SREENIVASA INSTITUTE OF TECHNOLOGY AND MANAGEMENT STUDIES

MOBILE PHONE CONING

by

A K BASHA
INTRODUCTION

- WHAT IS CELL PHONE CLONING?
- WHEN DID CELL CLONING START?
- GSM
- CDMA
- SECURITY FUNCTIONS OF THE GSM AND CDMA
- HOW BIG OF A PROBLEM IS CLONING FRAUD?
- HOW IS CELL CLONING DONE?
- ARE OUR CELL PHONES SECURED?
- CAN DIGITAL PHONES BE CLONED?
- HOW TO KNOW THAT THE CELL HAS BEEN CLONED?
- CAN CALLS ON CLONED PHONE BE TRACKED?
- HOW TO PREVENT CELL CLONING?
WHAT IS CELL PHONE CLONING?

- Cell phone cloning is copying the identity of one mobile telephone to another mobile telephone.
- The purpose of cell phone cloning is making fraudulent telephone calls.
- The bills for the calls go to the legitimate subscriber.
- The cloner is also able to make effectively anonymous calls, which attracts another group of interested users.
WHEN DID CELL CLONING START?

- 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.

- 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.
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, Vodafone etc.
• 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 like in GSM.
• Operators who provide CDMA service in India are Reliance and Tata Indicom.
BRIEF SECURITY FUNCTIONS OF
THE GSM AND CDMA

• Access control by means of a SIM CARD and PIN,
• Authentication of the users towards the network carrier
• Encryption of communication on the radio interface
• concealing the users’ identity on the radio interface,
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 CELL 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.
REQUIREMENTS

• Cloning required access to ESN and MIN pairs.
• ESN/MIN pairs were discovered in several ways:
  Sniffing the cellular,
  Trashing cellular companies,
  Hacking cellular companies.
• 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.
WHAT IS ESN NUMBER

• 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.
WHAT IS PIN NUMBER

- 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 like PATAGONIA.
- Patagonia used to clone CDMA phones.
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.
HOW TO PREVENT CELL CLONING?

- The MIN often can be dialed from other wireless or wireline 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.
- 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.
- Authentication
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 preprogrammed into both the mobile phone and the network before service is activated.
- Cloners typically have no access to this secret information, 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."
CONCLUSION:

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