ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICITCSA 2017

Pioneer College of Arts and Science, Coimbatore

Vol. 6, Special Issue 1, January 2017

Mobile Phone Cloning

Dr. S. Kirshnaveni[1], M.Kanagapriya[2], K. Zuvairiya[2]

[1]Assistant Professor, Dept. Computer Applications, Pioneer College of Arts & Science, Coimbatore, Tamilnadu, India

[2]III BCA Student, Dept. Computer Applications, Pioneer College of Arts & Science, Coimbatore, Tamilnadu, India

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. It is a relatively new invention, so not all people are quite familiar with its possibilities, in good or in bad. Its newness also means intense competition among mobile phone service providers as they are attracting customers. The major threat to mobile phone is from cloning.

Keywords: GSM, CDMA, ESN, MIN, PIN, IMEI, CTIA.

I. INTRODUCTION

Cloning is the creation of an organism that is an exact genetic copy of another .This means that every single bit of DNA is the same between the two.

Mobile Phone Cloning is copying the identity of one mobile telephone to identity of one mobile telephone to another mobile telephone. The purpose of mobile phone cloning is making fraudulent telephone calls. The bills for the calls go to the legitimate subscriber.

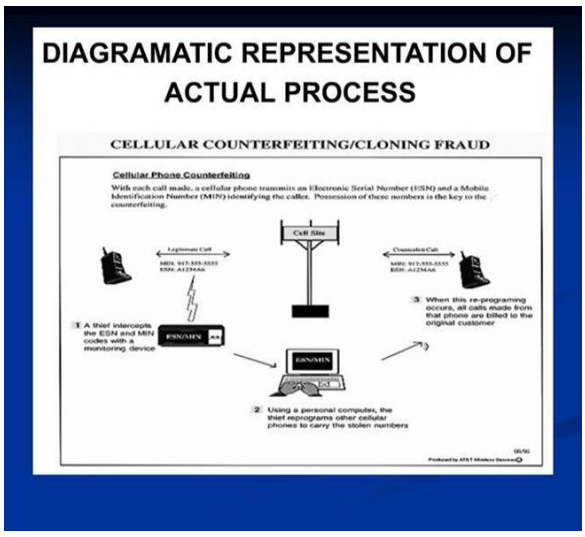

Fig1: Structure of an Actual Mobile Phone Cloning

The early 1990's were boom times for eaves droppers. 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.

II. HISTORY OF CLONING

On 13th April 1998, the Smartcard Developer Association and the ISAAC security research group announced a flaw in the authentication codes found in digital GSM cell phones. This allows an attacker with physical access to a target phone to make an exact duplicate (a ``clone'') and to make fraudulent calls billed to the target user's account.

In India mobile phone cloning first came to light in January 2005 when the Delhi police arrested a person with 20 cell phones, a laptop, a SIM scanner, and a writer. The accused was running an exchange illegally wherein he cloned CDMA-based mobile phones. He used software for the cloning and provided cheap international calls to Indian immigrants in West Asia. A similar racket came to light in Mumbai resulting in the arrest of four mobile dealers.

III. FEATURE OF MOBILE PHONE CLONING

GSM (Global System for Mobile Communications)

→ A digital cellular phone technology based on TDMA GSM phones use a Subscriber Identity Module (SIM) card that contains user account information.

→Any GSM phone becomes immediately programmed after plugging in the SIM card, this allowing GSM phones to be easily rented or borrowed. Operators who provide GSM service are Airtel, Vodafone etc.

Software used for GSM

If a cloner manages to also clone the IMEI (International Mobile Station Equipment Identity) number of the handset, for which software's are available, there is no way he can be traced. "BLUETOOTH HAC" is software available in the market which is used to hack/clone GSM phones.

CDMA (Code Division Multiple Access)

→ A method for transmitting simultaneous signals over a shared portion of the spectrum. There is no Subscriber Identity Module (SIM) card unlike in GSM.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICITCSA 2017

Pioneer College of Arts and Science, Coimbatore

Vol. 6, Special Issue 1, January 2017

→ An operator who provides CDMA service in India is Reliance and Tata Indicom.

Software Used For CDMA

If PIN (Personal Identification Number) and ESN (Electronic Security Number) are known a mobile phone can be cloned in seconds using some Software's like "PATAGONIA" which is used to clone CDMA phones.

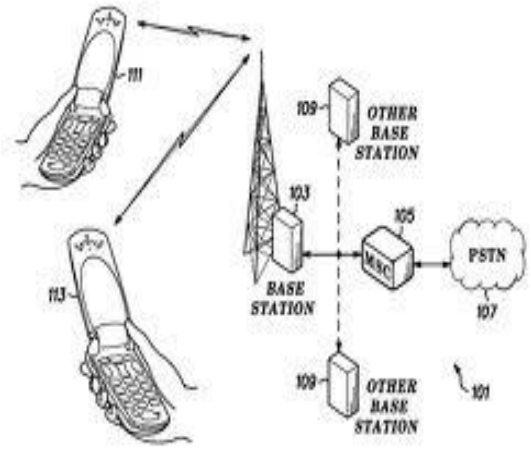

Fig2: Structure of an Software Process

IV. Security Functions of the GSM and CDMA

As background to a better understanding of the attacks on the GSM and CDMA network the following gives a brief introduction to the Security functions available in GSM.

The Following Functions Exist

→Access control by means of a personal smart card called (subscriber Identity module, SIM) and PIN (personal identification number),

→Authentication of the users towards the network carrier and generation of a session key in order to prevent abuse.

→Encryption of communication on the radio interface, i.e. between mobile Station and base station.

→Concealing the users' identity on the radio interface, i.e. a temporary valid Identity code (TMSI) is used for the identification of a mobile user instead Of the IMSI.

V. How serious the cloning fraud problem?

→ 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 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.

→The Cellular Telecommunications Industry Association (CTIA) estimates that financial losses due to cloning fraud are between $600 million and $900 million in the United States. Some subscribers of Reliance had to suffer because their phone was cloned. Mobile Cloning is in initial stages in India so preventive steps should be taken by the network provider and the Government.

VI. How to check whether your cell phone is cloned or not

Unfortunately, there is no way the subscriber can detect cloning.

Events like call dropping or anomalies in monthly bills can act as tickers.

But some points mentioned below can help you

Symptoms are:

- **a.** Frequently wrong numbers.
- **b.** Calls that hang- up after you answer.
- **c.** Problems making outgoing calls.
- **d.** Incoming calls that constantly get the busy signal.
- **e.** Large phone bills to numbers you have never heard of.
- **f.** Problem accessing your voicemail.

VII. Duplicate detection method

Duplicate detection is a method in which the network sees the same phone in several places at the same time. So the service provider will disconnect all of them so that the original customer will contact the operator questioning about loss of service.

RF Finger Printing

Some operator use Radio Frequency Fingerprinting, it is originally a military technology. Even identical radio equipment has its own „fingerprint". So the network software stores and compares fingerprints for all the phones that it sees. This way, it will spot the cloned phone with same identity, but different fingerprints.

Usage Profiling

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.

Call Counting

Call Counting is also a way to check the situation where 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.

Pin Codes

Prior to placing 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 by entering the PIN code again. Operators may share PIN information to enable safer roaming.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICITCSA 2017

Pioneer College of Arts and Science, Coimbatore

Vol. 6, Special Issue 1, January 2017

VIII. How to prevent from cloning?

→ The best way to prevent your SIM card or mobile phone from being cloned is to use Authentication feature.
→Authentication is a mathematical process by which identical calculations are performed in both the network and the mobile phone.
→These calculations use a key that is pre-programmed into both the mobile phone and the network before service is activated.
→Cloners do not have access to this key, and therefore it is nearly impossible for them to clone.

IX. To Check Out Your Mobile Phone Authentication Is Capable

→If the phone supports TDMA or CDMA digital radio, then yes. Otherwise, it depends on how old the phone is and the make and model.
→Almost all phones manufactured since the beginning of 1996 support the Authentication function. The best bet is to check with your service.

X. 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.
→Therefore it is absolutely important to check the functions of the security system which has been implemented once a year and if necessary update or replace it with better security system.

REFERENCES

[1] www.studymafia.org
[2] www.wikipediya.com
[3] www.google.com