ANI and Caller ID Spoofing

Intro

This article will explain many methods of caller ID and ANI spoofing that can still be used as of today. I have also included a brief FAQ for those of you who may not be familiar with the terminology and should help you understand this article more. I hope that this article will make many of you aware that Caller ID and ANI, though often can be used as great tools, can also be a waste of your time and money. Please don't confuse this article with past's articles I've wrote, though this article does mention techniques I have used in the past it does include up to date accurate information and is meant to be a reference article on how caller ID and ANI can be spoofed and has been spoofed in the past so that all of those telco techs out there that claim it can't be done have definite proof that it has been. You will also find some useful links at the end of this article, enjoy.

First some FAQs

So, just what is ANI?

ANI stands for Automatic Number Identification. ANI is a service feature that transmits a directory number or Billing Telephone Number(BTN) to be obtained automatically. In other words your number is sent directly to wherever you are calling to automatically. Unlike Caller ID you can not block this feature from happening.

What is flex ANI?

Flexible ANI provides "II"(identification indicator) digits that identify the class of service of the phone you are calling from.

What is CPN?

Calling Party Number, the number used for your caller ID.

What are ANI "II" digits?

Identification Indicator digits describe the class of service of the telephone.

Some examples are:

00 "POTS"(plain old telephone service) or home phone

07 Restricted line

27 ACTS payphone

29 Prison phones

62 Cellular phones

70 Cocot Payphone

What is an ANAC?

ANAC stands for Automatic Number Anouncement Circuit. This is a phone number you can call that will ring into a circuit that anounces the ANI or CPN number you are calling from. An example of an ANAC is 800-555-1140 and 800-555-1180. When you call this number you will get an ARU(Audio Response Unit) this is the circuit that anounces your ANI/CPN. When you call 800-555-1140 or 800-555-1180 the ARU will give you this information: "The ARU ID is [id], Your line number is [trunk number], the DNIS is [DNIS number] the ANI is [II digits followed by CPN, even though the recording claims to be reading ANI]"

(These ANACs don't work anymore, try 800-444-4444)

ARU ID: Audio Response Unit ID number, this identifies which ARU in a group of ARUs you reached.

Line number: The trunk you came in on.

DNIS: Dialed Number Identification Service -- Tells you which number YOU called.(i.e. 800-555-1140 is 03123, 800-555-1180 is 03125)

ANI: II digits followed by ANI.

What is a BTN(Billing telephone number)?

BTN is a phone number for which charges are to be billed to. It is not necessarily the phone number of the line you are calling from.

What is Psuedo ANI?

Psuedo ANI or PANI is a unique non-dialable number used to route cellular calls. PANI is used by 911 operators to find the cell site and sector from which the cellphone is calling.

What is an ANI fail?

An ANI fail is when no ANI is sent. Usually the areacode of the tandem office completing the call will be sent.(i.e. if the tandem office is in 213 the ANI will be sent as 213-000-0000.)

How do ANI fails occur?

ANI fails can occur when the tandem office completing a call didn't receive ANI from the central office originating the call. ANI fails can also be caused when ANI is intentionally not sent, this can happen by using a method called op diverting. Another way you can cause ANI fails is through the use of the AT&T long distance network. Simply dial 10-10-288-0 or dial 0 and ask your operator for AT&T. When AT&T comes on the line simply touch tone in a toll free number and the call will be completed with no ANI. Note however that this method is dependent on the AT&T center you reach, some AT&T centers still forward ANI, others send an AT&T BTN as ANI, but most AT&T centers currently don't forward ANI.

What is op diverting?

Op diverting is a term that describes the process of intentionally causing an ANI fail by having your local operator dial the number you wish to reach. Most operator centers are not equipped to forward ANI and so they complete the call with no ANI.

What's the difference between ANI and Caller ID?

ANI is the BTN associated with the telephone and is the direct number from where you are calling from. Caller ID is usually the BTN but occasionally can be incorrect, i.e. the main number of a business instead of the actual number being called from. Another difference in ANI is that it shows the class of service of the phone number while Caller ID just shows the name and number.

Now that you have an idea of what ANI is and how it differs from Caller ID I will explain some methods for spoofing both of them.

Spoofing Caller ID

Method #1 Using a PRI line.

Major companies that have a PBX with many hundreds of lines hooked up to a Primary Rate ISDN(PRI) line can spoof caller id by setting the caller ID number to whatever number you want for a given extension on that PBX by typing a simple command on the PBX's terminal.

NOTE: In my 2600 article I was talking about how this method also spoofs ANI, I'm actually wrong about this, it spoofs CPN, not ANI! hah maybe I should read my own FAQs! Anyways, CPN is the Directory Number on the switch, it is not the BTN! The real ANI is the BTN. Most 800 numbrs use CPN, not real ANI, so I thought ANI was being spoofed but in actuality it was only the CPN being spoofed.

Method #2 Orangeboxing

Orangeboxing is Caller ID signal emulation through the use of a bell 202 modem, sound card software, or a recording of a Caller ID transmission. Orangeboxing is not very effective because you have to send the signal AFTER the caller has answered their phone. However through the magic of social engineering you could have one friend call a number and pretend he has reached a wrong number while sending a Callwaiting Caller ID signal fooling the victim into believing he is receiving another incoming call from the name and number spoofed and when the victim "flashes over" have your friend hand you the phone nand continue with your social engineer.

Method #3 Calling Cards

I learned this method from some phone phreaks on a party line a long time ago. I can't recall the name of the calling card company but all one had to do was provide a credit card as a method of payment to obtain a pin number. Once you had the pin number you just op divert or cause an ANI fail to the 800 number for the calling card and it would ask you to please enter the number you are calling from, you touch tone in ANY number you want, then it would ask for your pin number and then what number you wanted to call. The person you called would see the number you touched tone in as the caller ID for that call, if the number was in the same area as the caller it would also show the name associated with the phone number.

Method #4 Social Engineering

This method for spoofing Caller ID is social engineering a Telus operator to do it for you. I stumbled upon this method when I was testing out a theory. In my previous 2600 article about spoofing ANI through AT&T I mentioned something known as the 710 trick. This was a method of making collect calls that the called party wouldn't be billed for. The way the 710 trick worked in the past was you'd op divert to 800-call-att and give the operator a 710 number as where you are calling from and have her place a collect call to the number you want to call. The called party would never get a bill because 710 is a non-existant area code. AT&T does it's billing rates by where the call is being placed from and to and because you used a 710 number there were undetermined rates. I was testing to see if the 710 trick also worked with a canadian phone company called Telus. After testing it out my friend in canada dialed *69 and it read back the 710 number I gave the operator, this is how I discovered Caller ID spoofing was possible through Telus and I began to come up with a social engineer to get them to place a call for me without selecting a billing method. I now know that it is also possible to spoof ANI through Telus.

Telus' toll-free "dial-around" is 800-646-0000, by simply calling this number with an ANI-fail you can give the operator any number as where you are calling from. As of January 2003, Telus can now place calls to many toll free numbers and the CPN will show up as whatever number you say you're calling from. So by simply causing an ANI-fail to Telus dial-around service you can spoof Caller ID to anyone you want to call, not only that if the person you are calling is in the same area as the number you are spoofing, the NAME and number shows up on the caller ID display. To cause an ANI fail to Telus all you have to do is op-divert to 800-646-0000 or dial 10-10-288-0 and touch tone 800-646-0000 when AT&T comes on the line.

You can social engineer the Telus operator to place "test calls" for you which is a free call with no billing, you simply tell the Telus operator at the beginning of the call that you are a "Telus technician" calling from [number to spoof] and need her to place a "Test call" to [number to call].

The social engineer pretext looks like this:

You pick up the phone, at dialtone 10102880

AT&T Automated Operator: "AT&T, to place a call"

Touch tone 800-646-0000

AT&T Automated Operator: "Thank you for using AT&T"

<RING>

Telus: This is the Telus operator, Lisa speaking. (or, This is the telus operator, what number are you calling from?)

You: Hi Lisa, This is the Telus technician, you should see an ANI failure on your screen, I'm calling from [number to spoof]

I need you to place a test call to [number to call]

Telus: Thank you from Telus

What just happened was AT&T sent an ANI fail to Telus, you told the operator to key in your new number calling from, Telus then places the call and uses the number you gave as both ANI and CALLER ID! NOTE about spoofing ANI to Toll freee numbers: Not all US toll free numbers are accessable from Canadian trunks, so even though you are spoofing a US number the call will not be able to be routed through Telus.

Of course, the social engineer will probably become ineffective soon, though I've demonstrated it at H2K2 in July 2002 and It's now 2003 and is still working. The spoofed caller ID also shows up on collect calls(though I think you can only call people in Canada collect with this service), third party billing (would you accept a third party bill call if the caller ID said your girlfriends number and the op said she was the one placing the call? :)), and calling card calls, so you could even legitamatily spoof Caller ID if you had a Telus calling card, however the rates are pretty expensive, though you can get one if you have Telus as your local phone company or if you live outside Canada you can pay with a credit card (you need a Canada billing address though!), call 1-800-308-2222 to order one.

Method #5 VXML

Using a vxml service like cafe.bevocal.com you can write a script to spoof caller ID for you. An example script can be found at www.erased.us/bevocal.xml

Method #6 Voicepulse

Order Voicepulse voip service, turn callforwarding on and forward your calls to who you want to spoof your caller ID to. Set Anonymous Call Rejection with Prompting on. Call your voicepulse number with your caller ID blocked, enter a phone number you want to spoof when asked for your number, your call will go through and be forwarded with your caller ID spoofed.

Method #7 Vonage

Call up and order vonage service, say you want to port your 'cellphone' number over while signing up for the service. When they ask for your cellphone number to port over give the number you want to spoof. You'll be notified that you have to send a Letter Of Authorization(LOA) in to them before they can port the number, however your caller ID will still show the number you're "porting". You can also RECEIVE calls at the 'ported' number if someon on vonage trys to call that number. All other callers will reach the right number, this is a vonage glitch.

Method #8 Asterisk

Find an IAX provider that allows you to set your own CPN, you can then set up the CPN for your outbound calls as anything you want.

Spoofing ANI

Spoofing ANI is a little more difficult than spoofing Caller ID unless you have access to a central office switch.

A while ago AT&T used to sendANI when you placed calls to toll free numbers through the AT&T network and you could only call 800 numbers that were hosted by AT&T, after publishing an article about how to spoof ANI by op diverting to 800-call-att AT&T had their networked changed within a month of publication. Their new network however just made it easier to cause ANI fails to toll free numbers. On the new network you could call any toll free number, not just AT&T hosted numbers, and their would be no ANI on the call, unless you were calling 800-call-att or a few other numbers that are internal numbers hosted by the call center it's self. All you have to do to cause ANI fails to toll free numbers now is dial 10-10-288-0 and touch tone the 800 number in when AT&T comes on the line. This method of causing ANI fails is great because you don't have to speak to a live operator and you can even have your modem wardial 800 numbers without fear of your ANI being logged.

However there might be some AT&T call centers that still forward ANI, and you may be able to reach them even if the call centers aren't in your area, try op diverting to an AT&T language assistance operator since it is not likely that your call center will have a Tagalog speaking operator so you will get routed to a different AT&T center that does, possibly an AT&T center that still forwards ANI. If you get an AT&T center that still forwards ANI you can spoof ANI by simply giving the operator the number you want to spoof as where you are calling from and social engineering her into placing a call to the toll free number you wish to call. Here are some AT&T language assistance numbers:

1 800 833-1288 Cantonese

1 800 233-7003 Hindi

1 800 233-8006 Japanese

1 800 233-8923 Korean

1 800 233-1823 Mandarin

1 800 233-8622 Polish

1 800 233-2394 Russian

1 800 233-9008 Spanish

1 800 233-9118 Tagalog

1 800 233-1388 Vietnamese

Links:

www.stromcarlson.com

- Strom Carlson's website.

www.verizonfears.com

- Verizown

lab.digitol.net/callerid.html

- Spoob Open Source Orangebox perl script and online CGI

www.artofhacking.com/orange.html

- Shareware 'Software Orange Box' for Windows.

www.codegods.net/cidmage

- CIDMAGE Caller ID tone generator and FSK analyst.

www.testmark.com/develop/tml_callerid_cnt.html

- Everything you ever wanted to know about caller ID.

UPDATES:

5/12/2003 - AT&T's AUTOMATED OPERATOR(10-10-288-0) has BLOCKED