MOBILE PHONE CLONING

Eureka S
PG Scholar
Department of Information Technology
PSNA College of Engineering and Technology
Dindigul
eureka.nw@gmail.com

Abstract

Mobile communication has been readily available for several years, and is major business today. It provides a valuable service to its users who are willing to pay a considerable premium over a fixed line phone, to be able to walk and talk freely. 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 between the mobile communication, Some of the features of mobile communication make it an alluring target for criminals. It is a relatively new invention, so not all people are quite familiar with its possibilities, in good or in bad. Its newness also means intense competition among mobile phone service providers as they are attracting customers. The major threat to mobile phone is from cloning.

Keywords-Mobile, GSM, CDMA, GSN, MIN, Cloning

I. INTRODUCTION

Cell phone cloning refers to the act of copying the identity of one mobile telephone to another. This is usually done to make fraudulent telephone calls. The bill for the calls go to the legitimate subscriber. This made cloning very popular in areas with large immigrant populations, where the cost to "call home" was very steep. The cloner is also able to make effectively anonymous calls, which attracts another group of interested law breakers. Cell phone cloning started with Motorola "bag" phones and reached its peak in the mid 90′s with a commonly available modification for Motorola "brick" phones such as the Classic, the Ultra Classic, and the Model 8000. Cloning involved modifying or replacing the EPROM in the phone with a new chip, which would allow one to configure an ESN (Electronic Serial Number) via software. The MIN (Mobile Identification Number) would also have to be changed. After successfully changing the ESN/MIN pair, the phone would become an effective clone of the other phone.

Cloning required access to ESN and MIN pairs. ESN/MIN pairs were discovered in several ways:

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

Cloning still works under the AMPS/ NAMPS system, but has fallen in popularity as older phones that can be cloned are more difficult to find and newer phones have not been successfully reverse engineered. Cloning has been successfully demonstrated

under GSM, but the process is not easy and currently remains in the realm of serious hobbyists and researchers. Furthermore, cloning as a means of escaping the law is difficult because of the additional feature of a radio fingerprint that is present in every mobile phone's transmission signal. This fingerprint remains the same even if the ESN or MIN are changed. Mobile phone companies can use the mismatch in the fingerprints and the ESN and MIN to identify fraud cases.

Electronic Serial Number (ESN)

The unique identification number embedded in a wireless phone by the manufacturer. Each time a call is placed, the ESN is automatically transmitted to the base station so the wireless carrier's mobile switching office can check the call's validity. The ESN cannot easily be altered in the field. The ESN differs from the mobile identification number, which is the wireless carrier's identifier for a phone in the network. MINs and ESNs can be electronically checked to help prevent fraud and Features. Each ESN is a 32-bit number consisting of three fields: a manufacturer code (eight bits), a unique serial number (18 bits), and an extension (six bits). In practice, the serial number and the extension have actually been combined into one 24-bit serial number to identify each mobile unit. Under this assignment format, 256 manufacturers could be distinguished by ESN. But when this number proved insufficient, the 32-bit ESN assignment was altered to reflect a 14-bit manufacturer code and an 18-bit unit identification number.

MIN (Mobile Identification Number)

The MIN (Mobile Identification Number) is a number that uniquely identifies a mobile telephone subscriber. MINs are 34-bits in length. The first 10 bits are sometimes known as MIN2, while the last 24 bits are referred to as MIN1. Together they are simply known as the MIN.

Advanced Mobile Phone Service (AMPS)

It is a standard system for analog signal cellular telephone service in the United States and is also used in other countries. AMPS allocates frequency ranges within the 800 and 900 Megahertz (MHz) spectrum to cellular telephone. The bands are divided into 30 kHz sub-bands, called channels. The receiving channels are called reverse channels and the sending channels are called forward channels. The division of the spectrum into sub-band channels is achieved by using frequency division multiple access (FDMA).

Narrowband Advanced Mobile Phone System (NAMPS)

Combines cellular voice processing with digital signaling, increasing the capacity of AMPS systems and adding functionality.

GSM (Global System for Mobile Communication)

GSM (Global System for Mobile communication) is a digital mobile telephony system that is widely used in Europe and other parts of the world. GSM uses a variation of time division multiple access (TDMA) and is the most widely used of the three digital wireless telephony technologies (TDMA, GSM, and CDMA). GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900 MHz or 1800 MHz frequency band. Since many GSM network operators have roaming agreements with foreign operators, users can often continue to use their mobile phones when they travel to other countries. SIM cards (Subscriber Identity Module) holding home network access configurations may be switched to those will metered local access, significantly reducing roaming costs while experiencing no reductions in service.

How CDMA Works?

IS-95 is a standard for CDMA (Code Division Multiple Access) Digital Cellular.

In a CDMA system, your encoded voice is digitized and divided into packets. These packets are tagged with "codes." The packets then mix with all of the other packets of traffic in the local CDMA network as they are routed towards their destination. The receiving system only accepts the packets with the codes destined for it.

What Is Cell Phone Cloning Fraud?

Every cell phone is supposed to have a unique factory-set electronic serial number (ESN) and telephone number (MIN). A cloned cell phone is one that has been reprogrammed to transmit the ESN and MIN belonging to another (legitimate) cell phone. Unscrupulous people can obtain valid ESN/MIN combinations by illegally monitoring the radio wave transmissions from the cell phones of legitimate subscribers. After cloning, both the legitimate and the fraudulent cell phones have the same ESN/MIN combination and cellular systems cannot distinguish the cloned cell phone from the legitimate one.

The legitimate phone user then gets billed for the cloned phone's calls. Call your carrier if you think you have been a victim of cloning fraud. The ESN is normally transmitted to the cellular company in order to ascertain whether the mobile phone user is the legitimate owner of that phone.

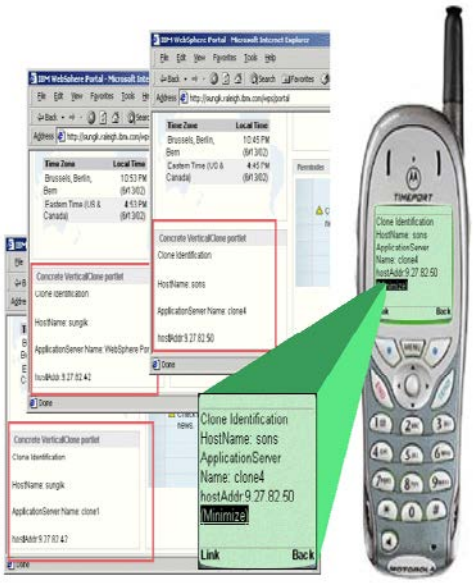
Modifying this, as well as the phone number itself (known as the mobile identification number, or MIN) paves the way for fraudulent calls, as the target telephone is now a clone of the telephone from which the original ESN and MIN numbers were obtained. Cloning has been shown to be successful on code division multiple access (CDMA) but rare on the Global System for Mobile communication (GSM), one of the more widely used mobile telephone communication systems.

CLONING GSM PHONES

- 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.
- 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 misuse.

METHODS TO DETECT CLONED PHONES

- **Duplicate detection** - 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 lost the service he is paying for, or tearing down connections so that the clone users will switch to another clone but the real user will contact the operator.
- **Velocity trap** - The mobile phone seems to be moving at impossible, or most unlikely speeds. For example, if a call is first made in Helsinki, and five minutes later, another call is made but this time in Tampere, there must be two phones with the same identity on the network.
- **RF (Radio Frequency)** - fingerprinting is originally a military technology. Even nominally 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**. - Profiles of customers' phone usage are kept, and when discrepancies are noticed, the customer is contacted. Credit card companies use the same method. 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.
- **Call counting -** Both the phone and the network keep track of calls made with the phone, and should they differ more than the usually allowed one call, service is denied.
- **PIN codes** - Prior to placing a call, the caller unlocks the phone by entering a PIN code and then calls as usual. After the call has been completed, the user locks the phone by entering the PIN code again. Operators may share PIN information to enable safer roaming.

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.
- 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.
- This 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.

HOW TO PREVENT CLONING?

- Service providers have adopted certain measures to prevent cellular fraud. These include encryption, blocking, blacklisting, user verification and traffic analysis.
- Blacklisting of stolen phones is another mechanism to prevent unauthorized use. An Equipment Identity Register (EIR) enables network operators to disable stolen cellular phones on networks around the world.
- User verification using Personal Identification Number (PIN) codes is one method for customer protection against cellular phone fraud.
- Tests conducted have proved that United States found that having a PIN code reduced fraud by more than 80%.
- Traffic analysis detects cellular fraud by using artificial intelligence software to detect suspicious calling patterns, such as a sudden increase in the length of calls or a sudden increase in the number of international calls.
- The software also determines whether it is physically possible for the subscriber to be making a call from a current location, based on the location and time of the previous call.

FACTS & FIGURES

- Southwestern Bell claims wireless fraud costs the industry $650 million each year

in the US. Some federal agents in the US have called phone cloning an especially `popular' crime because it is hard to trace. In one case, more than 1,500 telephone calls were placed in a single day by cellular phone thieves using the number of a single unsuspecting owner.

- A Home Office report in 2002 revealed that in London around 3,000 mobile phones were stolen in one month alone which were used for cell phone cloning
- Qualcomm, which develops CDMA technology globally, says each instance of mobile hacking is different and therefore there is very little an operator can do to prevent hacking.
- "It's like a virus hitting the computer. The software which is used to hack into the network is different, so operators can only keep upgrading their security firewall as and when the hackers strike," says a Qualcomm executive.

CONCLUSION

Mobile Cloning Is in initial stages in India so 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. Existing cellular systems have a number of potential weaknesses that were considered. It is crucial that businesses and staff take mobile phone security seriously. However, fraud in itself is a social problem. As such, it may be temporarily countered with technological means but they rarely work permanently. Mobile phones are a relatively new phenomenon and social norms to its use have not been formed. Some operators have tried the ``If you can't beat them, join them'' approach and provided services that would otherwise be attained by fraud. As mobile communication matures, both socially and technologically, fraud will settle to some level. Until then, it is a race between the operators, equipment manufacturers and the fraudsters.

REFERENCES

[1] H. Karl and A. Willig, Protocols and Architectures for Wireless Sensor Networks, John Wiley and Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, England,2005.

[2] D. Culler, D. Estrin, and M. Srivastava, “Overview of Sensor Networks”, IEEE Computer, August 2004.

[3] K. Martinez, J. K. Hart and R. Ong, “Environmental sensor networks”, IEEE Computer Journal, Vol. 37 (8), 50-56, August 2004.

[4] Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson, “Wireless sensor networks for habitat monitoring”, Proceedings of the 1st ACM International workshop on Wireless sensor networks and applications, Atlanta, Georgia, USA, 88-97,2002.

[5] F. Akyildiz, D. Pompili and T. Melodia,

[6] “Underwater acoustic sensor networks: research challenges”, Ad Hoc Networks, Vol. 3(3), 257-279, May 2005.

[7] Y. Ma, M. Richards, M. Ghanem, Y. Guo and J. Hassards, “Air Pollution Monitoring and Mining Based on Sensor Grid in London”, Sensors 2008, Vol. 8(6), 3601-3623.

[8] G. Hassard , M. Ghanem , Y. Guo , J. Hassard , M. Osmond , and M. Richards, “Sensor Grids For Air Pollution Monitoring”, in the Proceedings of 3rd UK e-Science All Hands Meeting, 2004.

[9] Khemapech, I. Duncan, and A. Miller, “A survey of wireless sensor networks technology,” in PGNET, In the Proceedings of the 6th Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking & Broadcasting , Liverpool, UK, EPSRC, June 2005.

[10] B. Warnekeand K.S.J PISTER, “MEMS for Distributed Wireless Sensor Networks,” 9th International Conference

on Electronics, Circuits and Systems, Croatia, September 2 002.

[11] B. Son, Y. Her, J. Kim, "A design and implementation of forest –fires surveillance based on wireless sensor networks for South Korea mountains", International Journal of Computer Science and Network Security (IJCSNS), 6, 9 124-130, 2006.