Reversing Caller ID Spoofing

By: Janette Archie
Caller ID was originally invented to allow people to identify the person that was calling them. Caller ID is available in digital phone systems and most VoIP applications. It can be used to limit prank calls, telemarketers and other annoyances. Caller ID is sent to a recipient using the Frequency Shift Keying (FSK) technique, which sends ASCII character data to the Caller ID box. This message is sent between the first and second ring. This message also contains a lot of valuable information about the caller other than just the phone number. It contains the length of the message, the month, day, hour and minute of the call, and the type of message that is being sent to the recipient. When a cellular phone call is being placed it radios into the nearest cell tower and sends the message that contains the phone number and other information to that tower. The tower then sends the message to a wireless access point that is connected to a multi-port switch. This switch then sends the phone call to the nearest cell tower of the recipient, which sends it to the recipient’s cellular phone displaying the caller’s phone number and name.

Caller ID spoofing is when you change the Caller ID number to any working number that you want to display to the recipient. There are different techniques that you can use to do so. One technique uses a PRI line, a PBX and a SIP. The most used PBX open source software is Asterisk. Asterisk powers the IP PBX systems, VoIP gateways, conference servers and more. There is a function in Asterisk that allows you to set the Caller ID number, “Set(CALLERID())”. This makes it easier for programmers because it gives you more flexibility with your calls and a direct connection with the VoIP provider. Another technique is by writing PERL or PHP scripts that allow you to do more than just spoof the phone call. These scripts can allow the caller to change their voice, record the phone call and have it emailed to the caller.

In this paper I will focus on the Caller ID Faker android application, which allows you to choose a working number to display instead of your number. This application also allows you to modify your voice to a male or female voice and record the phone call. To stop Caller ID spoofing I will attempt to write an application that uncovers the spoofed phone number and reveal the correct number of the caller. This application will use a direct callback system to call the incoming number to tell if the number is busy or idle. By using this method i will be able to determine if the caller is real or a fraud. This application will also help protect the recipients or victims of these fraudulent phone calls and possibly save lives.

Caller ID spoofing was originally used for companies so that customers could only see the company's public or main phone number and not each individual employee phone number. However, these companies were still using the company's phone number, making it perfectly legal. Now Caller ID spoofing is being used for prank calls, wire fraud, voice mail hacking, and threats. These villains use these techniques to get over on people or to cover their tracks when they are attempting an illegal mission. Such as, when a bomb threat is called in, the police send a bomb squad to whatever location that is connected with the phone number on the caller ID. This gives the bomber more time to escape or complete the mission he/she has planned. Some villains have used Caller ID spoofing to wire money out of innocent people's bank accounts, since some company's use Caller ID to make sure that the customer is calling from their home phone number. These villains spoof their phone numbers to transfer money out of these accounts pretending to be the owner of the account. Others use Caller ID spoofing to make threats over the phone. There have been instances of people using spoofing to get what they want. For example, a kidnapper my use spoofing to call the family of the child to place threats on the child and/or family. The most common way to use Caller ID spoofing now is for prank calls. Most people see prank calls as just a joke and harmless. However, there have been some known to cause emotional and mental distress.

It is important that we solve this problem so that these villains do not get away with hiding their identities.

The only research that has been done with this issue is from a company called TelTech, the owner of the application TrapCall. This application allows you to view who’s calling you if the caller’s...
number is blocked or private. However, their application has nothing to do with spoofed phone calls. My research is unique because this will be the first time anyone has attempted to create an application to prevent Caller ID spoofing.

For this project I researched two different approaches to prevent Caller ID spoofing. The first approach was to contact the cell tower and request the phone number that was calling the recipient's cellular phone. A cellular phone sends a message to the cell tower every few seconds to alert the cell tower that the cellular phone is available to place and receive calls and/or messages. This allows the tower to know the Caller ID number before it is changed. The process of doing this is simply writing a request to the cell tower and switch to find the caller of the incoming call. The second approach was to call back the phone number of the incoming phone call. By calling back the phone number I am looking for a tone stating that the phone is busy. If the tone is busy it will tell that there is a possibility that this is truly the incoming call. The process of doing this is to place the incoming call on hold and be able to dial out the number to the incoming call. In this I decided to use the already created Android source code modify a few of the telephony methods.

I chose to continue with the second approach due to time and preferring not to work with the network because I did not have access to the cell towers. Although I feel that the first approach would have been a better approach because there is a higher percentage that it will give the correct Caller ID number. Unlike the first approach which has its downfalls.