The Brief Study of Mobile Phone Cloning

Prof Archana Jyothikiran, Prof. Sujatha. K, Prof Archana KV

Faculty of Engineering and Technology, Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112

Email Id- archana.j@inurture.co.in, sujatha.k@inurture.co.in

ABSTRACT: Cloning mobile phones is a practice of taking the programs stored on a legitimate mobile phone and of crime in other mobile phones to program the same stuff. Mobile phone piracy has recently become more prevalent and is, of course, a serious matter in the world of computing as it is rising at an alarming pace. For many years, mobile contact has been available and is a big industry. It provides its customers a valuable service that they can pay a significant amount over a fixed-line phone to chat and talk freely. It is prone to fraud because of its value and the money involved in the business. Sadly, with the proliferation of mobile communication, improvement in the security standards has not kept pace. It is a lovely place for offenders with a few apps of mobile communication. It is a relatively new invention, so not everybody knows its implications in good or bad. It is also creative and attracts clients by the vigorous competition between mobile telephony service providers. Cloning is the biggest threat to mobile phones.

KEYWORDS: Handheld Device, Cloning, Cell phone cloning, Electronic Security Number, Mobile communication.

INTRODUCTION

Cell phones are dynamic, heat sensitive, cold and excess moisture electronic devices. However, the sensitivity of a mobile phone is not limited to extreme weather. In comparison to newer digital phones, analogy mobile phones can be cloned. This means you can tap into the personal identification number of your cellular phone and make calls to the same account. In other words, someone can steal your telephone number with a little technological know-how and can charge your phone calls. The integral part of our lives is cell telephones. The 3-E's communication cell phone works with ease of use, efficient and economic. It has a lot to do with fraud as well. The cell phone as a hardware is tough for the safety of the different manufacturers. The type of devices violates the various levels of safety. The security procedures on mobile telephones CDMA and GSM are different from the security hole of these cell phones. Cloning cell phones is one of the greatest risks to health. In India it's not just a huge threat, but also elsewhere. The paper addresses the harmful effects of cloning and different methods of avoiding cloning. This scam will be built to counter the potential threat. The process of cloning is illegal and uses knowledge from mobile telephones for criminal purposes. The data is installed illegally on another cell phone [1]. The second telephone is considered a cell clone. The cloned mobile phone is installed and the costs are paid to the original subscriber for those appeals. Whether the call is a legitimate phone or cloned phone, the service provider network does not.

Mobile telephone is the first electronic device cloned after another lifetime. Nevertheless, for illicit and criminal activities, it has been sadly cloned illegally. Either GSM or CDMA are primarily used by mobile telephone. Not only can the mobile phone be cloned for calling but confidential and private information can be stored on the mobile telephone. The first explanation or distinction is that the cell phone is cloned because the owner of a mobile phone collects substantial charges on calls never made by him. Cloning still operates in compliance with the NAMPS/AMPS systems and has still sunk into necessity as it is difficult to find existing phones which can be cloned and more modern telephones are not effectively available. Cloning was effectively displayed in GSM, although it is not a simple procedure and continues the field of genuine specialists and scientists at this time. Cloning as a way to get away with the law is also difficult provided the additional aspect of a radio specific mark present in the flag of any mobile phone. This particular mark is kept alive, no matter whether the ESN or MIN is altered [2]. The Fingerprints and the ESN and MIN can be used by cell phone organizations to classify extorsion cases.

HISTORY

In the early 1991s, eavesdroppers were booming. A curious teenager with a £100Tandy scanner can hear almost every phone call from analogy. Smartphone's replication began with "bags" phone from Motorola and achieved its height in middle 90's by a regularly accessible move to the "bricks" phone, including the Standard, Mega-Modern, and 7000. The Wireless Telephone Security Act of 1997 in the UK bans phone cloning. On 14 April 1997, a failure of verification code used in numeral GSM smartphones was confirmed by the Smartcard Developer Association and the ISAAC safety research community. This allows the physically accessible intruder to make exact replicates (a "clone") and charge the target user's account for fraudulent calls. Mobile cloning came out in India, in January 2006, when an individual with 20 cellular phone, the laptops, a SIM electronic scanners and the writer was detained by Delhi police. The defendant was unlawfully selling cellular phone based on CDMA [3]. He utilized cloning tools and supported Indian immigrants in West Asia with cheap international calls. The arrest of four mobile dealers resulted in a similar scam in Mumbai.

WHAT IS MOBILE CLONING?

Cloning of mobile phones is a process where secure data is moved from a mobilephone to other mobilephone. The other handset is the exact copy of the original handset. Mobile phone cloning is considered mobile phone piracy and has existed worldwide for decades [1]. This crime has recently arrived in India. It is commonly done to make phone calls that are fake. Calling and receiving calls may be made by the cloned handset, but the subscriber of the original telephone is paid. Most cell phone users today are at risk of being cloned to their phones, whether it be a Global Cell Communication System (GSM) or CDMA. And the worst thing is that you can't do anything to prevent it. The cloner will even listen to the calls that we don't know about when we receive or make phone calls [4]. Although several security algorithms are provided for communication channels, cloners are removed with the aid of loop hole systems. There is also the possibility that the phone may be cloned if you collect large bills.

ELECTRONIC SERIAL NUMBER (ESN)

The single ID number that the supplier incorporates into a wireless phone. The ESN is sent to the base stop immediately, so the mobile switching office of the wireless carrier can verify the validity of the call. In the field the ESN cannot be easily modified. The ESN varies from the telephone identification number that is the identifier of the cellular operator for a network phone. In order to avoid fraud and apps, MINs and ESNs can be electronically reviewed. Each ESN has three different fields: one producer code (eight bit), one serial number (18-bit), and one extension (6-bit). Each ESN has three fields [5]. The serial number and the extension are combined to classify each mobile device in use into a single 24-bit serial number. 256 manufacturers can be separated by ESN under this assignment model. If this number was not satisfactory, however, the ESN assignment for 32-bit was changed, representing a 14-bit producer code and an ID for 18-bit units.

MOBILE IDENTIFICATION NUMBER (MIN)

The MIN is a number that defines an exclusively cell phone subscriber. The length of the MINs is 34-bits. Often the first 10 bits are known as MIN2, while the last 24 are called MIN1. They're all known together as the MIN [6].

ADVANCED MOBILE PHONE SERVICE (AMPS)

This is a common system in the United States for Analog signal mobile telephone service and is also used in other countries. AMPS assign frequency ranges to cellular phones within a spectrum of 800 and 900 Megahertz (MHz). The bands are split in a sub band of 30 kHz, known as channels. The receiving channels are called reverse channels and forward channels are named. By using multiple access frequency division (FDMA), the divide of spectrum into sub-band channels is accomplished [7].

HOW MIN/ ESN ARE DETECTED

Cellular robberies can catch MIN /ESNs by devices such as ESN smartphone readers or DDIs. DDIs are specially built instruments for MIN /ESN intercepting. With cell theft, which tracked the transmission of the radio waves from the mobile phones of the legal subscriber, simply sitting close to active road where he amount of phone traffic is higher. Numbers can be manually registered, stored one-by-one or transferred to the machine in the box and later. The use of MIN /ESN readers can also increase difficulty of identification from inside the house, workplace and hotel room of the offender [8].

HOW MIN/ ESN ARE PROGRAMMED ON ANOTHER PHONE

To reprogram a handset, a system stuffed with specialized software is used to move the ESN/MINs for a device that only has the purpose of cloning telephones. The device is linked to mobile phones and new data is registered on phones. Less secret, concealed apps are also used to clone mobile phones. Cloning of computers or copycat boxes does not include plug and ES-Pro which is around the size of a Pager or small calculator. It takes 10-15 minutes per phone for the entire programming cycle [9].

GLOBAL SYSTEM FOR MOBILE COMMUNICATION

This system is a digital cellular telephone system, commonly utilized in the world. GSM is the commonly utilized among 3 optical wireless telephone systems by using a time-dividing multiple access (TDMA) variant. Global System for Mobile Communication digitize and compress information and then transmits it to its own time slot on the channel with two other sources of user data. This operates with either the frequency band 900 MHz or 1700 MHz. Because several GSM networks operator have traveling contracts with international network operator, as they visit other countries, customers also choose to use their mobile phones. Cloning has proven popular in the Multi-Access Code Division (CDMA), but uncommon in GSM, amongst most commonly utilized mobiles[10]. Cloning of GSM phones, however, does not necessarily require the cloning of internal data on the SIM card. No ESN or MIN on GSM phones, just an IMEI number. In addition, GSM SIM cards are copied with the removal of a SIM cards and barrier put among phone and SIM cards that allows for several days to work with KI or secret code removal. Duplicating has been demonstrated effectively in GSM, although it is hard and persists in domain of major investigators [11].

CLONING CDMA MOBILE PHONES

CDMA is a form of simultaneous signal propagation around a specific part of continuum. Unlike GSM, there is no SIM card. Qualcomm is designing the wireless cellular interface for CDMA. CDMA is a 2G standard for mobile telecoms. Under CDMA, different radio connections are allocated the same frequencies. It is a multiplexing method used to maximize the single-channel bandwidth. CDMA is a multiplexing type, allowing the usable bandwidth to be balanced by many signals. Mobile phone robbery tracks the spectrum of RF and steals the mobile phone couple as the cell phone pair is secretly registered. The system uses techniques of wide spectrum to connect bands of multiple conversations [12]. The knowledge of the subscriber is also encoded then digitally communicated. According to researchers, CDMA systems are mainly susceptible to duplicating.

Mobile telecom 1st-gen systems permitted frauds by Analog space interfaces to pump subscription information (such as ESNs and MINs) into the clone. Digital data interface can be used as a DDI tool to access pairs easily by mobilising and sitting in a quiet area of the road and gathering every detail that is require. The filched EMIN & ESN were then supplied in to the novel CDMA computer that has already been removed using the program that was downloaded. The user instead assigns it to new phones that are equivalent to the initial customer. In the recent case, however, CDMA & GSM set are perfectly cloneable. In Delhi trial, the accused utilized the app Patagonia to duplicate CDMA phone alone. Computer packages are however also ideal for copying GSM-telephones (e.g. Airtel, BSNL, Hutch, Idea). Awareness of the IMEI or the number of the instrument suffices for the Clone of a GSM phone.

HOW TO IDENTIFY MOBILE PHONES DUPLICATING IN THE NETWORKS

Numerous communications firms that introduce steps to detect/reduce fraud. The goal is for possible fraudulent activities to be identified. Many of such steps are basic, like the system search for reaching call received concurrently or over with the same mobile number, an unlikely case. Access to call logs and a decision on the operation takes place here. In fact, barely local phone call are permitted and the real tenant is called about condition and number is applied. It is also possible for the program to 'decrease' all numbers and avoid calls. It is a quick way to maintain interaction with customers. Since nobody wants to be service less. The exception reports are then available [8]. In this situation barely local telephone call are permitted and communicate with the company is received in conjunction with company, until this stage is reached. In fact, the true condition can only be verified by the customer. Clearly, between the consumer and the service provider a degree of confidence must exist as the customer's word on use must be acknowledged. How genuine the vast majority of clients are is amazing [13]. The operator gives the consumer the ability to keep the original number after a cell phone has been cloned, but to switch freely to the new service. It of course would not allow someone to pay for unheard calls, including a reduction in their account.

1. *Speed Trap*

Phone system appears to travel with unusual or impossible velocities. If a call is made in Helsinki, like, calls are made 5 minute after, the two calls have a same identity on the network, this time in Tampere. If the phone is moving continuously or the location is in an unlikely period of time far from the last call, it is subjected to a speed trap. If the initial call is made within fifteen minutes from Mumbai, or if the call from Thane and Ghansoli is made within 5 minutes, for example, Velocity Trap is identified.

2. *Duplicate Detection*

If the provider detects signs of the same telephone at multiple occasions, the provider must turn the entire network off. The legitimate user must respond to the service provider when the network is down, and the ESN/MIN can be reprogrammed. The fraudulent consumer is immediately circumvented. The only flaw in this system is that the service provider considers duplicates very difficult.

3. *RF (Radio Frequency)*

Radio fingerprinting is a method that uses a special fingerprint characteristic of the signal transmission of a mobile phone or of some other radio transmitter. An electronic fingerprint allows a wireless computer to be detected with its specific features. Cellular operators typically use radio fingerprinting to avoid cell phone cloning. A cloned mobile phone has the same numerical identification but a different fingerprint radio [5]. If the service provider detects a single existing unit's fingerprint, the service is temporarily suspended.

4. *Usage Profiling*

The device use habits are studied. When there are some inconsistencies, the client will be contacted. Of instance, if a legitimate user is typically used to local calls and rarely STD calls and a call is unexpectedly traced back to a foreign country, a risk of cloning may be present. Telephone usage profiles are established and the consumer is notified if discrepancies are found. The same approach is used by the credit card companies. Of instance, when customers just make local networks call, but unexpectedly make call of hours of air time to foreign countries, a potential clone is seen.

5. *Calls counting*

Operator as well as the networks maintain tracks of phone call and if they vary further than the calls that are usually allowed, service is declined.

6. *Pin Codes*

The client enters a PIN code to open the handset and afterwards continues to dial as normal till a call is received. The consumer lock the mobile as well after finishing the contact by inserting the PIN code. To make roaming easier, operators can exchange PIN information.

SAFETY MEASURES FOR CLONING

Network operators have used different technologies in several countries to counter this hazard. Any of these are as follows: the duplicate identification approach enables the network to see the same phone simultaneously in many locations. The reactions include turning them off to the user as the real customer has missed the service he charges for. Pace Trap is another test to verify the situation, which seems to make cell phones travel at most unlikely or impossible speeds. For ex. if they call in Delhi first and 5 minute afterward, you call again, but in Chennai this period, two phones must have the similar uniqueness on networks. Few operator do utilize Radio Frequencies finger-printing, which was initially a military technique. Only a distinctive fingerprint of the same radio equipment is retained and fingerprints are matched with all the phones they use [9]. Thus, clones of the same name, but fingerprints are identified differently. Customized profiling is a new way to establish mobile user profiles and to contact consumers when anomalies are found. For example, if, for hours of sky time, a consumer usually only does local networks call, but instead makes a call abroad, then a probability of a clone is indicated. In addition, call counting is a way to test whether both the telephone and the network track phone calls, and if they vary more than normally the one-time call permitted, service is refused.

Unique in the wireless network is the identification of a mobile device. The MIN may also be linked to other wireless or wired networks. The number is different from that of a telephone manufacturer's electronic serial number (ESN). Electronically regulated MINs and ESNs may be used to avoid fraud. For communication / storage of sensitive information, cell phones should never be trusted. Set the pin they need before you can use the handset. Make sure you have a corporate security policy for all mobile devices[4]. Make sure that one person maintains track of who has which equipment and updates the central ledger. How are service providers dealing with cloned telephone reports? Legitimate phone-cloned customers collect bills for calls that they did not make. Sometimes these charges in addition to the legal charges amount to several thousand dollars. The facility providers typically bear price of the fraudulent further call. Nevertheless, the service provider must interrupt a valid telephone subscription to prevent the cloned phone from receiving the service. A modern payment through a specific phone figure that requires re-programming of modem, plus the added complications that accompany changes in the telephone number, would then be needed by the subscriber.

CONCLUSION

In a period when the mobile phone is a crucial element of our lives, security threats and risks are growing more and more. The cell phone itself is not secure as it can easily produce mobile telephone replicas. Mobile cloning was introduced in the UK and the US in 1998, but in India, it continues to expand and started in 2005 in India. There are very high future aspects of cell phone security, as mobile phone crimes are now a priority. It may also lead to the resolution of the crime. The contact of mobile phones is one of the most trustworthy, effective and commonly used. Constructive or harmful use of the device can be modified. Sadly, it is really easy to crack because of the safety requirements which takes far less time. Cloning can also be developed quickly and effectively enforced. It must also be taken into account that the safety currently employed is not adequately successful to protect the network in the future. It is therefore very important to test how the safety system operates on a timely basis and must also adjust or upgrade it once a month or year. The network operator will take preventive action, although the government does not find the passage of legislation to deter mobile phone-related crime a priority. There are many flaws in the current cellular network, it isn't perfect for us. The security personnel will also take these cloning issues seriously. And that is dangerous for our society.

REFERENCES

[1] V. Harrison, J. Proudfoot, P. P. Wee, G. Parker, D. H. Pavlovic, and V. Manicavasagar, “Mobile mental health: Review of the emerging field and proof of concept study,” *Journal of Mental Health*. 2011, doi: 10.3109/09638237.2011.608746.

[2] M. N. Burns *et al.*, “Harnessing context sensing to develop a mobile intervention for depression,” *J. Med. Internet Res.*, 2011, doi: 10.2196/jmir.1838.

[3] Y. Fukuoka, E. Kamitani, K. Bonnet, and T. Lindgren, “Real-time social support through a mobile virtual community to improve healthy behavior in overweight and sedentary adults: A focus group analysis,” *J. Med. Internet Res.*, 2011, doi: 10.2196 /jmir.1770.

[4] M. Chóliz *et al.*, “Development of a brief multicultural version of the Test of Mobile Phone Dependence (TMDbrief) questionnaire,” *Front. Psychol.*, 2016, doi: 10.3389 /fpsyg.2016.00650.

[5] T. Munezawa *et al.*, “The Association between Use of Mobile Phones after Lights Out and Sleep Disturbances among Japanese Adolescents: A Nationwide Cross-Sectional Survey,” *Sleep*, 2011, doi: 10.5665/sleep.1152.

[6] B. D. Kennard *et al.*, “Developing a Brief Suicide Prevention Intervention and Mobile Phone Application: A Qualitative Report,” *J. Technol. Hum. Serv.*, 2015, doi: 10.1080 /15228835.2015.1106384.

[7] Z. Zou, H. Wang, F. d’Oleire Uquillas, X. Wang, J. Ding, and H. Chen, “Definition of substance and non-substance addiction,” in *Advances in Experimental Medicine and Biology*, 2017.

[8] J. Van Ouytsel, E. Van Gool, K. Ponnet, and M. Walrave, “Brief report: The association between adolescents’ characteristics and engagement in sexting,” *J. Adolesc.*, 2014, doi: 10.1016/j.adolescence.2014.10.004.

[9] Z. Kirtava, T. Gegenava, M. Gegenava, Z. Matoshvili, S. Kasradze, and P. Kasradze, “Mobile telemonitoring for arrhythmias in outpatients in the republic of georgia: A brief report of a pilot study,” *Telemed. e-Health*, 2012, doi: 10.1089/tmj.2011.0170.

[10] J. Gold *et al.*, “A randomised controlled trial using mobile advertising to promote safer sex and sun safety to young people,” *Health Education Research*. 2011, doi: 10.1093/her/cyr020.

[11] K. Pal *et al.*, “Computer-based diabetes self-management interventions for adults with type 2 diabetes mellitus,” *Cochrane Database of Systematic Reviews*. 2013, doi: 10.1002/14651858.CD008776.pub2.

[12] B. Suffoletto, C. W. Callaway, J. Kristan, P. Monti, and D. B. Clark, “Mobile phone text message intervention to reduce binge drinking among young adults: Study protocol for a randomized controlled trial,” *Trials*, 2013, doi: 10.1186/1745-6215-14-93.

[13] R. B. Marasinghe, S. Edirippulige, D. Kavanagh, A. Smith, and M. T. M. Jiffry, “Effect of mobile phone-based psychotherapy in suicide prevention: A randomized controlled trial in Sri Lanka,” *J. Telemed. Telecare*, 2012, doi: 10.1258/jtt.2012.SFT107.