The Survey of Mobile Phone Cloning: Process, Current Scenario and Protective Techniques

Sandeep Kaur[1], Tanisha Saini[2]
M.Tech (Scholar), Assistant Professor
Chandigarh Group of College, Landran

Abstract - The process mobile which was not overheard off fifteen years ago has become a portion of our daily life. A mobile phone is a cell-phone that could kind and collect telephone calls over a radio-link while transferring around a wide-geographic area. Mobile communications has been speedily available for numerous years and is a major ecommerce today. Due to the money elaborate in the business there is a maximum chance that people might problems that device. The main threats that the mobile phone companies are fronting are from cloning. Cloning is the procedure of moving identify of individual phone to the other. At recent cloning is active in USA, some countries Asia, Africa and other continents. The latest mode of communication is defined as most significant as it added' 3e's, easily to be use, economic and efficient. The endless possibilities and applications which are newly designed and analysed allure the gray and dark clients to make the misuse of this communication medium. The important aspect to mobile phone is from cloning. Un-expectedly increase mobile phone bills and hateful nature of service are the major indications of possibility of mobile cloning. In this paper presents that about the overview of Mobiles, procedure of mobile cloning, current trends and possible protective techniques.

Keywords: Mobile Phone Cloning, trends, protective techniques i.e CDMA and GSM.

I. INTRODUCTION

Mobile phone cloning resources copying the subscriber data from individual from one phone to another with the intention of obtain free calls. The other mobile phone develops the exact imitation of the original mobile phone like a clone. As a consequence, while calls can be made from both phones, only the original is billed. Mobile phone cloning is a process in which the safe data from one mobile phone is transfer to another mobile phone. The other mobile phone will become the exact copy of the original phone [1]. Mobile Phone Cloning is also known as cell phone piracy and has been taking place all over the world since decades. In recent times this crime has come to India. This is generally done for making fake telephone calls. A cloned phone can make calls and get calls but the charges for those calls will be billed to the subscriber of the original phone. In India mobile phone cloning primary came to bright in January, 2005 when the Delhi police stopped a person with 20 cell receivers, a laptop, a SIM scanner, and a writer. The accused was running a replace illegally wherein he cloned CDMA-based mobile phones. He used software for the clone and provides cheap international calls to Indian immigrants in West Asia [2]. A related racket came to light in Mumbai resulting in the take into custody of four mobile dealers. What the main point is how a mobile phone cloning is done. Cloning is the method of taking the programmed information that is store in a legitimate mobile phone and criminally programming the identical evidence into another mobile phone. The culprits clone and hack into your phone by software that is easily accessible, once the software is installed they just require the unique IMEI number of the phone and they can digitally imprint these statistics on any of the phone they want. Once this is done they can send communications, make calls to anyone and the person whose phone has been duplicated and chopped will be held responsible.

Some more points for a subscriber to detect his phone are cloned or not are [3]:

- Difficulty in placing outgoing calls.
- Regular wrong number phone calls to the subscriber's phone.
- Incoming calls constantly getting busy signals.
- Unusual numbers appear on the phone bills.

There is an advanced way to detect the cloned phone which is used by the government called cell phone controller (CPC). Cell phone controller (CPC) is a system developed to identify, control and manage mobile phones. Within 5 minutes or less, the unit is fully operational. CPC uses an advanced mobile phone discovery functionality that can hunt for a specific cloned phones using CDMA (ESN) or GSM (IMSI) serial number. Once the cloned handset's general place has been determined, investigators working with law enforcement can pin point the handset's correct location [4].

II. RELATED WORK

Manjula .et.al, (2015) described the cellphone cloning with operation in GSM and CDMA technology phones. It gives an understanding into the security instrument in CDMA and GSM phones along with the loop holes in the organizations and discusses on the different ways of avoiding this cloning. Later it gives around the futuristic ideas for tackling the nuisance of cloning [5]. **Igor Gepko et.al (2015)** introduced "provable experience" confirmation factor of mobile device which is dual with respect to the "social network" verification factor of user. A novel technique of

multi-factor confirmation of mobile device is proposed based on this, which allows effective obstructive of clones in cellular networks and does not require standardization or changes in mobile device construction [6]. **YanzhiRen et.al (2012)** presented clone attack discovery scheme through extensive reproductions using a trace-driven approach by utilizing data sets composed from mobile phones. The consequences authorize that our method can detect clone attacks competently with high detection ratio and low false positive rate. This strongly indicates the possibility of exploiting the social community material derived from mobile sensing data for detecting the clone attacks [7]. **Katsuro Inoueet.al (2012**) developed a tool Clone Inspector to detect such inconsistent changes in the code clones, and applied it to two mobile software organizations. Using this tool, we were successfully able to find latent bugs in those systems. **Yanzhi Ren et.al (2013) [8]** describes derives both analytical and training based approaches to determine the threshold setting of the community between for robust clone attack detection. Extensive trace-driven reproduction studies expose that our social closeness based method can detect clone attacks with high detection ratio and low false positive rate [9]. **Zhen YANG et.al (2014**) firstly discloses the relationship between clone serving area and the MD. Secondly, the TCS scheme splits the clone network into Triangle topology by our Clone Triangulation Topology Construction and Reconstruction (CTTCR) algorithm. It can exactly obtain the target clone for clone relocation. We also prove the correctness of CTTCR algorithm. Simulation results show that our scheme works very well[10].

III. HOW MOBILE PHONE WORK AND CELL CLONING DONE?

Mobile phones send radio frequency transmissions through the sky on two distinct channels, one for voice infrastructures and the other for control signals. When a mobile phone figures a call, it normally transmits its Electronic Security Number (ESN), Mobile Identification Number (MIN), its Station Class Mark (SCM) and the quantity called in a tiny torrent of data. This burst is the short buzz you hear after you press the SEND button and before the tower catches the data [11]. These four things are the mechanisms the cellular contractor 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 together known as the 'Pair' which is used for the cell phone empathy. When the cell site gets the pair signal, it determines if the requester is a valid registered user by associating 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 repetition, known as Unidentified Registration, is carried out each time the telephone is turned on or picked up by a new cell site.

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 was discovered in several ways:

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

IV. ENCRYPTION TECHNIQUES

Mainly two encryption techniques are used in mobile cloning. GMS and CDMA explain in below:

a) Global Service for Mobile communications (GSM) [11]

The aim of GSM has been to make the system as safe as the public switched telephone network. With this goal security mechanisms prevent unauthorised network access and impersonation of subscribers, and protect confidentiality (preventing eavesdropping) and privacy (tracking of the user depend on his/her phone signal) of the mobile users.

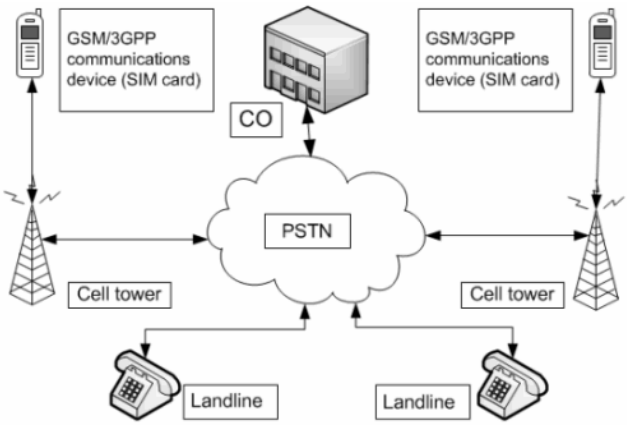

Fig.1 Architecture of Global Service for Mobile communications

In GSM system, a smart card will be the Subscriber Identity Module (SfM) that is used to recognize the subscriber. GSM system uses this information and a challenge-response protocol to authenticate the user, and an algorithm called A5 to encrypt the communication. The system has databases that contain administrative information and the current location of active subscriber in the network. To prevent the user's identity to be revealed, or his calls to be linked, the user will receive a dissimilar temporary identity by the system in each call. However the user's identity information and location can always be obtained from the network operator. Cryptographic set of rules used in GSM were

initially kept secret with the aim of providing higher security. However they were gradually leaked or reverse engineered and subsequently shown to be insecure.

b) CDMA (Code-Division Multiple Access)

In CDMA each user is assigned a unique code sequence that is used to encode his signal and decode the signal sent to him. The encoding process enlarges (spreads) the spectrum

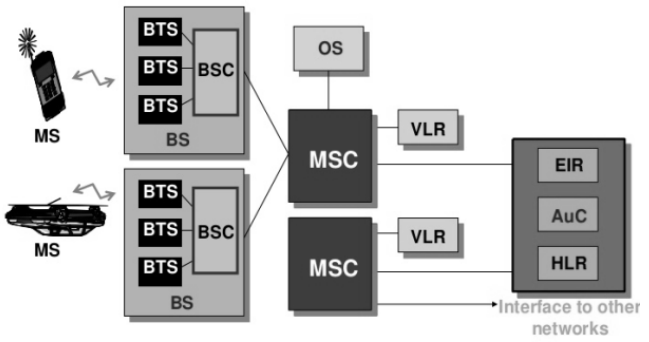

Fig.2 Architecture of Code-Division Multiple Access

V. DETECT THE CLONING

Mobile Phone cloning is use for send the secure data from one phone user to another user throw network. But some time problems are happen when some third person uses our data .so we resolved this problems with some techniques like duplication detection method, RF fingerprinting method etc. All these techniques described in below:

a) Duplicate Detection method

Duplicate detection is a process in which the network sees the similar phone in several places at the similar time. So the service provider will disconnect all of them so that the original customer will contact the operator questioning about defeat of service[13].

b) RF fingerprinting

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 mark the cloned phone with same identity, but dissimilar fingerprints.

c) Usage profiling

Usage Profiling is a different way wherein profiles of clientele phone usage are kept, and when discrepancies are notice, the customer is contacted. For example, if a consumer normally makes only local network calls but is unexpectedly placing calls to foreign countries for hours of airtime, it indicates a possible clone.

of the sign and is therefore known as spread spectrum modulation (SS). SS signals allow multiple accesses to the communication channel because the receiver can distinguish between the users who are assigned different codes. SS is particularly attractive because it provides higher security for air signals. It increases privacy because the data can single be recovered if the code is known to the receiver. It also provides anti-jamming capability [12].

d) Call counting

Call Counting is also a way to verify the condition where both the phone and the network keep track of calls made with the phone, and should them different more than the usually allowable one call, service is denied.

e) PIN Codes[14]

Prior to placing call, the caller unlocks the phone through entering a PIN code and then calls as usual. After the call has been finished, the user locks the through entering the PIN code again. Operators may share PIN information to enable safer roaming.

VI. WHO IS HARMLESS? AND MOBILE PHONE SAFETY MEASURES

Together CDMA and GSM hand-sets are advantages to cloning. Basically technically defined, it is easy to clone a CDMA hand-set over GSM. Individual, although cloning a GSM mobile phone is n't impossible. There are also internet sites that give information on how individual can go about hacking into the mobile phones.

The mobile phone safety measure in operators many countries have implemented technologies to deal with this risk. Some of them are as follows:

There's the copy detection method where the network sees the similar phone in several places at the similar time. Reactions add shutting them all off, so that the original customer will contact the operator since he has lost the service he is paying for. Pace trap is another analysis test to cross verify the situation, whereby the mobile phone speeds [15].

VII. CONCLUSION

Existing cellular systems have a number of potential weaknesses that were considered. It is crucial that productions and staff take mobile phone security extremely. Awareness and a few sensible protections as part of the overall enterprise security policy will deter all but the most sophisticated criminal. It is also compulsory to keep in mind that a system which is described as safe today can be the most unsecured technique in the future. Therefore it is absolutely important to check the meaning of a security system once a year and if needed update or substitute it. Finally, cell-phones have to go a long way in security before they can be used in critical applications like m-commerce.

VIII. REFERENCES

[1]. Wang, Yating, Ray Chen, and Ding-Chau Wang. "A survey of mobile cloud computing applications: perspectives and challenges." *Wireless Personal Communications* 80, no. 4 (2015): 1607-1623.

[2]. Soh, Charlie, Hee Beng Kuan Tan, Yauhen Leanidavich Arnatovich, and Lipo Wang. "Detecting clones in Android applications through analyzing user interfaces." In *2015 IEEE 23rd International Conference on Program Comprehension*, pp. 163-173. IEEE, 2015.

[3]. Vaezpour, Seyed Yahya, Rui Zhang, Kui Wu, Jianping Wang, and Gholamali C. Shoja. "SWAP: Security aware provisioning and migration of phone clones over mobile clouds." In *Networking Conference, 2014 IFIP*, pp. 1-9. IEEE, 2014.

[4]. Saxena, Nitesh, Md Borhan Uddin, Jonathan Voris, and N. Asokan. "Vibrate-to-unlock: Mobile phone assisted user authentication to multiple personal RFID tags." In *Pervasive Computing and Communications (PerCom), 2011 IEEE International Conference on*, pp. 181-188. IEEE, 2011.

[5]. Singhal, Navin, Rajeshwari Pandey, and Neeta Pandey. "DUAL MODE BIQUADRATIC FILTER USING SINGLE VDTA." International Conference on Emerging Trends in Science and Cutting Edge Technology (ICETSCET-2014).

[6]. Gepko, Igor. "General requirements and security architecture for mobile phone anti-cloning measures." In *EUROCON 2015-International Conference on Computer as a Tool (EUROCON), IEEE*, pp. 1-6. IEEE, 2015.

[7]. Ren, Yanzhi, Yingying Chen, and Mooi Choo Chuah. "Social closeness based clone attack detection for mobile healthcare system." In *2012 IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS 2012)*, pp. 191-199. IEEE, 2012.

[8]. noue, Katsuro, Yoshiki Higo, Norihiro Yoshida, Eunjong Choi, Shinji Kusumoto, Kyonghwan Kim, Wonjin Park, and Eunha Lee. "Experience of finding inconsistently-changed bugs in code clones of mobile software." In *Proceedings of the 6th International Workshop on Software Clones*, pp. 94-95. IEEE Press, 2012.

[9]. Ren, Yanzhi, Yingying Chen, and Mooi Choo Chuah. "Social closeness based clone attack detection for mobile healthcare system." In *2012 IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS 2012)*, pp. 191-199. IEEE, 2013.

[10]. Yang, Zhen, and Xing Liu. "Dynamic Clone Sharing Scheme in Mobile Cloud Computing: A Delaunay Triangulation Approach." *Computational Science and Engineering (CSE), 2014 IEEE 17th International Conference on*. IEEE, 2014.

[11]. Racic, Radmilo, Denys Ma, and Hao Chen. "Exploiting MMS vulnerabilities to stealthily exhaust mobile phone's battery." In *Securecomm and Workshops, 2006*, pp. 1-10. IEEE, 2006.

[12]. Gilhousen, Klein S., Roberto Padovani, and Charles E. Wheatley III. "Method and system for providing a soft handoff in communications in a CDMA cellular telephone system." U.S. Patent 5,101,501, issued March 31, 1992.

[13]. Singh, Sapana, and Pratap Singh. "Key concepts and network architecture for 5G mobile technology." *International Journal of Scientific Research Engineering & Technology (IJSRET)* 1, no. 5 (2012): 165-170.

[14]. Misra, Santosh K., and Nilmini Wickamasinghe. "Security of a mobile transaction: a trust model." *Electronic Commerce Research* 4, no. 4 (2004): 359-372.

[15]. Lin, P. Paul, and Kevin F. Brown. "Smartphones provide new capabilities for mobile professionals." *The CPA Journal* 77, no. 5 (2007): 66.