The Approaches to Prevent Cell Phone Cloning In Cdma Enviornment

Aaruni Goel
I.T. Department
IMT Engineering College
Meerut, U.P., India

Madhup Sharma
I.T. Department
IIMT Engineering College
Meerut, U.P. India

Paresh Pathak
I.T. Department
IIMT Engineering College
Meerut, India

ABSTRACT

The rapid growth of mobile communication has changed the vision of cellular phones security. An easy accessibility condition causes cellular phones to be vulnerable against numerous and potentially devastating threats from hackers. Up to the moment, researchers have developed Intrusion Detection Systems (IDS) capable of detecting attacks in several available environments. Intrusion Prevention Systems (IPS) evolved after that to resolve ambiguities in passive network monitoring by placing detection systems on the line of attack. This paper presents an overview cellular phones security based upon CDMA technology specially on cell phone cloning.

Keywords

Spread Spectrum, Soft handoff, Multipath, CAVE (Cellular Authentication and Voice Encryption), A-Key.

1. INTRODUCTION

The digital cellular standard for CDMA is developed by Qualcomm. CDMA is a 2G (also name for IS-95/cdmaOne) and 3G (other CDMA2000) mobile telecommunications standard. It utilizes to send and receive voice transmission, data transmission and various other types signaling managements. In CDMA the same frequencies are allocated to share multiple radios links. It is a type of multiplexing which is used to optimize the bandwidth of single channel. CDMA is a form of multiplexing, which allows several signals to optimize the available bandwidth. The technology works in between 800Mhz to 1900Mhz i.e in the range of ultra-high-frequency (UHF) band. The size of CDMA channel is about 1.23MHz and offers a scheme of 14.4Kbps to 115 Kbps depending on the size channels i.e. 1 to 8 respectively. CDMA service providers presently in India are Reliance Telecom and Tata Indicom.

CDMA, Code Division Multiple Access, is a technology which enables many wireless devices to transmit at the same time and on the same frequency. This is the reason CDMA is also referred as Multiple-access mechanism. In CDMA environment cellular phone, has a unique precise identity. It encoded this identity to the original signal and sends the altered signal. A receiver at destination decodes this received signal to recover the original signal [13].

CDMA uses spread spectrum technique [11] for the aforesaid reason. The working of CDMA is as under:

1. The analog audio input is digitized into binary values.
2. The transmitted signal is then varied as per the predefined code received by genuine receiver. This is so because the reply pattern of receiver is also encoded with the analogous pattern sent by receiver.

Since there are infinite numbers of frequency-sequencing codes this leads to increase the confidentiality. So still the CDMA based phone cloning difficult but not impossible.

2. MAJOR ADVANTAGES OF CDMA TECHNOLOGY

1. The CDMA channel size is about 1.23 MHz wide. Further CDMA networks engages soft hand off, by which the chances of signal breakup is minimal whenever a CDMA based handset involves in inter cell movement or at low network coverage. Basically the soft handoff means as the process by which the call is actually be transmitted by more than one tower at a time which reduces the chance call dropping at its minimal [3],[13].
2. In comparison to analog modes the amalgamation of digital and spread-spectrum [3], [11] modes wired-up many signals per unit bandwidth.
3. CDMA is well-matched with other cellular technologies. This approach is very helpful roaming in national and international level [3], [12].
4. CDMA also prevents interference and destruction of service caused due to Multipath [3].
5. Call rates are low as in comparison with existing GSM technology [3].
6. Phone call clarity is also much better [3].

Due to afore said reasons it can be observed that CDMA is far good technology but still there some security loop holes in CDMA based mobile systems. Till date three security flaws have been identified [7-8-9]:

1. The listening or capturing conversation during the active call. This involves the process of cell phone tracking and interception [1].
2. A cell phone can be turned on without the knowledge of customer i.e. as microphone to listen his or nearby conversations. This is the only reason that mobile is prohibited in high profile security areas.
3. A cell phone can be cloned by anybody so that one can pretend himself to be genuine customer while the charge is to be paid real customer.

The above said technologies require the support of cell service provider.

3. CELL PHONE WORKING

Cell phone transmits the radio frequencies with the help of two separate channels one for voice and another for control signaling information. When a call is done through cell phone along with other three important components are transmitted- a) Electronic Serial Number (ESN), b) Mobile Identification Number, c) Station Class mark. These four parts are very important to service provider since they provide the billing information to the cellular service that how much a customer has to be charged. After receiving this ESN and MIN, cell service provider verifies them with their genuine subscriber list. If this pair is genuine then a control signal is generated and permits the customer to make the call. The successfully registering this way is known as Anonymous Registration [5].

4. CLONING METHODOLOGY

Cloning involved alteration or replacement of the EPROM (discussed later) in the phone with a new chip which would allow to configure an ESN (Electronic serial number) via software. One would also have to change the MIN (Mobile Identification Number) then this cell phone is cloned of other phone [4].

ESN/MIN pairs can be obtained in numerous ways:

- By Sniffing the radio waves sniffing devices.
- By using garbage of cellular phones (E-wastes of obsolete components) or hacking the cell phone service provider company.
- Gain unauthorized access in cellular companies through breach of privilege by any disgruntled employee.

In recent times many new softwares/hardwares are available for mobile cloning. Patagonia is the name of one such famous software used for cloning the CDMA phones.

The following steps are taken by fake identity to make his phone cloned copy to other genuine phone [4]:

1. Once authentication of cell during anonymous registration takes the ESN/MIN data is transmitted to MSC without Encryption. One can sniff or capture these signals through the use of appropriate hardware (Digital Data Interface), software (Patagonia) and PC. These along with other values are copied and used by fake person to place a call. This results the transfer of billing amount to the account of genuine customer. Further the fake person can also make his call during the time when the genuine person call is active.
2. Number Assignment Module (NAM) – It is the EPROM that stores the telephone number (MIN) and an electronic serial number (ESN). This is generally altered or replaced when a call is going to placed by genuine customer and this is the moment when fake user clone his new cellular phone. Phones with dual or multi-NAM characteristics provide users the choice of registering the phone with a local number in more than one market (Wireless in Local Loop). Some mobile handsets are equipped with NAM's which can hold multiple telephone numbers. This makes the one phone have multiple telephone numbers from one carrier or multiple telephone numbers from multiple carriers to the same phone.
3. The NAM module also has SIDH (System IDentification for Home System). The data fields stored in a phone's NAM change with respect to other prevalent technologies like AMPS/NAMPS, GSM, PCS, CMDA. But in recent times NAM is reprogrammed over the air. The SIDH or SID ensures that from which cellular carrier one's cellular service is initiated from. This particular information is used at the roaming time in those regions where cellular service is used by customer is other than that of his own cellular provider.

   There are two SIDH codes for every region, one for the wire-line carrier (i.e. local telephone company) and one for the non wire-line (another company). The SIDH for the wire-line carrier is always an even number, while the SIDH for the non wire-line carrier is always an odd number. By changing the value SIDH tells the cellular carrier where to forward the billing information in case if user is in roaming.
4. The MIN (Mobile Identification Number) is a number that uniquely identifies a mobile telephone subscriber.

Station Class mark (SCM) is the component which tells service provider about the make or model of cell phone through its cellular carrier. If this number ic change then service provider during his forensics can also be made fooled. Since service provider will be searching only a phone with that particular model.

5. THREATS IDENTIFYING MEASURES AND COUNTERMEASURES

1. The Operator knows that if there is same ESN/MIN combinations are traced from different places then cell phone is assumed to be cloned. In this case it is the duty of operator to switch off all the phones having the same pairs. This will enable genuine customer forced to contact operator regarding no activation of services.
2. Operators and Customers should also check the bill details regularly to identify the divergence from average monthly bill to a bill of monthly having discrepancies regarding high cost in mobile bills.

3. A personal identification number (PIN) is a secret numeric password shared between a user and a MSC that can be used to authenticate the user to the network. The cellular operators also provides non-secret user ID. When a system (MSC) receives the user ID and the PIN then it simply checks its database to find out whether the entry is valid or not. If it is not valid then the data transfer or call is simply discarded. If it is valid then user it shows that the user is authenticated and permitted to grant access.

   But be cautious, if a mobile phone PIN is entered incorrectly three times, the SIM card is blocked until a Personal Unblocking Code (PUC or PUK), provided by the service operator, is entered. If the PUC is entered incorrectly ten times, the SIM card is permanently blocked and new SIM card is required.
4. A Distance can also be another important factor to identify security threat. It is just like that a call is placed from Meerut at 3PM but after five minutes, some call also is placed from the same ESN/MIN pair from Banglore which is thousands of miles apart. So this is quite obvious that the cell phone has been cloned of real subscriber.
5. Radio Frequency Fingerprinting (RFF) is another technique used by operators. The RFF is always unique. Basically every cell phone has some unique features like phase-noise, rise time, harmonics, peak deviation etc. that differs from phone to phone and are the integral part of RFF. Since this technique is the momentary detection followed by momentary extraction of the fingerprint so if anyone of the above said unique features do not match from the pre described feature of original phone during network access then it is sure that phone has been cloned. After that the operator has full right to activate the service of customer.
6. The customers are also recommended that always try to avoid cellular telephones in busy traffic areas like malls, railway stations etc. Since these are the places where persons fake use scanners for random monitoring of calls and if he finds any interesting he can start continuous monitoring of cell phone of user.
7. CAVE Security protocol- CDMA Network have a security protocol- CAVE (Cellular Authentication and Voice Encryption) that requires 64-bit authentication key called A-Key or Authentication key. This key is secret and known only Mobile station (MS) and Authentication Center (AC). A 64-bit primary secret key is known only to the MS and AC. In the case of RUIM equipped mobiles, the A-key is stored on the RUIM otherwise A- key is stored in Mobile station semiconductor memory. Otherwise, it is stored in semi-permanent memory on the MS. It should be noted that A-key is not at all shared with roaming partners. However, this key it is enables the a secondary key known as SSD (Shared Secret Data). The SSD is shared with a roaming partner to permit local authentication in the visited network. After proper authentication the billing operation is generated on the basis data or call transfer [10].

   Other advices for subscribers that can be sign of caution include [4]:

- Frequent wrong number phone calls to phone, or hang-ups.
- Difficulty in placing outgoing calls.
- Difficulty in retrieving voice mail messages.
- Incoming calls constantly receiving busy signals or wrong numbers.
- Unusual calls appearing on phone bills.

6. TOOLS USED FOR CDMA TRACKING IN PRESENT SCENARIO

There are many tools which are used by forensic experts to analyze the CDMA technology based cellular phones completely or in some extent on certain models. Some of them are [2][6] :
Device Seizure: For acquisition, Examination and Reporting.
GSM.xry: For acquisition, Examination and Reporting.
TULP2G: For acquisition, Examination.
SecureView: For acquisition, Examination and Reporting.
BitPiM: For acquisition, Examination.
PhoneBase2: For acquisition, Examination and Reporting.
CellDEK: For acquisition, Examination and Reporting.

The acquisition involves logical and physical capture of data which enable the observation of internal memory and its associated data files including the database. These files include- Phonebook, Wallpapers (graphic files present on the phone), Audios, Calendar entries, text messages, call history, Memo entries and phone lock codes. But this all depends upon the type model to be analyzed i.e. model dependent. Depending on the different types of tools as mention earlier, a cable or Bluetooth or infrared connectivity is used. to establish a data-link between the phone and the forensic workstation. After proper examinations the report is generated for to remove security flaws.

7. CONCLUSION

Presently the cellular phone industry relies on common law (fraud and theft). As in initial stages in country like India 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. Well this typical task is already under process after the enactment of I.T. Act 2008(amendment) in India.

Existing cellular systems have a number of potential weaknesses that need to be 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.

Further due to advent and interconnectivity of cellular devices with Internet opens the cellular device to variety of security issues such as viruses, buffer overflows, denial of service attacks etc.

Finally, cell-phones have to go a long way in security before they can be used in critical applications like m-commerce. 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 before being implemented. It is therefore mandatory to keep in mind that a technique which is described as safe today can be the most unsecured technique in the future.

REFERENCES

[1] Krueger, C. (2011, February 11). Man found guilty of lesser charge in murder recorded on cell phone. *St. Petersburg Times*.

[2] Rehault, F. (2010). Windows mobile advanced forensics: An alternative to existing tools. *Journal of Digital Investigation*, 7(1–2).

[3] Mislan, R., Casey, E., & Kessler, G. (2010). The growing need for on-scene triage of mobile devices. *Journal of Digital Investigation*, 6.

[4] Murphy, C. (2009). The fraternal clone method for CDMA cell phones. *Small Scale Digital DeviceForensicsJournal*, 3(1). Available from http://www.ssddfj.org/papers/SSDDFJ_V3_1_Murphy.pdf.

[5] Moore, H. D. (2007, September 25). A root shell in my pocket (and maybe yours). Available from http://blog.metasploit.com/2007/09/root-shell-in-my-pocket-and-maybe-yours.html.

[6] Rick Ayers, Wayne Jansen, Ludovic Moenner, Aurelien Delaitre, Cell Phone Forensic Tools: An Overview and Analysis Update, NIST Interagency Report (IR) 7387, March 2007, http://csrc.nist.gov/publications/nistir/nistir-7387.pdf

[7] Ken Hutchiunson, *Wireless Intrusion Detection Systems*, SANS Institute, October 2004

[8] Bruce Potter, *Wireless Intrusion Detection*, Network Security Volume 2004, Issue 4

[9] Chris Bennett, Challenges of Mobile Security, SearchCIO.com, TechTarget, December 17, 2003,

[10] Fluhrer, Mantin and Shamir, *Weaknesses in the Key Scheduling Algorithm of RC-4*, 2001

[11] Spread spectrum access methods for wireless communications. R. Kohno, R. Meidan, and L. Milstein, IEEE Communication Magazine,
Jan. 1995.

[12] On the capacity of a cellular CDMA system. K. Gilhousen, I. Jacobs, R. Padovani, A. viterbi, L. Weaver, and C. Wheatley, IEEE Trans. on Vehicular Technology, May 1991.http://searchcio.techtarget.com/tip/0,289483,sid182_gci952382,00.html .

[13] IEEE 802.11 Standards Website, http://**ieee**802.org/11/