MOBILE CLONING

INTRODUCTION

1. Cell phone cloning is a technique wherein secured data from one cell phone is transferred into another phone. 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 and received by both phones, only the legitimate subscriber is billed as the service provider network does not have a way to differentiate between the legitimate phone and the “cloned” phone. The cloner can set the options to ring his phone when you make a call and you will have no idea that the cloner is listening from his own mobile. He can read text message, phone book entries, look at pictures etc. Also he can dial phone numbers from their phone and a whole lot more. So when one gets huge bills, the chances are that the phone is being cloned. Millions of cell phones users, be it GSM or CDMA, run at risk of having their phones cloned.

PROCESS

2. Cloning is the process of taking the programmed information that is stored in a legitimate mobile phone and illegally programming the identical information into another mobile phone. The culprits clone and hack into your phone using software’s that are easily available, once the software is installed they just need the unique IMEI number of the phone and they can digitally imprint these numbers on any of the phone they want. Once this is done they can send messages, make calls to anyone and the person whose phone has been cloned and hacked will be held responsible.

3. **FOR CDMA** 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.

4. **FOR GSM** 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. However, cloning GSM phones is achieved by cloning the SIM card contained within, not necessarily any of the phone’s internal data. GSM phones do not have ESN or MIN, only an IMEI number. GSM SIM cards are actually copied by removing the SIM card and placing a device between the handset and the SIM card and allowing it to operate for a few days and extracting the KI, or secret code. 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.
SOFTWARES AVAILABLE FOR CLONING

5. **FOR CDMA.** If PIN and ESN are known, a mobile phone can be cloned in seconds using some software’s like Patagonia which is used to clone CDMA phones.

6. **FOR GSM.** 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. BLUETOOTH HACK is the software available in the market which is used to hack/clone GSM phone.

CLONING FRAUD PROBLEM

7. 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. The Cellular Telecommunications Industry Association (CTIA) estimates that financial losses 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.
CHECKOUTS WHETHER YOUR CELLPHONE IS CLONED OR NOT

8. Unfortunately, there is no way the subscriber can detect cloning. Events like call dropping or anomalies in monthly bills can act as tickers. But some points mentioned below can help you.

(a) Frequent wrong number phone calls to your phone, or hang-ups.
(b) Difficulty in placing outgoing calls.
(c) Difficulty in retrieving voice mail messages.
(d) Incoming calls constantly receiving busy signals or wrong numbers.
(e) Unusual calls appearing on your phone bills.

PREVENTIVE MEASURES TO PROTECT YOUR MOBILE FROM CLONING

9. The best way to prevent your SIM card or mobile phone from being cloned is to use Authentication feature. 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”) pre-programmed 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.”

AUTHENTICATION EFFECTIVENESS

10. 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

11. 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.
CONCLUSION

12. To conclude, cell phone communication is one of the most reliable, efficient and widespread. The usage of the system can be changed in either constructive or destructive ways. Unfortunately the security standards are quite easy to breach and takes very less amount of time. Moreover, cloning methodology is widespread and can be implemented easily. Hence, it must be considered that the security system which was implemented lately must not be fruitful enough to secure the system in future. Therefore it is absolutely important to verify the working of a protection system over a precaution system every once a while and change or update it every once a year.

REFERENCES

13. References are as under:-


(b) Security Management Against Cloned Cellular Phones : Mirela Sechi Moretti Annoni Notare Fernando Augusto da Silva Cruz Bernardo Gonçalves Riso Carlos Becker Westphall Federal University of Santa Catarina (UFSC).

(c) Cellular Telephone Cloning Final Report Economic Crimes Policy Team United States Sentencing Commission, January 25, 2000