SPECIAL ISSUE FOR NATIONAL CONFERENCE ON RECENT ADVANCES IN TECHNOLOGY AND MANAGEMENT FOR INTEGRATED GROWTH 2013 (RATMIG 2013)

Mobile Phone Cloning: History, Present Scenario and Precautionary Techniques

Manjush Talmale¹, Abhishek Kinhekar² Akshay Saraf³ Milind Bhajan⁴

¹Manjusha Talmale
GNIEM Nagpur
manjutalmale@gmail.com

²Abhishek Kinhekar
GNIEM Nagpur
Abhi.abhi888@gmail.com

³Akshay D. Saraf
GNIEM Nagpur
akshaydsaraf@gmail.com

⁴Milind Bhajan
GNIEM Nagpur
bhajamilind@gmail.com

ABSTRACT

Mobile phones have become the most important and integral part of today’s lifestyle. This latest mode of communication is considered as most significant as it involves ‘3e’s, ease of use, economic and efficient. As the money is involved in this business, it is subjected to fraud. The more sophisticated and advanced security mechanisms are regrettably not up to the mark. The endless possibilities and applications which are now designed and implemented allure the gray and dark users to make the misuse of this communication medium. The major threat to mobile phone is from cloning. Unexpectedly high mobile phone bills and malicious nature of service are the major symptoms of possibility of mobile cloning. Following paper introduces about the history of mobile cloning, recent trends and possible precautions.

Keywords: Cloning, CDMA, GSM, ESN/MIN.

1. INTRODUCTION

Across the globe, instant communication is available with computers, emails, internet, and cell phones. The last, however, have increasingly become something of a household item in the past few decades. Launched to facilitate communication in all places and at all times, cell phones have developed into sophisticated gadgets offering numerous Prospects. The epic discussion of advantages and disadvantages of using the cell phones is never ending. 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 gets altered even if the use changes the phones’ MIN(Mobile Identification Number) number or ESN.
2. A BRIEF HISTORY OF CELL PHONE CLONING

Cloning of mobile phones is the done by copying phones or subscribers information from one to another device for purposes of obtaining free calls, using different services, for secret information and data. The newer cell phone becomes the accurate imitation of the original cell phone like a twin. As a result, while the services are used from the original phone as well as the twin phone, only the original cell phone is billed. Cloning is performed in high usage area, multiple service providing and fraudulent environments.

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.

Cloning required access to ESN and MIN pairs. ESN and MIN pairs were exposed in several ways:

- By sniffing the radio waves sniffing devices.
- By using garbage of cellular phones or hacking the cell phone service provider company.
- Gain unauthorized access in cellular companies through breach of security.

3. LOOP HOLES IN CELL PHONE NETWORKS

3.1. 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 vell 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

3.2. 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.

3.3. 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.

4. 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 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.

4.2. 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.
4.3. **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] If the service provider spots the same fingerprint of one existing unit, it temporarily suspends the service.

4.4. **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.

4.5. **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.

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.

5. **CREATING A CDMA CELL PHONE FRATERNAL CLONE**
The aim of CDMA Clone is to transfer all of the user settings and user created data from the original legitimate phone into a fraudulent phone that is indistinguishable in make, model and firmware version. The Fraternal Clone is so named because the data in the clone will be the same to that in the legitimate phone but some extra files can be present in the clone phone.
CDMA cloning involves gaining access to the devices Embedded File System /nv/nm directory via specialized software or placing a modified EEPROM into the target mobile telephone, allowing the electronic serial number (ESN) & or Mobile Equipment Identifier (MEID) of the mobile phone to be changed. The ESN or MEID is typically transmitted to the cellular company's MTSO in order to authenticate device onto the mobile network. 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.[11]
6. PREVENTIONS AND COUNTERMEASURES FROM CELL PHONE CLONING.

Following are some avoidance methods by which we can avoid phone from cloning:

6.1. Confidential information should never be saved in mobiles.
6.2. A password protected phone locking system may prevent the cloning to certain extent.
6.3. All devices should be covered by a company policy.

7. FACTS AND FIGURES

1. According to the hacker news, sim card cloning hack affect 750 million users around the world (Mohit Kumar, the hacker news Sunday, July 21, 2013)
2. Tech2.in.com says 1,300 cases of IMEI cloning found in India between 2009-2012
3. There are numerous freeware software available for sniffing, thrashing and cloning of cell phone.
4. The cloning process takes less than an hour to program, changing of EEPROM, and reassembling.
5. Practically there is still no solution to counter this problem. Only preventive measures are suggested.
6. The cloners are nearly impossible to trace down and can clone any cell phone of the same model and make.

8. 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.

References

2. Security Management Against Cloned Cellular Phones: Mirela Sechi Moretti Annoni Notare Fernando Augusto da Silva Cruz Bernardo Gonçalves Riso Carlos Becker Westphall Federal University of Santa Catarina (UFSC) - Technological Center (CTC)- Network and Management Laboratory (LRG)


4. Cell Phone Cloning Submitted by: Prateek Patni Email ID: prateek_r_patni@yahoo.co.in

5. SECURITY MANAGEMENT AGAINST CLONING MOBILE PHONES Mirela Sechi Moretti Annoni Notare Azzedine Boukerche Fernando A. S. Cruz Carlos G. Riso Carlos B. Westphall


8. A Safe and Secure Web-Based Management for Mobile Phone Operations Mirela Sechi Moretti Annoni Notare Azzedine Boukerche Carlos Becker Westphall


Organized By: GNI Nagpur, India