A

Seminar report

On

MOBILE PHONE CLONING

Submitted in partial fulfillment of the requirement for the award of degree
Of Bachelor of Technology in Computer Science

SUBMITTED TO:
www.studymafia.org

SUBMITTED BY:
www.studymafia.org

Preface

I have made this report file on the topic **MOBILE PHONE CLONING**, I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to …………..who assisting me throughout the preparation of this topic. I thank him for providing me the reinforcement, confidence and most importantly the track for the topic whenever I needed it.

Acknowledgement

I would like to thank respected Mr…….. and Mr. ……..for giving me such a wonderful opportunity to expand my knowledge for my own branch and giving me guidelines to present a seminar report. It helped me a lot to realize of what we study for.

Secondly, I would like to thank my parents who patiently helped me as i went through my work and helped to modify and eliminate some of the irrelevant or un-necessary stuffs.

Thirdly, I would like to thank my friends who helped me to make my work more organized and well-stacked till the end.

Next, I would thank Microsoft for developing such a wonderful tool like MS Word. It helped my work a lot to remain error-free.

Last but clearly not the least, I would thank The Almighty for giving me strength to complete my report on time.

Content

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 of 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.

WHAT IS MOBILE PHONE CLONING?

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.

WHEN DID MOBILE CLONING START?

The early 1990s were boom times for eavesdroppers. Any curious teenager with a £100 Tandy Scanner could listen in to nearly any analogue mobile phone call.

As a result, Cabinet Ministers, company chiefs and celebrities routinely found their most intimate conversations published in the next day's tabloids

Cell phone cloning started with Motorola "bag" phones and reached its peak in the mid 90's with a commonly available modification for the Motorola "brick" phones, such as the Classic, the Ultra Classic, and the Model 8000.

GSM

Global System for Mobile Communications. A digital cellular phone technology based on TDMA GSM phones use a Subscriber Identity Module (SIM) card that contains user account information.

Any GSM phone becomes immediately programmed after plugging in the SIM card, thus allowing GSM phones to be easily rented or borrowed.Operators who provide GSM service are Airtel,Hutch etc.

CDMA

Code Division Multiple Access. A method for transmitting simultaneous signals over a shared portion of the spectrum. There is no Subscriber Identity Module (SIM) card unlike in GSM.Operators who provides CDMA service in India are Reliance and Tata Indicom.

IS FIXED TELEPHONE NETWORK SAFER THAN MOBILE PHONE?

The answer is yes. In spite of this, the security functions which prevent eavesdropping and Unauthorized uses are emphasized by the mobile phone companies. The existing mobile communication networks are not safer than the fixed Telephone networks. They only offer protection against the new forms of abuse

SECURITY FUNCTIONS OF THE GSM AND CDMA

As background to a better understanding of the attacks on the GSM and CDMA network The following gives a brief introduction to the Security functions available in GSM. The following functions exist:

- Access control by means of a personal smart card (called subscriber Identity module, SIM) and PIN (personal identification number),

- Authentication of the users towards the network carrier and generation of A session key in order to prevent abuse.

- Encryption of communication on the radio interface, i.e. between mobile Station and base station,

- concealing the users' identity on the radio interface, i.e. a temporary valid Identity code (TMSI) is used for the identification of a mobile user instead Of the IMSI.

HOW BIG OF A PROBLEM IS CLONING FRAUD?

The Cellular Telecommunications Industry Association (CTIA) estimates that financial losses in due to cloning fraud are between $600 million and $900 million in the United States. Some subscribers of Reliance had to suffer because their phone was cloned. Mobile Cloning Is in initial stages in India so preventive steps should be taken by the network provider and the Government.

HOW IS MOBILE CLONING DONE?

Cloning involved modifying or replacing the EPROM in the phone with a new chip which would allow you to configure an ESN (Electronic serial number) via software. You would also have to change the MIN (Mobile Identification Number). When you had successfully 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 pairs were discovered in several ways:

Sniffing the cellular

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 clone able phones 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 it currently remains in the realm of serious hobbyists and researchers.

ARE OUR CELL PHONES SECURED?

Too many users treat their mobile phones as gadgets rather than as business assets covered by corporate security policy. Did you realize there's a lucrative black market in stolen and "cloned" Sim cards? This is possible because Sims are not network specific and, though tamper-proof, their security is flawed. In fact, a Sim can be cloned many times and the resulting cards used in numerous phones, each feeding illegally off the same bill.

But there are locking mechanisms on the cellular phones that require a PIN to access the phone. This would dissuade some attackers, foil others, but might not work against a well financed and equipped attacker. An 8-digit PIN requires approximately 50,000,000 guesses, but there may be ways for sophisticated attackers to bypass it.

With the shift to GSM digital - which now covers almost the entire UK mobile sector - the phone companies assure us that the bad old days are over. Mobile phones, they say, are secure and privacy friendly.

This is not entirely true. While the amateur scanner menace has been largely exterminated, there is now more potential than ever before for privacy invasion.

The alleged security of GSM relies on the myth that encryption - the mathematical scrambling of our conversations - makes it impossible for anyone to intercept and understand our words. And while this claim looks good on paper, it does not stand up to scrutiny.

The reality is that the encryption has deliberately been made insecure. Many encrypted calls can therefore be intercepted and decrypted with a laptop computer.

WHAT ARE EMIE AND PIN?

ESN mean Electronic Serial Number. This number is loaded when the phone number is manufactured. this number cannot be tampered or changes by the user or subscriber. if this number is known a mobile can be cloned easily.

Personal Identification Number (PIN).every subscriber provides a Personal Identification Number (PIN) to its user. This is a unique number. If PIN and ESN are know a mobile phone can be cloned in seconds using some software's like Patagonia. Which is used to clone CDMA phones.

WHAT IS PATAGONIA?

Patagonia is software available in the market which is used to clone CDMA phone. Using this software a cloner can take over the control of a CDMA phone i.e. cloning of phone. There are other Software's available in the market to clone GSM phone. This software's are easily available in the market. A SIM can be cloned again and again and they can be used at different places. Messages and calls sent by cloned phones can be tracked. However, if the accused manages to also clone the IMEI number of the handset, for which software's are available, there is no way he can be traced.

CAN DIGITAL PHONES BE CLONED?

Yes. Digital phones can be cloned however; the mobile phones employing digital TDMA and CDMA technology are equipped with a feature known as "Authentication." Some newer model analog phones also have this feature. Authentication allows the mobile service provider network to determine the legitimacy of a mobile phone. Phones determined to be "clones" can be instantly denied access to service before any calls are made or received.

HOW TO KNOW THAT THE CELL HAS BEEN CLONED?

- Frequent wrong number phone calls to your 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 your phone bills

CAN CALLS ON CLONED PHONE BE TRACKED?

Yes. A SIM can be cloned again and again and they can be used at different places. Messages and calls can track sent by cloned phones. However, if the accused manages to also clone the IMEI number of the handset, for which software's are available, there is no way the cell can be traced.

HOW TO PREVENT MOBILE CLONING?

Uniquely identifies a mobile unit within a wireless carrier's network. The MIN often can be dialed from other wireless or wire line networks. The number differs from the electronic serial number (ESN), which is the unit number assigned by a phone manufacturer. MINs and ESNs can be checked electronically to help prevent fraud.

.Mobiles should never be trusted for communicating/storing confidential information.

Always set a Pin that's required before the phone can be used.

Check that all mobile devices are covered by a corporate security policy.

Ensure one person is responsible for keeping tabs on who has what equipment and that they update the central register. How do service providers handle reports of cloned phones?
Legitimate subscribers who have their phones cloned will receive bills with charges for calls they didn't make. Sometimes these charges amount to several thousands of dollars in addition to the legitimate charges.

Typically, the service provider will assume the cost of those additional fraudulent calls. However, to keep the cloned phone from continuing to receive service, the service provider will terminate the legitimate phone subscription. The subscriber is then required to activate a new subscription with a different phone number requiring reprogramming of the phone, along with the additional headaches that go along with phone number changes.

WHAT EXACTLY IS AUTHENTICATION?

Authentication is a mathematical process by which identical calculations are performed in both the network and the mobile phone. These calculations use secret information (known as a "key") preprogrammed into both the mobile phone and the network before service is activated. Cloners typically have no access to this secret information (i.e., the key), and therefore cannot obtain the same results to the calculations.

A legitimate mobile phone will produce the same calculated result as the network. The mobile phone's result is sent to the network and compared with the network's results. If they match, the phone is not a "clone."

ARE THESE METHODS EFFECTIVE?

Yes, for the most part. However, Authentication is the most robust and reliable method for preventing cloning fraud and it is the only industry "standard" method for eliminating cloning. The fact that it is standardized means that all mobile telecommunications networks using IS-41 can support Authentication. There is no need to add proprietary equipment, software, or communications protocols to the networks to prevent cloning fraud.

IS MY PHONE AUTHENTICATION CAPABLE?

If the phone supports TDMA or CDMA digital radio, then yes. Otherwise, it depends on how old the phone is and the make and model. Almost all phones manufactured since the beginning of 1996 support the Authentication function. The best bet is to check with your service

ROLE OF SERVICE PROVIDER TO COMBAT CLONING FRAUD?

They are using many methods such as RF Fingerprinting, subscriber behavior profiling, and Authentication. RF Fingerprinting is a method to uniquely identify mobile phones based on certain unique radio frequency transmission characteristics that are essentially "fingerprints" of the radio being used. Subscriber behavior profiling is used to predict possible fraudulent use of mobile service based on the types of calls previously made by the subscriber.

Calls that are not typical of the subscriber's past usage are flagged as potentially fraudulent and appropriate actions can be taken.

Authentication has advantages over these technologies in that it is the only industry standardized procedure that is transparent to the user, a technology that can effectively combat roamer fraud, and is a prevention system as opposed to a detection system.

WHAT IS IS-41?

IS-41(Interim Standard No. 41) is a document prescribing standards for communications between mobile networks. The standard was developed by the Telecommunications Industry Association (TIA) and is used primarily throughout North America as well as many Latin American countries and Asia.

The IS-41 network communications standard supports AMPS, NAMPS, TDMA, and CDMA radio technologies. IS-41 is the standard that defines the methods for automatic roaming, handoff between systems, and for performing Authentication.

WHAT CAN BE DONE?

With technically sophisticated thieves, customers are relatively helpless against cellular phone fraud. Usually they became aware of the fraud only once receiving their phone bill.

Service providers have adopted certain measures to prevent cellular fraud. These include encryption, blocking, blacklisting, user verification and traffic analysis: Encryption is regarded as the most effective way to prevent cellular fraud as it prevents eavesdropping on cellular calls and makes it nearly impossible for thieves to steal Electronic Serial Number (ESN) and Personal Identification Number (PIN) pairs.

Blocking is used by service providers to protect themselves from high risk callers. For example, international calls can be made only with prior approval. In some countries only users with major credit cards and good credit ratings are allowed to make long distance calls.

- 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. Currently, South Africa's two service providers, MTN and Vodacom, use traffic analysis with the International Mobile Equipment Identity (IMEI) — a 15 digit number which acts as a unique identifier and is usually printed on the back of the phone underneath the battery — to trace stolen phones.

Other warning signs that subscribers should watch out for to detect fraudulent activity include:

Frequent wrong number phone calls to your 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 your phone bills.

CONCLUSION

Presently the cellular phone industry relies on common law (fraud and theft) and in-house counter measures to address cellular phone fraud.
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.

REFERENCES

Wireless A-Z
Nathan J.Muller.

Fundamentals of Mobile and Pervasive Computing
Frank Adelstein, Sandeep Gupta.

Wireless and Cellular Communication 3rd Edition
William C.Y.Lee.

Introduction to Telecom Communication Converging Technologies 1st Edition
Kimberly Massey.

3G Networks 1st Edition
Clint Smith, Saniel Collins