PHONE CLONING

OUATTARA LAGNINY ISMAEL ,student, Department of Master of Computer Applications, Parul University.

Abstract

A long time ago, the communication has been one the most important factor in the human life particularly in the business area. The communication is defined as an exchange of information between two or more actors (entities). However, this communication need to be private and secured to avoid an unexpected damage. Unfortunately, despite the implementation of the privacy and the security system, the societies are victims from various forms of attacks. Among those attacks appears the cloning, which defines the fact of copying the information of an original model to reprogram another model to achieve some malicious activities such as stealing information, intercepting calling, place an outgoing calling, increase the legitimate user's bills. Regardless of the above activities, not all people are aware of their possibility to interfere with their ongoing business. Therefore, this has resulted a tremendous competition among mobile phone service providers in providing security system.

This review paper globally presents both technologies CDMA & GSM, which stands for Code-Division Multiple Access and Global System for Mobile communication respectively, depicts the ways of detection and finally some methods for prevention.

Keywords: Phone Cloning, CDMA (Code-Division Multiple Access), GSM (Global System for Mobile communication), IMEI, MIN.

I) INTRODUCTION

Many years ago, the cloning has been experienced on frogs, which were the first animals to be cloned by using embryonic cells. Later embryonic cell, techniques were being used to clone laboratory animals, including mice and livestock, including cattle and sheep. Beside of the animal cloning, the humanity is facing for the first time with a clear harmful threat of cloning in the field of technology like mobile phone and the target of this version of cloning is to make malicious activities [1]. Phone cloning is a technique wherein secured data from one cell phone is transferred to another phone. By cloning, we have to understand that it consists of replicating an identity of the original object to another object. By this way, assume that phone cloning is the act of copying of one mobile phone to another. However, this malicious activity is used to make fraud calls and it results to an increased bill to the legitimate subscriber. This led to the popularity of the cloning in certain zone where the cost for placing call was very abstract. The cloner is also able to make effectively anonymous calls, which attracts another group of interested lawbreakers. Mobile phone cloning started with Motorola "bag" phones and reached its highest value in the middle part of 90's with a commonly available modification for Motorola "brick" phones such as the Model 8000. [1] The cloner may set the options to ring or vibrate his phone when you make a call and you will have no knowledge that the cloner is listening from his own mobile. He can have an access right to read text message, phone book entries, look at pictures. In addition, he can get 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 loopholes in systems. Therefore, when one receives huge bills, the chances raise that the phone is being cloned. Many of cell phones users, be it GSM or CDMA, run at risk of having their phones cloned [1].

II) LITTERATURE SURVEY

1) Functioning of mobile phone

Cell phone transmits the radio frequencies over two separate channels one for voice and another for control signaling information. [5] When a call is done through cell phone along with other three important components are transmitted-

- Electronic Serial Number (ESN),
- Mobile Identification Number,
- Station Class mark.

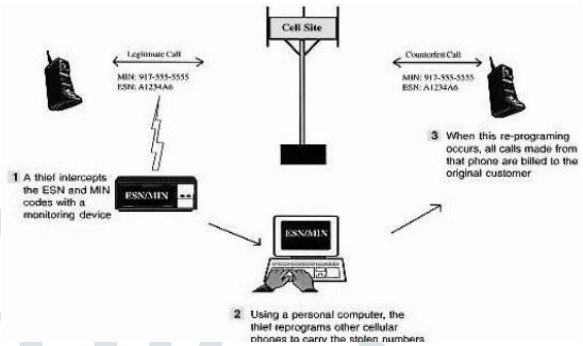
These three components are very important to service provider since they provide the billing information to the cellular service that how much amount of money a customer has to be charged. After receiving the pair ESN/MIN, cell service provider checks them with their authentic subscriber list. If this pair ESN/MIN is genuine then a control signal is generated and allows the customer to place the call. The successfully pair registering this way is called as Anonymous Registration. [5]

2) Important terms

- CDMA stands for Code-Division Multiple Access is a channel access method used by a diversity radio communication. CDMA is an

example of multiple access where multiple senders can send information simultaneously with the use of a single communication channel. There is no Subscriber Identity Module (SIM) card. CDMA use a Mobile Identification Number (MIN) card that contains user account information [2].

- GSM stands for Global System for Mobile communication uses a variation of Time Division Multiple Access (TDMA) and is the most widely used of the three digital wireless telephone technologies (TDMA, GSM and CDMA). GSM uses a Subscriber Identity Module (SIM) card that contains user account information. Any GSM phone becomes immediately programmed after plugging in the SIM card. Operators who provide GSM service and Airtel, Vodafone, Idea [3].
- IMEI stands for International Mobile Equipment Identifier is a 10 digits universally unique number of our GSM handset. The term Universal Unique is used because there cannot be two mobile phones having the IMEI number. Moreover, this is a very valuable number and used in tracking mobile phones [4].
- SIM stands for Subscriber Identity Module provides storage of subscriber related information of three types:
  - Fixed data stored before the subscription is solid.
  - Temporary network data.
  - Service related data.
- ESN stands for Electronic Serial Number is same as the IMEI but used in CDMA handsets.



- MIN stands for Mobile Identification Number is the same as the SIM of GSM [4].

3) How is a phone cloned?

When the account number of a victim telephone user stolen and reprogrammed into another cellular telephone then is said to be cloned. Each cellular phone has a unique pair to identify numbers: the Electronic Serial Number (ESN) and the Mobile Identification Number (MIN). The ESN/MIN pair can be cloned in a number of ways without the knowledge of the subscriber with the help of electronic scanning devices. Once the ESN/MIN pair is captured, the cloner reprograms 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 may take 10 to 15 minutes per mobile phone. Any call made with cloned phone are counted to and traced to a legitimate phone account. Unfortunately, Innocent citizens end up with unexplained monthly phone bills. Patagonia is a software available in the market that is used to clone CDMA phone. With the help of this software,

the hacker can take control over a CDMA phone i.e. phone cloning. There are other software available in the market. This software's are easily available in the market. A SIM card can be cloned repeatedly and they can be used at different places. All the transactions such as messages and calls from cloned phones can be tracked. However, if the accused manages to also clone the IMEI number of the handset, for which software are available, there is no way he can be traced [6].

Fig-9: Cloning fraud retrieved from [seminaronly.com]

4) Methods to detect cloned phones

Following are different ways to detect cloned phone:

- Double identity: At the same time, the network observe the movement of the same phone in many places. Observing this anomaly in the network, the network service provider will cut them off so that the legitimate subscriber will immediately contact the service to have been disconnected from the network and then the cloner will not be able to use the same phone. The major point of this method is to detect whenever two same ESN/MIN are present in the network [7].
- Pace trap: The mobile phone seems to be moving at impossible or most unlikely speeds. For example, if a call is made in Vadodara and five minutes later another call is made but this time in Ahmedabad, there must be two phones with the same identity on the network.
- RF (Radio Frequency): Fingerprint system commonly called under the name of Fingerprinting is originally a technology used in Army. This technology is helpful for identifying the phone over the network. Therefore, the network software has a function of storing and comparing fingerprints for all the phones that it sees. By this way, it will detect the clones with the same identity but different fingerprints.
- Profile historic: Profiles of customer's phone usage are kept and when inconsistencies are noticed, the customer is contacted. Credit card companies use the same method. Let us consider the consumer behavior who usually made a local network call then suddenly place a foreign call, it raise the chance of cloning.
- Call counting: Both the phone and the network keep track of calls made with the phone, and they should differ more than the usually allowed one call, service is denied.
- PIN (Personal Identification Number): Prior to placing a call, the call 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 [5].

5) How to know that the cell has been cloned?

A cell phone is cloned by identifying a variety of reason based on the following statements:

- Frequent fake calls to your phone,
- Difficulty in placing outgoing calls,
- Difficulty in retrieving voice mail messages,
- Constant incoming calls receiving busy the signal,
- Unusual calls appearing on your phone bills,

From the above reasons, we can say that the phone is cloned.

6) Techniques to prevent cloning

In fact, the service provider will consider the cost of the additional fraudulent calls. Furthermore, to keep the cloned phone from continuing to receive service, the service provider will shut the legitimate phone subscription off. 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 numbers changes [8].

- The MIN often can be composed from other wireless,
- The number differs from the electronic serial number (ESN), which is the unique number set by a phone manufacturer,
- Electronically or technically check MINs and ESNs to help the fraud prevention,
- Frequently set PIN code before any phone call,
- Check that all mobile devices are converted by a corporate security policy [8].

7) Facts and figures

There are several data about the phone cloning and as far as we are concerned, some are mentioned below:

- Southwestern Bell claims wireless fraud costs the industry $650 million yearly in the United States.
- Some federal agents in the United States consider phone cloning as a special 'popular' crime due the difficulty level to trace.
- In one case, cellular phone thieves using the number of a single unsuspecting owner placed more than 1500 telephone calls in a single day.
- In 2002, the ministerial department of the United Kingdom responsible for security, law revealed that in London around 3,000 mobile phones were stolen in one month alone which were used for cell phone cloning [7].

III) CONCLUSION

Therefore, it is important to check the function of a security system once a year and if necessary update or replace it. Preventive steps should be taken by the network provider and the government the enactment of legislation to prosecute crimes. Moreover, a standard organization for security can be created to take control over different products made by the mobile phone provider to ensure the protection of data as well as personal identity.

REFERENCES

[1] Akash Kumar Mahato, Ambar Kumar, Akashdeep Singh, “Mobile Phone Cloning”, Vol.2Issue IX, and September2014 ISSN: 2321-9653 retrieved from https://www.ijraset.com/fileserve.php?FID=902

[2] “CDMA-Technology”, retrieved from https://www.tutorialspoint.com/cdma/cdma_technology.htm on 01/02/2019

[3] "Code Division Multiple Access", retrieved from https://www.en.m.wikipedia.org on 30/01/2019

[4] “What is an ESN, IMEI, SIM, MSN (SN) and PIN?”, published 10/16/2007 02:42PM retrieved from http://ecenter.custhelp.com/app/answers/detail/a_i

d/512/~/what-is-an-esn%2C-imei%2C-sim%2C-msn-%28sn%29-and-pin%3F on date 04/02/2019

[5] Aaruni Goel Madhup Sharma Paresh Pathak, "The Approaches to Prevent Cell Phone Cloning in Cdma Environment", International Journal of Computer Applications (0975 – 8887) Volume 45– No.21, May 2012 pp.: 17 retrieved from https://pdfs.semanticscholar.org/7a86/9e0c574b43d273605fbd5029b137f34ac109.pdf on 04/02/2019

[6] Megha. Mutalik Desai, "Mobile Phone Cloning:Past, Present, Precaution", International Journal of Recent Advances in Engineering & Technology (IJRAET) retrieved from http://www.irdindia.in/journal_ijraet/pdf/vol3_iss2/6.pdf on 21/03/2019

[7] Akash Kumar Mahato, Ambar Kumar, Akashdeep Singh, "Mobile Phone Cloning", INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET), Vol. 2 Issue IX, September 2014 ISSN: 2321-9653 retrieved from https://www.ijraset.com/fileserve.php?FID=902 on 21/03/2019

[8] M.Dhivya, S.Dhivya, V.Abiram, "Security Measures for CDMA Mobile Phone Cloning", Volume III, Issue IX, September 2014 IJLTEMAS ISSN 2278 – 2540 retrieved from https://www.ijltemas.in/DigitalLibrary/Vol.3Issue9/76-79.pdf on 21/03/2019