ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

Approaches and Techniques to Prevent Cloning in Mobiles

R.Waheetha, J.Maria Merceline Vijila

Head & Associate Professor, Department of Computer Science, Holy Cross Home Science College, Thoothukudi, Tamil Nadu, India

Associate Professor, Department of Computer Science, Holy Cross Home Science College, Thoothukudi, Tamil Nadu, India

ABSTRACT: Mobile phone cloning is copying the identity of one mobile telephone to another mobile telephone. 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. 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. . 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 : GSM, CDMA, IMEI, 8-digit PIN, Patagonia, Velocity Trap, Mobile Identification Number

I.INTRODUCTION

Cloning is the process of taking the programmed information that is stored in a legitimate mobile phone and illegally programming the identical information into another mobile phone. Cell phone cloning is a technique wherein secured data from one cell phone is transferred into another phone. The other cell phone becomes the exact replica of the original cell phone like a clone. As a result, while calls can be made from and received by both phones, only the legitimate subscriber is billed as the service provider network does not have a way to differentiate between the legitimate phone and the "cloned" phone. The cloner can set the options to ring his phone when you make a call and you will have no idea that the cloner is listening from his own mobile. He can read text message, phone book entries, look at pictures etc. Also he can dial phone numbers from their phone and a whole lot more. So when one gets huge bills, the chances are that the phone is being cloned. Millions of cell phones users, be it GSM or CDMA, run at risk of having their phones cloned.

II. PROCESS

Cloning is the process of taking the programmed information that is stored in a legitimate mobile phone and illegally programming the identical information into another mobile phone. The culprits clone and hack into your phone using software's that are easily available, once the software is installed they just need the unique IMEI number of the phone and they can digitally imprint these numbers on any of the phone they want. Once this is done they can send messages, make calls to anyone and the person whose phone has been cloned and hacked will be held responsible.

A.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.

DOI: 10.15680/IJIRCCE.2016. 0412081

Any GSM phone becomes immediately programmed after plugging in the SIM card, thus allowing GSM phones to be easily rented or borrowed. Operators who provide GSM service are Airtel, Hutch etc. cloning GSM phones is achieved by cloning the SIM card contained within, not necessarily any of the phone's internal data. GSM phones do not have ESN or MIN, only an IMEI number. GSM SIM cards are actually copied by removing the SIM card and placing a device between the handset and the SIM card and allowing it to operate for a few days and extracting the KI, or secret code. Cloning has been successfully demonstrated under GSM, but the process is not easy and it currently remains in the realm of serious hobbyists and researchers.

B.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.Operators who provides CDMA service in India are Reliance and Tata Indicom. Cloning involved modifying or replacing the EPROM in the phone with a new chip which would allow you to configure an ESN (Electronic serial number) via software. You would also have to change the MIN (Mobile Identification Number). When you had successfully changed the ESN/MIN pair, your phone was an effective clone of the other phone. Cloning required access to ESN and MIN pairs.

III. IMPACT OF CLONING

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 persons. Often these cloned phones are used to place hundreds of calls, often long distance, even to foreign countries, resulting in thousands of dollars in airtime and long distance charges. Cellular telephone companies do not require their customers to pay for any charges illegally made to their account, no matter how great the cost. But some portion of the cost of these illegal telephone calls is passed along to cellular telephone consumers as a whole.

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.His phenomenon is especially prevalent in drug crimes. Drug dealers need to be in constant contact with their sources of supply and their confederates on the streets. Traffickers acquire cloned phones at a minimum cost, make dozens of calls, and then throw the phone away after as little as a days' use.

In the same way, criminals who pose a threat to our national security, such as terrorists, have been known to use cloned phones to thwart law enforcement efforts aimed at tracking their whereabouts.

IV.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.

V. SECURITTY/PREVENTION

***A. ARE OUR CELL PHONES SECURED*?** Too many users treat their mobile phones as gadgets rather than as business assets covered by corporate security policy. Did you realize there's a lucrative black market in stolen and "cloned" SIM cards? This is possible because Sims are not network specific and, though tamper-proof, their security is flawed. In fact, a SIM can be cloned many times and the resulting cards used in numerous phones, each feeding illegally off the same bill. But there are locking mechanisms on the cellular phones that require a PIN to access the phone. This would dissuade some attackers, foil others, but might not work against a well financed and equipped attacker. An 8-digit PIN requires approximately 50,000,000 guesses, but there may be ways for sophisticated attackers to bypass it.

With the shift to GSM digital - which now covers almost the entire UK mobile sector - the phone companies assure us that the bad old days are over. Mobile phones, they say, are secure and privacy friendly. This is not entirely true. While the amateur scanner menace has been largely exterminated, there is now more potential than ever before for privacy invasion. The alleged security of GSM relies on the myth that encryption - the mathematical scrambling of our conversations - makes it impossible for anyone to intercept and understand our words. And while this claim looks good on paper, it does not stand up to scrutiny. The reality is that the encryption has deliberately been made insecure. Many encrypted calls can therefore be intercepted and decrypted with a laptop computer.

B.WHAT ARE EMIE AND PIN?

ESN mean Electronic Serial Number. This number is loaded when the phone number is manufactured. this number cannot be tampered or changes by the user or subscriber. if this number is known a mobile can be cloned easily.

Personal Identification Number (PIN).every subscriber provides a Personal Identification Number (PIN) to its user. This is a unique number. If PIN and ESN are know a mobile phone can be cloned in seconds using some software's like Patagonia. Which is used to clone CDMA phones.

C.WHAT IS PATAGONIA?

Patagonia is software available in the market which is used to clone CDMA phone. Using this software a cloner can take over the control of a CDMA phone i.e. cloning of phone. There are other Software's available in the market to clone GSM phone. This software's are easily available in the market. A SIM can be cloned again and again and they can be used at different places. Messages and calls sent by cloned phones can be tracked. However, if the accused manages to also clone the IMEI number of the handset, for which software's are available, there is no way he can be traced.

VI. HOW TO PREVENT MOBILE CLONING?

Uniquely identifies a mobile unit within a wireless carrier's network. The MIN often can be dialed from other wireless or wire line networks. The number differs from the electronic serial number (ESN), which is the unit number assigned by a phone manufacturer. MINs and ESNs can be checked electronically to help prevent fraud.

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.

How do service providers handle reports of cloned phones? Legitimate subscribers who have their phones cloned will receive bills with charges for calls they didn't make. Sometimes these charges amount to several thousands of dollars in addition to the legitimate charges.

Typically, the service provider will assume the cost of those additional fraudulent calls. However, to keep the cloned phone from continuing to receive service, the service provider will terminate the legitimate phone subscription. 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 number changes.

VII.WHAT EXACTLY IS AUTHENTICATION?

Authentication is a mathematical process by which identical calculations are performed in both the network and the mobile phone. These calculations use secret information (known as a "key") preprogrammed into both the mobile phone and the network before service is activated. Cloners typically have no access to this secret information (i.e., the key), and therefore cannot obtain the same results to the calculations.

A legitimate mobile phone will produce the same calculated result as the network. The mobile phone's result is sent to the network and compared with the network's results. If they match, the phone is not a "clone."

VIII.ROLE OF SERVICE PROVIDER TO COMBAT CLONING FRAUD?

They are using many methods such as RF Fingerprinting, subscriber behavior profiling, and Authentication. RF Fingerprinting is a method to uniquely identify mobile phones based on certain unique radio frequency transmission characteristics that are essentially "fingerprints" of the radio being used. Subscriber behavior profiling is used to predict possible fraudulent use of mobile service based on the types of calls previously made by the subscriber.

Calls that are not typical of the subscriber's past usage are flagged as potentially fraudulent and appropriate actions can be taken. Authentication has advantages over these technologies in that it is the only industry standardized procedure that is transparent to the user, a technology that can effectively combat roamer fraud, and is a prevention system as opposed to a detection system.

IX. 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

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.

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.

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

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.

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

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

X. FUTURE THREATS

Resolving subscriber fraud can be a long and difficult process for the victim. It may take time to discover that subscriber fraud has occurred and an even longer time to prove that you did not incur the debts. As described in this article there are many ways to abuse telecommunication system, and to prevent abuse from occurring it is absolutely necessary to check out the weakness and vulnerability of existing telecom systems. If it is planned to invest in new telecom equipment, a security plan should be made and the system tested.

XI.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

1. Fundamentals of Mobile and Pervasive Computing   Frank Adelstein, Sandeep Gupta.
2. Introduction to Telecom Communication Converging Technologies 1st Edition Kimberly Massey
3. Pro-Active Prevention of Clone Node Attacks in Wireless Sensor
Networks Anandkumar, K.M, C. Jayakumar Journal of Computer Science 8 (10): 1691-1699, 2012 ISSN 1549-3636.
4. 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 SantaCatarina (UFSC)
5. Ken Hutchiunson, *Wireless Intrusion Detection Systems*, SANS Institute, October 2004
6. http://www.cdmasoftware.com/eng.html
7. http://wiretap.spies.com
8. http://www.hackinthebox.org/