing difficulty in placing outgoing calls.
3. When user is facing difficulty in retrieving voice call messages.
4. When user is making calls and getting the message of busy signal or wrong numbers.
5. When the unusual calls appears on the phone bills of user and these calls were not made by users.

Following are the different ways that help the service provider to detect whether the phone is cloned or not.

1. If service provider finds out the traces of the same phone at the several places at the same time then the service provider has to shut down the complete network. If the network is down, the legitimate user will respond back to service provider to reprogram the ESN/MIN. In this process the fraudulent user will bypass easily. This system has big hole that it is very much difficult for the service provider to trace out the duplicates.
2. The second way is velocity trap which shows that if the location of the phone is continuously changing or the location is too far away from the last call in impossible amount of time.
3. A cloned mobile phone may have same numeric identity but a different radio fingerprint. The radio finger printing is commonly used by mobile phone operator to prevent mobile phone cloning. If the service provider spots the same fingerprint of one existing unit, it temporarily suspends the service.
4. The pattern of users is studied and if any discrepancy is found the customer is contacted for such a reason.
5. Each mobile phone records the logs of utilized services. The service provider also keeps the track of same logs. If the phone is cloned then there is discrepancy between the log record of company and subscriber.

Each user is given a smart pin number by service provider. The user demands for service privilege from service provider. After making the call the user may again ask for temporary suspension of service. The pin is shared by user and mobile company. All the security measures like encryption standards, security algorithms can be implemented on the PIN rather than ESN/MIN pair.

**Financial loss due to mobile cloning**

According to cellular telecommunication industry association (CTIA) the financial loss due to mobile cloning is on higher side in United States. It is between $600 and $900 million. But in India it is in initial stage, so the Indian government and network service provider can take preventive steps to control the frauds. According to hacker news 2013 SIM card cloning hacking has affected 750 million users around the world. Tech2.in.com poised that there were 1300 cases of IMEI cloning in India between 2009 and 2012. This data is increasing from then. Now it has increased to the level. In May 2005, Delhi police solved such a case of mobile phone cloning.

They arrested a person having 20 mobile phones, a laptop a SIM scanner and writer. The accused was arrested for cloning CDMA based mobile phones. This was the entry of mobile phone cloning in India.

**Preventive measures to protect the phone**

Authentication feature is the best way to prevent the SIM or mobile phone from being cloned. Authentication is mathematical process by which identical calculations are performed in both the network and the mobile phone. These calculations use secret key which is preprogrammed into both the mobile phone and the network. The hacker or cloner may not have the access to this secret information so cannot get the same result of calculations. A legitimate mobile phone will produce the same calculated result as the network. The mobile phone's result is sent to the network and compared with network's result. If they match, the phone is not a clone. Authentication is the most robust and reliable method for preventing cloning fraud and it is the only industry standard method to prevent cloning. All mobile telecommunication networks use IS-41 that can support authentication so there is not a requirement of software and communication protocol to prevent mobile cloning.

All the phones since 1996 support the authentication function and the phone which support TDMA or CDMA digital radio are also authentication capable.

Modifying this, as well as the phones PRL & number itself (known as the mobile identification number, or MIN) can pave the way for fraudulent calls, as the target telephone is now a clone of the telephone from which the original ESN and MIN numbers were obtained.

**Conclusion**

In today's era where mobile phone is one of the essential components of our life, the threats and risk related to its security are increasing at a higher pace. The mobile phone as a device is itself is not secure as the replica of mobile phone can be easily generated. In UK and US the mobile phone cloning was entered in 1998 but in India, it is still growing and entered in 2005. The future aspects to protect the mobile phones are very high as now crimes related to mobile phones are viewed as a priority. It can also help to solve the criminal cases. The advancement is on the top in the case of software security but a comprehensive and legislative approach is required to control this emerging fraud activity.

**References**

The hacker news Sunday, July 21, 2013

Anandkumar, K.M, C. Jayakumar,2012. *Pro-Active Prevention of Clone Node Attacks in Wireless Sensor Networks.* Journal of Computer Science, 8 (10): 1691-1699, 2012 ISSN 1549-3636.

Mirela Sechi Moretti Annoni Notare Fernando Augusto da Silva Cruz Bernardo Gonçalves Riso Carlos Becker Westphall, 2000. *Security Management Against Cloned Cellular Phones.* Federal University of Santa Catarina (UFSC) :

Cellular Telephone Cloning Final Report.2000, *Economic Crimes Policy Team United States Sentencing Commission* , January 25, 2000

Small Scale Digital Device,2009 *Forensics Journal*, Vol. 3, No. 1, June 2009 ISSN 1941-6164

A. Murphy,2012. *The Fraternal Clone Method For Cdma Cell Phones* International Journal of Computer Applications Volume 45 No.21, May 2012 [online] Available at : https://www.movzio.com/howto/cell-phone-cloning-guide/

Yi-Bing Lin, Ming-Feng Chen Rao, .C.H.2002 *Potential fraudulent usage in mobile telecommunications networks Mobile Computing*, IEEE Transactions on Volume: 1 , Issue: 2 , Page(s): 123 - 131

WuShaoBo, LiChengShu,2010. *A method of USIM anticloning in LTE/SAE,Information Science and Engineering(ICISE).* 2nd International Conference, Page(s):4277–4280, PublicationYear:2010

Notare,M.S.M.A., DaSilva Cruz, F.A, Riso,B.C., Westphall,C.B, 1999.*Wireless communications : security management against cloned cellular phones*, Wireless Communications and Networking Conference. WCNC.1999 IEEE ,Page(s):1412416 vol.3

Barbera,M.V., Mei,A.2012. *Personal Marks and Community Certificates : Detecting Clones in Wireless Mobile Social Networks*, Distributed Computing in Sensor Systems (DCOSS ), 2012 IEEE8thInternationalConference,Page(s):83 –91

**Key words: Cloning, CDMA, GSM, ESN, MIN, PIN.**

**Abbreviations used**

GSM- Global System for Mobile Communications

CDMA- Code Division Multiple Access

ESN- Electronic Security Number

MIN- Mobile Identification Number

IMEI- International Mobile Station Equipment Identity