International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Mobile Phone Cloning

Nidhi Tanwar[1], Sachin Chauhan[2]

[1]Poornima Institute of Engineering & Technology, ISI-2, Sitapura, 302022, Jaipur
nidhipiet127@poornima.org

[2]Poornima Institute of Engineering & Technology, ISI-2, Sitapura, 302022, Jaipur
sachinchauhan@poornima.org

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. This business is subjected to fraud as the money is included in it. The more sophisticated and advanced security mechanisms are regrettably not up to the required level. The endless chances 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 fromits cloning. The unexpected high mobile phone bills and malicious nature of service are the major symptoms of possibility of the mobile phone cloning. The 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 internet, cell phones,computers and emails. However, this has increasingly become something of a household item in the past few decades. Launched to facilitate communication in the all places and everywhere , 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 restrictions. Each cell phone usually contains a specific broadcasting fingerprint in its transmitted information wave. This content of fingerprint is very unique for a particular number.

This fingerprint does not gets altered even if the use changes the phones' MIN (Mobile Identification Number) number or ESN (Electronic Serial Number) number.

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 priceless calls, 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 duplicate phone having all similar features but only the original cell phone is billed. Cloning is performed in high usage area, multiple service providing and illegal environments. A Software tool is used for modifying and configuring the mobile phone. The memory used in EEPROM chip is replaced and modified with a new chip which will reconfigure ESN (Electronic Serial Number) or IMEI (International Mobile Equipment Identity) and via MIN (Mobile Identification Number) . When the ESN/MIN pair had changed successfully then an effective clone of the original phone has generated. Here Cloning requires access to ESN and MIN pairs. The exploitation of ESN and MIN pairs is there in different ways:

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

3. Loop Holes in Cell Phone Networks

3.1 ESN/MIN

ESN/MIN pair is not encrypted while using the phone to the MSC (Mobile Switching Centre) for further verification. Hence only by scanning the data , the phone can be very well 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)

The Station Class Mark (SCM) can also be changed. The cellular tower provided 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)

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 mobile phone cloning. One of the most easiest 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 service network is not up to the mark, then the legal user will respond back to the service provider and the ESN/ MIN can be reprogrammed resulting in detection of the false user cheating . 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. This can be understood by taking an example, if first call is made from Mumbai and another is made from Bangalore within 15-20 minutes, or if the calls are encountered 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. The identification of a wireless device is done by the electronic fingerprint detected due to its unique radio transmission characteristics. Cellular operators use Radio fingerprinting to prevent cloning of mobile phones. A cloned mobile will have a similar numeric equipment identity but a different radio fingerprint.

4.4 Usage Profiling

The usage patterns of the users are studied. If any differences are noted ,then the original authenticated user is contacted. For example, if a legitimate user is normally accustomed to the local calls and often a STD call, or if a call is tracked immediatelyfrom foreign country, then there can be chance of cloning.

4.5 Call Counting

Each phone records the logs of its utilization of the service . Each service provider also keeps the same logs. If the logs from the company and subscriber are not matched, then decision can be made 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 giving its services. After the call only the authenticate user will again ask for temporary suspension of service. This PIN can be shared only by authenticated user and service provider company. The encryption standards and the security algorithms, can be implemented on this PIN rather than ESN/MIN Pair. Indications that shows the phone is Cloned.

1) Difficulty in receiving voice mail messages.
2) Difficulty in placing outgoing calls.
3) Incoming calls continuously receiving busy signals or the message of wrong numbers.
4) Recurrent wrong number phone calls
5) Unusual call noticed 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 in differentiability in manufacture , model and its 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 /nvm/num 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 MEID or ESN is transmitted to the cellular company's MTSO in order to authenticate device onto the mobile phone network. By Modifying this, and the PRL of the phone with the number itself (known as the mobile identification number, or MIN) can make the way for fraud calls, as the destined and targeted telephone is now a clone of the original telephone from which the original ESN and MIN numbers were obtained.

6. Preventions and Counter Measures 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.
- A password protected phone locking system may prevent the cloning to certain extent.
- All devices should be covered by a company policy.
- Review your monthly usage from time to time.
- Report to service provider for discrepancies in service.

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 21 July, 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 detection , routing and cloning of cell phone.
4) The cloning process takes very less time to program, changing of the memory of EEPROM, along with its reassembling.
5) Practically there is still no solution to counter this mobile cloning. Only precautions 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 efficient, reliable and widespread. The utilization of the system can be altered in either destructive or constructive manner. The security standards unfortunately are quite easy to breach and takes very less time. Moreover, mobile phone cloning methods is now widespread and can be implemented very easily. Hence, it must be taken into consideration about the security system which was implemented lately must not be fruitful enough to secure the system in future aspects. Therefore it is very 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

[1] Security Management Against Cloned Cellular Phones.
[2] Small Scale Digital Device Forensics Journal.
[3] International Journal of Computer Applications.
[4] International Journal of advances in computing & communications, www.ijacc.org.
[5] http://en.wikipedia.org/wiki/Radio_fingerprinting.
[6] http://en.wikipedia.org/wiki/Phone_cloning.

Author Profile

Nidhi Tanwar is currently pursuing her engineering from Electronics and Communication branch from Poornima Institute of Engineering and Technology, Jaipur and is in her final year(8th semester)current