



Mobile Phone Cloning: Past, Present, Precaution

Megha. Mutalik Desai

MCA, ATSS-IICMR Nigadi, Pune, India

Email: meghaklkrn@gmail.com

Abstract — 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 communication make it an alluring target for criminals. Cell phone cloning is copying the identity of one mobile telephone to another mobile telephone.

Usually this is done for the purpose of making fraudulent telephone calls. The bills for the calls go to the legitimate subscriber. The cloner is also able to make effectively anonymous calls, which attracts another group of interested users. The major threat to mobile phone is from cloning.

Index Terms: Cell phone cloning, GSM, CDMA, EMIE and PIN, Patagonia

I. INTRODUCTION

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 result is that the "cloned" phone can make and receive calls and the charges for those calls are billed to the legitimate subscriber. The service provider network does not have a way to differentiate between the legitimate phone and the "cloned" phone

While mobile cloning is an emerging threat for Indian subscribers, it has been happening in other telecom markets since the 1990s, though mostly with regard to CDMA phones. Pleas in an US District Court in 1997 effectively ended West Texas authorities' first case of 'phone cloning.' Authorities in the case estimated the loss at \$3,000 to \$4,000 for each number used. 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. Back home, police officers say the Yasin case is just the tip of the iceberg and have

asked operators to improve their technology. But the operators claim they can't do much for now.

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. The use and advantages of phone cloning is restricted to certain limitations. Each mobile phone usually contains 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 the phone's MIN (Mobile Identification Number) number or ESN



Fig. 1. Example of a cloned phone.

II. WHAT IS CLONING?

When we look up the dictionary meaning of cloning it states, "To create the exact replica or a mirror image of an subject under study. The subject can be anything living or non-living so here we take into consideration the cellular or mobile phones. So Mobile cloning is copying the identity of one mobile telephone to another mobile telephone. Cell phone cloning is a technique wherein 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 phone 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. 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. Millions of cell phones users, be it GSM or CDMA, run at risk of having their phones cloned.

A. How it is done?

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.

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. If PIN and ESN are known, a mobile phone can be cloned in seconds using some software's like Patagonia which is used to clone CDMA phones. FOR GSM:- However, if the accused manages to also clone the IMEI number of the handset, for which software's are available, there is no way he can be traced. BLUETOOTH HACK is the software available in the market which is used to hack/clone GSM phone. It is simple to use.

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.

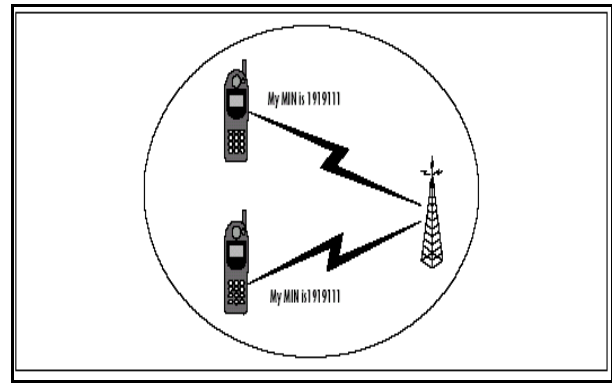


Fig. 2. Example of a CDMA phone cloning.

B. What are GSM and CDMS mobile phone sets?

CDMA is one of the newer digital technologies used in Canada, the US, Australia, and some South-eastern Asian countries (e.g. Hong Kong and South Korea). CDMA differs from GSM and TDMA (Time Division Multiple Access) by its use of spread spectrum techniques for transmitting voice or data over the air. Rather than dividing the radio frequency spectrum into separate user channels by frequency slices or time slots, spread spectrum technology separates users by assigning them digital codes within the same broad spectrum. Advantages of CDMA include higher user capacity and immunity from interference by other signals.

GSM is a digital mobile telephone system that is widely used in Europe and other parts of the world. GSM uses a variation of TDMA and is the most widely used of the three digital wireless telephone technologies. GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900 MHz or 1,800 MHz frequency band.

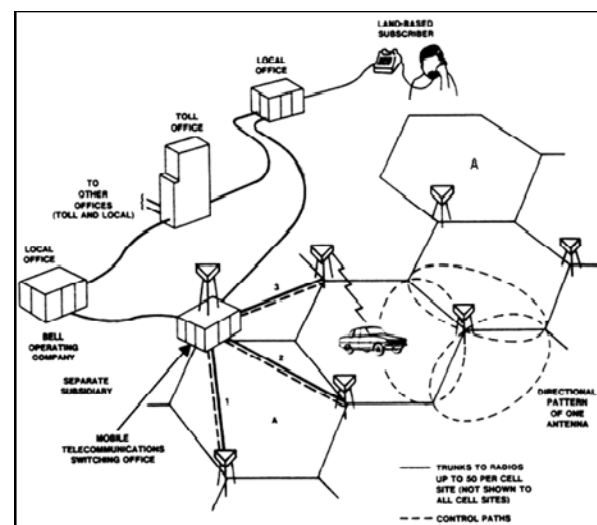


Fig. 3. Example of GSM Technology.

C. Rise of Cell 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 started with Motorola "bag" phones and reached its peak in the mid 90's with a commonly available modification for the Motorola "brick" phones, such as the Classic, the Ultra Classic, and the Model 8000.

III. LOOP HOLES IN CELL PHONE NETWORKS

1. ESN/MIN pair is not encrypted while using the phone to the MSC (Mobile Switching Centre) for further authentication. Hence just by scanning the data i.e. ESN/MIN pair, the phone can be very well be cloned. By changing ESN and MIN, the Service provider will accept the call and bill it to the legitimate user or provide service unaware of the fact that it is not a disconnected receiver

2. The Station Class Mark (SCM) can also be changed. By providing the cellular tower with a false SCM, the Service Provider, or whoever happens to pursue this fraud is often looking for a particular phone which in reality is not the phone they are looking for.

3. The SIDH (System Identification for Home System) is also programmed in Number Assignment Module (NAM). The allowance of the SIDH number tells the carrier where to forward the billing information to in case the user is "roaming". Changing an SIDH is programming job that takes only minutes.

IV. MOBILE PHONE CLONING SOFTWARE

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. ESN/MIN pairs were discovered in several ways:

- Sniffing the cellular
- Trashing cellular companies or cellular resellers
- Hacking cellular companies or cellular resellers

Cloning still works under the AMPS/NAMPS system, but has fallen in popularity as older clone able phones are more difficult to find and newer phones have not been successfully reverse-engineered. 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.

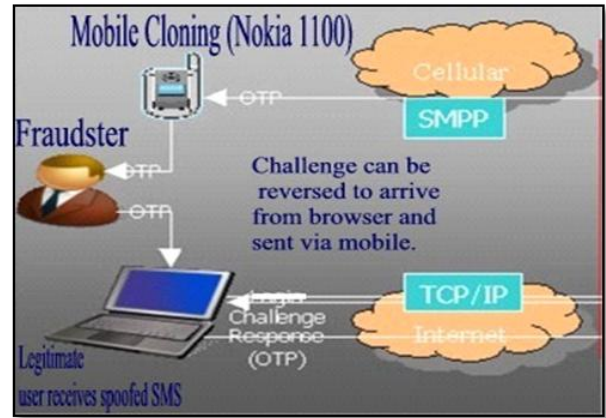


Fig. 4. Example of a process of phone cloning

D. How is a phone cloned?

Cellular thieves can capture ESN/MINs using devices such as cell phone ESN reader or digital data interpreters (DDI). DDIs are devices specially manufactured to intercept ESN/MINs. By simply sitting near busy roads where the volume of cellular traffic is high, cellular thieves monitoring the radio wave transmissions from the cell phones of legitimate subscribers can capture ESN/MIN pair. Numbers can be recorded by hand, one-by-one, or stored in the box and later downloaded to a computer. ESN/MIN readers can also be used from inside an offender's home, office, or hotel room, increasing the difficulty of detection.

The ESN/MIN pair can be cloned in a number of ways without the knowledge of the carrier or subscriber through the use of electronic scanning devices. After the ESN/MIN pair is captured, the cloner reprograms or alters the microchip of any wireless phone to create a clone of the wireless phone from which the ESN/MIN pair was stolen. The entire programming process takes 10-15 minutes per phone. Any call made with cloned phone are billed to and traced to a legitimate phone account. Innocent citizens end up with unexplained monthly phone bills. To reprogram a phone, the ESN/MINs are transferred using a computer loaded with specialized software, or a "copycat" box, a device whose sole purpose is to clone phones. The devices are connected to the cellular handsets and the new identifying information is entered into the phone. There are also more discreet, concealable devices used to clone cellular phones. Plugs and ES-Pros, which are about the size of a pager or small calculator, do not require

computers or copycat boxes for cloning. The entire programming process takes ten-15 minutes per phone.

This was how CDMA handsets are cloned but now we face a question that being: -Do GSM sets run the risk of 'cloning'?

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.

But the GSM-based operators maintain that the fraud is happening on CDMA, for now, and so their subscribers wouldn't need to worry. Operators in other countries have deployed various technologies to tackle this menace. They are:-

1) 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.

2) Velocity 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.

3) Some operators also use Radio Frequency fingerprinting, originally a military technology. Even 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.

4) Usage profiling is another way wherein profiles of customers' phone usage are kept, and when discrepancies are noticed, the customer is contacted. 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. What is Patagonia?

Patagonia is 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 phone i.e. cloning of phone. There are other Software's available 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 accuser manages to also clone the IMEI number of the handset, for which software's are available there is no way he can be traced.

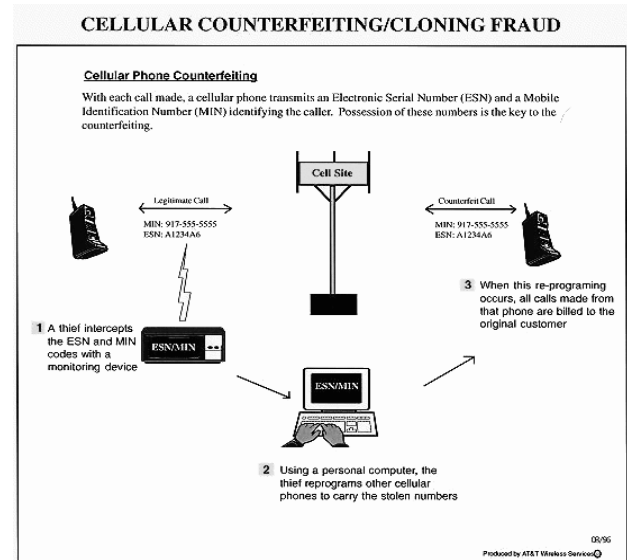


Fig. 5. Example of a process of Cellular cloning

V. IMPACT OF CLONING

Each year, the mobile phone industry loses millions of dollars in revenue because of the criminal actions of persons who are able to reconfigure mobile phones so that their calls are billed to other phones owned by innocent third persons. Often these cloned phones are used to place hundreds of calls, often long distance, even to foreign countries, resulting in thousands of dollars in airtime and long distance charges. Cellular telephone companies do not require their customers to pay for any charges illegally made to their account, no matter how great the cost. But some portion of the cost of these illegal telephone calls is passed along to cellular telephone consumers as a whole.

Many criminals use cloned cellular telephones for illegal activities, because their calls are not billed to them, and are therefore much more difficult to trace.

This phenomenon is especially prevalent in drug crimes. Drug dealers need to be in constant contact with their sources of supply and their confederates on the streets. Traffickers acquire cloned phones at a minimum cost, make dozens of calls, and then throw the phone away after as little as a day's use.

In the same way, criminals who pose a threat to our national security, such as terrorists, have been known to use cloned phones to thwart law enforcement efforts aimed at tracking their whereabouts.

VI. METHODS TO DETECT CLONED PHONES IN NETWORK

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

- 1) 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.
- 2) 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.
- 3) 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.
- 4) 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.

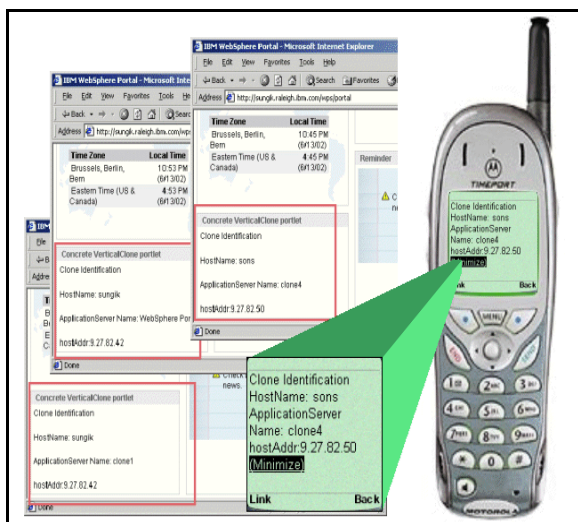


Fig. 6. Example of a process of Duplicate Detection

- 5) 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.

- 6) 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.

VII. 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

- 1) Duplicate Detection

If the service provider finds out the traces of the same phone in the at 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.

- 2) 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 Virar within 5 minutes, Velocity Trap is encountered.

- 3) 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) 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.

5) 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

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.



Fig. 7. Example Showing the process of phone cloning

VIII. PREVENTION FOR CLONING?

Uniquely identifies a mobile unit within a wireless carrier's network. The MIN often can be dialed from other wireless or wire line networks. The number differs from the electronic serial number (ESN), which is the unit number assigned by a phone manufacturer. MINs and ESNs can be checked electronically to help prevent fraud. Mobiles should never be trusted for communicating/storing confidential information.

Always set a Pin that's required before the phone can be used. Check that all mobile devices are covered by a corporate security policy. Ensure one person is responsible for keeping tabs on who has what equipment and that they update the central register. How do service providers handle reports of cloned phones? Legitimate subscribers who have their phones cloned will receive bills with charges for calls they didn't make. Sometimes

these charges amount to several thousands of dollars in addition to the legitimate charges.

Typically, the service provider will assume the cost of those additional fraudulent calls. However, to keep the cloned phone from continuing to receive service, the service provider will terminate the legitimate phone subscription. The subscriber is then required to activate a new subscription with a different phone number requiring reprogramming of the phone, along with the additional headaches that go along with phone number changes.

IX. SOLUTION TO THIS PROBLEM

Cloning, as the crime branch detectives divulge, starts when someone, working for a mobile phone service provider, agrees to sell the security numbers to gray market operators. Every mobile handset has a unique factory-coded electronic serial number and a mobile identification number. The buyer can then program these security numbers into new handsets.

The onus to check the misuse of mobile cloning phenomenon falls on the subscriber himself. The subscribers, according to the officials, should be on the alert and inform the police on suspecting any foul play. It would be advisable for them to ask for the list of outgoing calls, as soon as they realize that they've been overcharged. Meanwhile, the crime branch is hopeful to find out away to stop the mobile cloning phenomenon.

1) For example

The Central Forensic Laboratory at Hyderabad has reportedly developed software that would detect cloned mobile phones. Called the Speaker Identification Technique, the software enables one to recognize the voice of a person by acoustics analysis. These methods are only good at detecting cloning, not preventing damage. A better solution is to add authentication to the system. But this means upgrading the software of the operators' network, and renewing the SIM-cards, which is not an easy or a cheap task. This initiative by the Forensic Laboratory had to be taken up in the wake of more and more reports of misuse of cloned mobiles.

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 article 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

Presently the cellular phone industry relies on common law (fraud and theft) and in-house counter measures to address cellular phone fraud. Is in initial stages in India so preventive steps should be taken by the network provider and the Government the enactment of legislation to prosecute crimes related to cellular phones is not viewed as a priority, however. It is essential that intended mobile crime legislation be comprehensive enough to incorporate cellular phone fraud, in particular "cloning fraud" as a specific crime.

Existing cellular systems have a number of potential weaknesses that were considered. It is crucial that businesses and staff take mobile phone security seriously.

Awareness and a few sensible precautions as part of the overall enterprise security policy will deter all but the most sophisticated criminal. It is also mandatory to keep in mind that a technique which is described as safe today

can be the most unsecured technique in the future. Therefore it is absolutely important to check the function of a security system once a year and if necessary update or replace it. Finally, cell-phones have to go a long way in security before they can be used in critical applications like m-commerce.

REFERENCE:

- [1] Manjush Talmale, Abhishek Kinhekar, Akshay Saraf, Milind Bhajan "Mobile Phone Cloning: History, Present Scenario and Precautionary Techniques", Nagpur, 2013 International Journal of Application or Innovation in Engineering & Management (IJAEM) 2013
- [2] <http://www.cdmasoftware.com/eng.html>
- [3] <http://wiretap.spies.com>
- [4] <http://www.hackinthebox.org/>
- [5] <http://www.google.com>
- [6] <http://www.wikipedia.com>

