Cell Phone Cloning

Cyber Terrorism & Digital Forensic Consultant

Md. Tawhidur Rahman Pial

Remember Dolly the lamb, cloned from a six-year-old ewe in 1997, by a group of researchers at the Roslin Institute in Scotland? While the debate on the ethics of cloning continues, human race, for the first time, are faced with a more tangible and harmful version of cloning and this time it is your cell phone that is the target.

Millions of cell phones users, be it GSM or CDMA, run at risk of having their phones cloned. As a cell phone user if you have been receiving exorbitantly high bills for calls that were never placed, chances are that your cell phone could be cloned. Unfortunately, there is no way the subscriber can detect cloning. Events like call dropping or anomalies in monthly bills can act as tickers.

According to media reports, recently the Delhi (India) police arrested a person with 20 cell- phones, a laptop, a SIM scanner, and a writer. The accused was running an exchange illegally 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.

Security Vulnerabilities in Cell Phone

Your cellular telephone has three major security vulnerabilities:

Monitoring of your conversations while using the phone.

Your phone being turned into a microphone to monitor conversations in the vicinity of your phone while the phone is inactive.

Cloning or the use of your phone number by others to make calls that are charged to your account.

What is Cell Phone Cloning?

Cloning of mobile phones is the act of copying the subscriber information from one phone onto the other for purposes of obtaining free calls. 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 both phones, only the original is billed.

Cloning occurs most frequently in areas of high cell phone usage — valet parking lots, airports, shopping malls, concert halls, sports stadiums, and high-congestion traffic areas in metropolitan cities.

Loop holes in Cell phone Networks

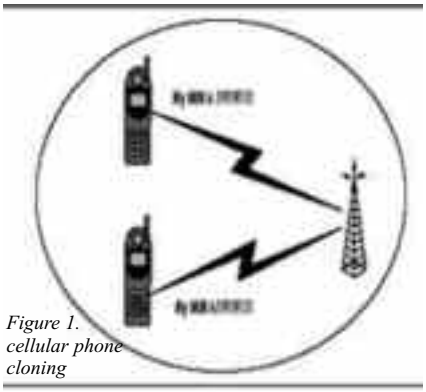

Figure 1. cellular phone cloning

ESN/MIN data is NOT encrypted on the way to the MSC (Mobile Switching Centre) for further authentication. Thus, scanning the airwaves 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.

The Station Class Mark can also be changed if you wish to prevent the cellular carrier from determining the type of phone that is placing the call. By providing the cellular tower with a false SCM, the cellular carrier, the FCC, or whoever happens to chase down cellular fraud is often looking for a particular phone which in reality is not the phone they are looking for.

The Number Assignment Module (NAM) also has the SIDH (System Identification for Home System) number programmed into it. The transmittal of the SIDH number tells the carrier where to forward the billing information to in case the user is "roaming". The SIDH table tells the major cities and their identifying numbers. Changing an SIDH is programming job that takes only minutes, but be aware that the ESN is still sent to the cellular phone company. After they realize that the ESN is connected to either a fake number or a phone that is not in the network, they will block service. They only way around this is to reprogram the ESN.

Who's Safe?

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

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.

Cloning CDMA Cell Phones.

Cellular 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 air interface and use this data to clone phones. A device called as DDi, **Digital Data Interface** (which comes in various formats from the more expensive stand-alone box, to a device which interfaces with your 800 MHz capable scanner and a PC) 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.

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 fairly sophisticated asymmetric-key cryptosystem for over-the-air transmission of subscriber information. Cloning a SIM using information captured over-the-air 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 make GSM a far secure technology.

GSM networks which are considered to be impregnable can also be hacked. The process is simple: a SIM card is inserted into a reader. After connecting it to the computer using data cables, the card details were transferred into the PC. Then, using freely available encryption software on the Net, the card details can be encrypted on to a blank smart card. The result: A cloned cell phone is ready for misu.

Identifying the ESN in your Cellular Phone

Depending on what model phone you have, the ESN will be located on a PROM. The PROM is programmed at the factory, and installed usually with the security fuse blown to prevent tampering. The code on the PROM might possibly be obtained by unsoldering it from the cellular phone, putting it in a PROM reader, and then obtaining a memory map of the chip.

The PROM is going to have from sixteen to twenty-eight leads coming from it. It is a bipolar PROM. The majority of phones will accept the National Semiconductor 32x8 PROM, which will hold the ESN and cannot be reprogrammed. If the ESN is known on the phone, it is possible to trace the memory map by installing the PROM into a reader, and obtaining the fuse map from the PROM by triggering the "READ MASTER" switch of the PROM programmer. In addition, most PROM programming systems include verify and compare switch to allow you to compare the programming of one PROM with another.

As said earlier, the ESN is uniformly black with sixteen to twenty-eight leads emanating from its rectangular body, or square shaped body. If it is the dual-in-line package chip, (usually found in transportable and installed phones), it is rectangular. If it is the plastic leaded chip carrier (PLCC), it will be square and have a much smaller appearance. Functionally, they are the same chip, but the PLCC is used with hand held cellular phones because of the need for reduced size circuitry.

ESN Replacement

De-solder the ESN chip.

Solder in a zero insertion force (ZIF) replacement, so that replacement chip can be changed easily.

After the ZIF socket has been successfully soldered in, reinsert the ESN and attempt to make a phone call (Be sure the NAM is programmed correctly). If it doesn't, check the leads on the ZIF to insure that you have soldered them correctly.

After that, insert your ESN into your PROM reader and make sure it provides some sort of reading. You should use the search mode to look for the manufacturer's serial number to identify the address on the PROM where to reprogram the ESN.

Cellular Phone Security Measures

Cellular operators in many countries have deployed various technologies to tackle this menace. 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.

Velocity 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 identical 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.

Usage Profiling is another way wherein profiles of customers' phone usage are kept, and when discrepancies are noticed, the customer is contacted. For example, if a customer normally makes only local network calls but is suddenly placing calls to foreign countries for hours of airtime, it indicates a possible clone. On the other hand, the consumers can check regularly the unbilled amount details. Users with ILD facility need to be more careful as fraudsters attempt to make as many international calls as possible within a short time due to fear of getting caught. Since ILD rates are higher than other calls, fraudsters try to derive maximum benefits in the shortest time.

If your cellular service company offers **Personal Identification Numbers (PIN)**, consider using it. Although cellular PIN services are cumbersome and require that you input you're PIN for every call, they are an effective means of thwarting cloning.

The Central Forensic Laboratory at Hyderabad has developed software to detect cloned mobile phones. The laboratory helped Delhi Police identify two such cloned mobile phones recovered recently. Called the **Speaker Identification Technique**, the software enables one to recognize the voice of a person by acoustics analysis, using a computerized speech laboratory machine. For the process, developed by Dr S.K. Jain, a voice sample of four seconds is adequate for an accurate result.

The best detection measure available in CDMA today is the **A Key Feature**. The A key is a secret 20 digit number unique to the handset given by the manufacturer to the service provider only. This number is loaded in the Authentication Center for each mobile. As this number is not displayed in mobile parameters this cannot be copied. Whenever the call is originated / terminated from a mobile with authentication active, the network checks for the originality of the set using this secret key. If the data matches at both mobile and network end the call is allowed to go through otherwise it is dropped.

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 ▣