ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 4, April 2015

Study of Cell Phone Cloning

Mukesh Patel[1], Ankit Naik[2], Purushottam Patel[3]
Student,CSE, Kirodimal Institute of Technology, Raigarh,India[1]
Lecturer CSE, Kirodimal Institute of Technology, Raigarh,India[2]
HOD CSE, Kirodimal Institute of Technology, Raigarh,India[3]

Abstract: Nearly 1.1 billion telecom subscriber worldwide ,as because of not only the ease to communicate with the other person over worldwide by a cell phone and also through its the modern technology providing lots of features and facilities like banking , shopping, social networking and many more in a cell phone. That's why everyone want their own individual cell phone. Estimated that worldwide mobile phone fraud will reach $40 billion dollars soon. Cell phone cloning means that to preparing an another cell phone that have same ESN(electronic serial number) or CTN (cellular telephone number) for CDMA (Code Division Multiple Access) and IMEI (International Mobile Station Equipment Identity Number) for GSM (Globle System of Mobile Communication) by which also make and receive call from its but only the original one will pay for it.
Keywords: Cloning, Cell phone cloning.

I. INTRODUCTION

Cell phones are complex electronic devices, sensitive to heat, cold and excess moisture. But a cell phone's sensitivity isn't limited to extreme weather conditions. Analog cell phones, as opposed to the newer digital phones, can be cloned. This means that someone can tap into your cell phone's personal identification number and makes calls on the same account. In other words, with a little technical know-how, someone can steal your phone number and charge the calls made to your account. You won't even know it's happened, until you get your phone bill. How does cloning happen if each phone has its own unique identifying features? Whenever you dial a number from your cell phone, the ESN (electronic serial number) and MIN (mobile identification number) of your phone are transmitted to the network, identifying the cell phone dialed from and who to bill. Some people, who work in the way that computer hackers operate, can use a scanner to listen in to this transmission and capture the code. They can then use the information they gather to make calls that are then charged to the account of the phone number they have in effect "broken into." Cloning is the creation of an organism that is an exact genetic copy of another. Cell Phone Cloning is the cloning of process of taking the programmed information that is stored in a legitimate Mobile phone and illegally programming the identical information into another mobile phone.

II. PROCESS OF CLONING

Cloning involves 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. MIN (Mobile Identification Number) should also have to change. When the ESN/MIN pair had changed successfully then an effective clone of the original phone has created. Cloning Required Access to ESN and MIN pairs.ESN/MIN pairs were discovered in several ways:

1. Sniffing the cellular.
2. Trashing celling companies or cellular resellers.
3. Hacking cellular companies or cellular resellers.

A. Cloning In GSM Cell Phone

GSM stands for Global System for Mobile Communication. Its use a Subscriber Identity Module (SIM) Card. It's Standard Set Developedby European Telecommunications Standard Institute (ETSI) To Describe Technologies for Second Generation (2G) Digital Cellular Network.

- The Important Information Is IMSI, Which is Stored on the Removal Sim Card.
- Sim Card Inserted Into a reader.
- Connect to computer and card details transferred.
- Use encrypted card to interpret details as result a cloned cell phone is ready for replica.

B. Cloning In CDMA Cell Phone

CDMA stands For Code Division Multiple Access. A method oftransmitting simultaneous signals over a shared portion of the spectrum. It's Use a Mobile Identification Number (MIN) Card That Contains User account Information.

- Cellular Telephone thieves monitor the radio frequency Spectrum.
- Steal their Cell Phone pair as it is being anonymously registered with a cell site.
- Subscriber information is also encrypted and transmitted digitally.
- A device called DDI, Digital Data Interface Can Be Used to Get Pairs.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 4, April 2015

- Stolen ESN and MIN were then fed into a New CDMA Handset.

III. WHAT CAN HAPPEN

Researchers were able to eavesdrop and record all voice calls, intercept incoming SMS and MMS messages, launch a man-in-the-middle attack to view Web sites being accessed, and strip SSL from secure pages, Tom Ritter, principal security engineer at iSec Partners said. They were also able to clone mobile devices without having physical access to the device. It could intercept cellular signals at even 40 feet away, depending on certain environmental factors, Ritter said.

Ritter and DePerry demonstrated how a phone call to DePerry's phone was recorded, and displayed a phone's incoming text messages on a computer screen. They also intercepted MMS messages, a list of Web sites being accessed from a mobile device, and any information entered on those Websites (including passwords).

"Eavesdropping was cool and everything, but impersonation is even cooler," DePerry said, noting that femtocells are essentially mini towers. With a rogue femtocell, an attacker can become the person holding the targeted mobile device without ever touching the phone, he said. If someone was calling the victim's phone, the attacker's cloned phones would also ring, letting the attacker listen to the call in a "2.5 way" calling. Without a femtocell, an attacker interested in cloning a mobile device could "wait for the victim to go to the bathroom and write down the identifiers associated with the phone," DePerry said. It's much easier, and harder to get caught, if you just set up the femtocell and wait for mobile devices to register automatically with the tower. All the necessary identifiers are transmitted during the registration process, so attackers can easily get the information to create a cloned phone without ever touching the victim's device, DePerry said.This hack targeted a Verizon femtocell, which is on a CDMA network. Verizon has patched the issue, although both Ritter and DePerry declined to discuss the patch's effectiveness. A similar vulnerability was found in a femtocell from Sprint, as it was made by the same manufacturer. However, it is nad've to think the problem is specific to a manufacturer or to a particular carrier. "Femtocells are a bad idea," Ritter said, noting that Verizon, Sprint, and AT&T all offer femto cells.While the immediate danger has been addressed, iSec Partners has "serious architectural concerns about femtocells," DePerry said. The better option is for carriers to stop using femtocells altogether and look into WiFi calls using IPSec or SSL Tunnels for security. Until the carriers take steps to secure the calls, users can encrypt their calls, using tools such as RedPhone or Ostel, Ritter said.

PATAGONIA Software 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. 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.

IV. DETECTION TECHNIQUES

Velocity trap: The mobile seems to be moving at impossible or most unlikely speed.

RF Radio Frequency: Normally identical Radio Equipment has a distinguishing "fingerprint", so the network software stores and compares fingerprint for the entire phone that it sees.

Call Counting: Both the phone and the network keep track of calls made with the phone, and should the differ more than the usually allowed one call, service is Denied.

Pin Codes: Prior to placing a call, the caller unlock the phone by entering a pin code and then calls as usual.

V. CELL PHONE CLONING SYMPTOMS & MEASURES

A. *SYMPTOMS*

- Difficulty in placing outgoing.
- Difficulty in retrieving voice mail message.
- Incoming calls constantly receiving busy signal or wrong number.
- Unusual calls appearing on your phone bills.

B. *MEASURES TO BE TAKEN*

Blacklisting: -blacklisting of stolen phones is another Mechanism to prevent unauthorized use.

PIN: User Verification Using Personal Identification Number (PIN) codes is one method for customer Protection against Cellular Phone Fraud.

Encryption : Encryption is regarded as the effective way to prevent cellular Fraud.

Blocking : Blocking is used by Service provider to Protect themselves from high risk Callers.

VI. ADVANTAGES & DISADVANTAGES

A. *ADVANTAGES*

- If your phone has been lost , you can use your cloned cell phone.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 4, April 2015

- If your phone got damaged or if you forgot your phone at home or any other place . Cloned phone can be helpful

B. *DISADVANTAGES*

- It can be used by the terrorists for criminal activities.
- It can be used by the cloner for fraud calls.
- It can be used for illegal money transfer.

VII. CONCLUSION

Cell Phone is in Initial Stages in Some Countries. Preventive Steps Should be taken by the network Provider and the Government. The Enactment of legislation to prosecute crimes related to cellular phone is not viewed as a priority. The cloning of a CDMA Mobile phones was Possible because there was no protection to the identity information.

REFERENCES

[1] http://www.cdmasoftware.com/eng.html

[2] http://infotech.indiatimes.com

[3] http://www.hackinthebox.org/

[4]http://blog.metasploit.com/2007/09/root-shell-in-my-pocket-and-maybe-yours.html.