INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Mobile Phone Cloning

Akash Kumar Mahato[1], Ambar Kumar[2], Akashdeep Singh[3]

[1,2,3](B.Tech 3rd sem) Dept. of Computer Science Engineering, Dronacharya College of Engineering, Gurgaon, India

Abstract—This paper describes about the cell phone cloning with achievement in GSM and CDMA technology phones. It gives an insight into the security method in CDMA and GSM phones all along with the loop holes in the systems and discusses on the different ways of preventing this cloning. Also, the future threat of this scam is being elaborated.

Cloning is the practice of taking the programmed information that is stored in a valid mobile phone and criminally programming the same information into another mobile phone. The result is that the "cloned" phone can build and get calls and the charges for those calls are billed to the valid subscriber. The service supplier network does not have a way to distinguish the valid phone and the "cloned" phone.

Keywords--- GSM (Global System for Mobile Communications), CDMA (Code Division Multiple Access), ESN (Electronic Security Number), MIN (Mobile Identification Number), SCN (Station Class Mark), DDI (Digital Data Interface).

I. INTRODUCTION

Remember frogs were the first animals to be cloned using embryonic cells, in the early 1950's. By the early 1980's embryonic cell techniques were being used to clone laboratory animals, including mice & livestock, including cattle and sheep. While the argue on the beliefs of cloning continues, human race, for the first time, are faced with a clearer and harmful version of cloning and this point it is your mobile phone that is the target.

Millions of mobile phones users, be it GSM or CDMA, run at threat of having their phones cloned. As a mobile phone user if you have been receiving enormously high bills for calls that you never placed, chances are that your mobile phone is possibly cloned. unluckily, there is no way the subscriber can detect cloning. actions like call falling or anomalies in monthly bills can act as tickers.

According to media information, recently the Delhi (India) police detained a person with 20 mobile- phones, a laptop, a SIM scanner, and a writer. The accused was running an exchange criminally wherein he cloned CDMA based cell phones. He used software named Patagonia for the cloning and provided cheap international calls to Indian immigrants in West Asia.

II. HOW MOBILE PHONE WORKS?

Mobile phones send radio frequency transmissions through the sky on two distinct channels, one for voice communications and the other for control signals. When a mobile phone builds a call, it normally transmits its

Electronic Security Number (ESN), Mobile Identification Number (MIN), its Station Class Mark (SCM) and the number called in a tiny burst of data. This burst is the short buzz you hear after you press the SEND button and before the tower catches the data. These four things are the components the cellular supplier uses to ensure that the phone is programmed to be billed and that it also has the identity of both the customer and the phone. MIN and ESN is collectively known as the 'Pair' which is used for the cell phone identification.

When the cell site gets the pair signal, it determines if the requester is a valid registered user by comparing the requestor's pair to a cellular subscriber list. Once the cellular telephone's pair has been recognized, the cell site emits a control signal to permit the subscriber to place calls at will. This practice, known as Anonymous Registration, is carried out each time the telephone is turned on or picked up by a new cell site.

III. WHAT IS MOBILE PHONE CLONING?

Cloning of mobile phones means copying the subscriber information from one phone onto the other with the intention of obtaining free calls. The other mobile phone becomes the exact replica of the original mobile phone like a clone. As a result, while calls can be made from both phones, only the original is billed.

IV. WHEN DID CELL CLONING START?

The early 1990s were boom times for eavesdroppers. Any curious youngster with a Tandy scanner could listen in to nearly any analogue mobile phone call. As a result, cabinet minister, company chiefs and celebrities usually 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 usually existing adjustment for the Motorola "brick" phones, such as the classic, the ultra classic, and the model 8000.

V. HOW IS CELL CLONING DONE?

Cloning concerned modifying or replacing the EPROM in the phone with a new chip which would allow you to organize an ESN (electronic serial number) via software. You would also have to change the MIN (mobile identification number). When you had effectively 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 pair, your phone was an effective clone of the other phone. ESN/MIN pair were discovered in several ways:

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

Cloning silent works under the AMPS/NAMPS system, but has fallen in attractiveness as older clone able phones and more difficult to find and newer phones have not been successfully demonstrated under GSM, but the practice is not simple and it presently remains in the province of serious hobbyists and researchers.

VI. LOOP HOLES IN CELL PHONE NETWORKS

ESN/MIN data is NOT encrypted on the way to the MSC (Mobile Switching Centre) for further verification. Thus, scanning the sky-waves for this data if you wish to clone a phone. By changing ESN and MIN, the cellular carrier will accept the call and bill it to either a wrong account or provide service based on the fact that it is NOT a disconnected receiver. It will also look at the other two components, in order to insure that it is actually a cellular phone and to forward billing information to that carrier.

VII. HOW TO DETECT THE CLONING?

There are several ways to identify the cloning. One of the most fruitful and mostly used ways are discussed here

7.1. *Replica recognition:*

If the service supplier finds out the traces of the same phone in the at several places at a time, then the service supplier has to shut down the complete network. If the network is down, the valid user will respond back to the service supplier and the ESN/ MIN can be reprogrammed. The fake user will be automatically bypassed. The only loophole in this system is that it is very much difficult for the service supplier to trace out the duplicates.

7.2. Pa*ce 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 pace trap. For example, if first call is made from Delhi and another is made from Kolkata within 10 minutes, or if the calls are made from India and America within 5 minutes, pace Trap is encountered.

7.3. *RF (Radio Frequency):*

Radio fingerprinting is a practice that identifies a cellular phone or any other radio transmitter by the unique "fingerprint" that characterizes its signal transmission. An electronic fingerprint builds 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. If the service supplier spots the same fingerprint of one existing unit, it temporarily suspends the service.

7.4. *Custom Profiling*:

The custom patterns of the users are studied. If any inconsistency are noticed, the customer is contacted. For example, if a valid user is normally used 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.

7.5. *Call Counting*:

Each phone records the logs of the service utilized. Each service supplier 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

7.6. *PIN Codes:*

The service supplier can assign a smart PIN (Personal Identification Number) code to each user. Before calling, the user will request for service license from service supplier. 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. Regular wrong number phone calls
2. Complexity in placing outgoing calls.
3. Complexity in retrieving voice mail messages.
4. Incoming calls continuously receiving busy signals or wrong numbers.
5. Strange call appearing on your phone bills.

VIII. HOW DO I KNOW THAT MY MOBILE IS GETTING CLONED?

There's nothing that can help a subscriber detect cloning.There are several techniques that can be adopted by service Suppliers though. However, huge mobile bills could act as a ticker for subscribers.

IX. WHO IS SAFE?

Both GSM and CDMA handsets are prone to cloning. Technically, it is easier to clone a CDMA handset over a GSM one, though cloning a GSM cell phone is not impossible. There are also Internet sites that provide information on how one could go about hacking into cell-phones.

X.CLONING CDMA CELL PHONES

Mobile telephone thieves monitor the radio frequency spectrum and steal the cell phone pair as it is being anonymously registered with a cell site. The technology uses spread-spectrum techniques to share bands with multiple conversations. Subscriber information is also encrypted and transmitted digitally. CDMA handsets are particularly vulnerable to cloning, according to experts. First generation mobile cellular networks allowed fraudsters to pull subscription data (such as ESN and MIN) from the analog sky interface and use this data to clone phones. A device called as DDI, Digital Data Interface can be used to get pairs by simply making the device mobile and sitting in a busy traffic area (freeway overpass) and collect all the data you need. The stolen ESN and EMIN were then fed into a new CDMA handset, whose existing program was erased with the help of downloaded software. The buyer then programs them into new phones which will have the same number as that of the original subscriber.

XI. CLONING GSM PHONES

GSM handsets, on the contrary, are safer, according to experts. Every GSM phone has a 15 digit electronic serial number (referred to as the IMEI). It is not a particularly secret bit of information and you don't need to take any care to keep it private. The important information is the IMSI, which is stored on the removable SIM card that carries all your subscriber information, roaming database and so on. GSM employs a fskyly sophisticated asymmetric-key cryptosystem for over-the-sky transmission of subscriber information. Cloning a SIM using information captured over-the-sky is therefore difficult, though not impossible. As long as you don't lose your SIM card, you're safe with GSM. GSM carriers use the COMP128 authentication algorithm for the SIM, authentication center and network which build GSM a far secure technology.

XII MOBILE PHONE SAFETY MEASURES

Cellular operators in many countries have deployed various technologies to deal with this threat. Some of them are as follows:

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. Pace 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.

Some operators also use Radio Frequency Fingerprinting, originally a military technology. Even the same 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.

Custom Profiling is another way wherein profiles of customers' phone usage are kept, and when inconsistency are noticed, the customer is contacted. For example, if a customer normally builds only local network calls but is suddenly placing calls to foreign countries for hours of sky-time, it indicates a possible clone.

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.

XIII. SOME FACTS AND FIGURES

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. In one case, more than 1,500 telephone calls were placed in a single day by cellular phone thieves using the number of a single unsuspecting owner.

A Home Office report in 2002 revealed that in London around 3,000 mobile phones were stolen in one month alone which were used for cell phone cloning. Authorities, in the case, estimated the loss at $3,000 to $4,000 for each number used in cell phone cloning.

According to a school of thought, the Telecom Regulatory Authority of India (TRAI) should issue a directive, which holds the operators responsible for duplications of mobile phones.

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. "It's like a virus hitting the computer. The software which is used to hack into the network is different, so operators can only keep upgrading their security firewall as and when the hackers strike," says a Qualcomm executive.

XIV. HOW CAN ORGANIZATIONS HELP THEMSELVES?

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.

XV. CONCLUSION

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.

REFRENCES

[1] Fundamentals of Mobile and Pervasive Computing.
[2] http://en.wikipedia.org/wiki/radiofingerprinting
[3] http://en.wikipedia.org/wiki/phone_cloning
[4] http://seminarproject.com/threat-mobile-phone-cloning-full-report
[5] http://edutwin.com/t-mobile-phone-cloning-full-report