# 7

# UNCONVENTIONAL VOIP SECURITY THREATS

In addition to protocol attacks on SIP, H.323, IAX, and RTP, as well as attacks against specific VoIP products, many unconventional attacks against VoIP networks can cause a lot of harm. For example, in the email world, a spam attack is neither sophisticated nor complex to perform; however, the headaches spam has brought to email users, from the nuisance of bulk email to phishing attacks, make spam a major issue for email users. This chapter will take a similar approach to VoIP by showing existing attacks that have the potential to be a major nuisance.

The focus of this chapter will be how VoIP technologies, while very complex themselves, are still open to many simple attacks that can cause a lot of damage. When these minor flaws are applied to trusted entities, such as a user's telephone, they have the ability to trick users into doing things they normally would not do. When, for example, an email asks you to click a link and submit your personal information, most users are wise enough to ignore that request. However, what if users received an automated phone call purportedly from their credit card company's fraud detection services? Would users follow the directions in the message? Would they check if the 800 number provided in the message matches the one on the back of their credit card? This scenario, along with many others, is discussed in this chapter.

The attacks shown in this chapter combine the weaknesses of VoIP networks, the ability to perform social engineering attacks on human beings, and the ability to abuse something we all feel is trustworthy (our telephone) to compromise VoIP end users. Specifically, the attacks shown in this chapter are the following:

- VoIP phishing
- Making free calls (in the United States and United Kingdom)
- Caller ID spoofing
- Anonymous eavesdropping/call redirection
- Spam Over Internet Telephony (SPIT)

Before we begin this chapter's discussions, take a few moments to set up the necessary lab environment. Completing the following steps will ensure that the proof of concept attacks shown in this chapter will work correctly.

1. Load the Asterisk PBX.
   a. Download the Asterisk PBX virtual machine (VoIPonCD-appliance) from *http://www.voiponcd.com/downloads.php*.
   b. Download VMware Player from *http://www.vmware.com/products/free_virtualization.html*.
   c. Unzip *VoIP-appliance.zip* onto your hard drive.
   d. Using VMware Player, load VoIPonCD.
2. Back up *iax.conf*, *sip.conf*, and *extensions.conf* on the Asterisk PBX system with the following commands:

```
$ cp /etc/asterisk/extensions.conf /etc/asterisk/extensions.original.conf
$ cp /etc/asterisk/sip.conf /etc/asterisk/sip.original.conf
$ cp /etc/asterisk/iax.conf /etc/asterisk/iax.original.conf
```

3. Configure the Asterisk PBX system.
   a. Download *iax.conf*, *sip.conf*, and *extensions.conf* from *http://labs.isecpartners.com/HackingVoIP/HackingVoIP.html*.
   b. Copy all three files to */etc/asterisk*, overwriting the originals.
4. Restart the Asterisk PBX system with **`/etc/init.d/asterisk restart`**.
5. Download the SIP client X-Lite from *http://www.xten.com/index.php?menu=download* and the IAX client iaxComm from *http://iaxclient.sourceforge.net/iaxcomm/*.

Done! You now have a lab setting for this chapter.

## VoIP Phishing

Phishing is nothing new to most computer users, as messages for Viagra, stock tips, or just a note from their favorite friend in Nigeria is received almost every day. Furthermore, anyone who owns a fax machine can also fall victim to a form of phishing. Who hasn't received unsolicited advertisements by fax (although this was made illegal by the Junk Fax Prevention Act of 2005)?

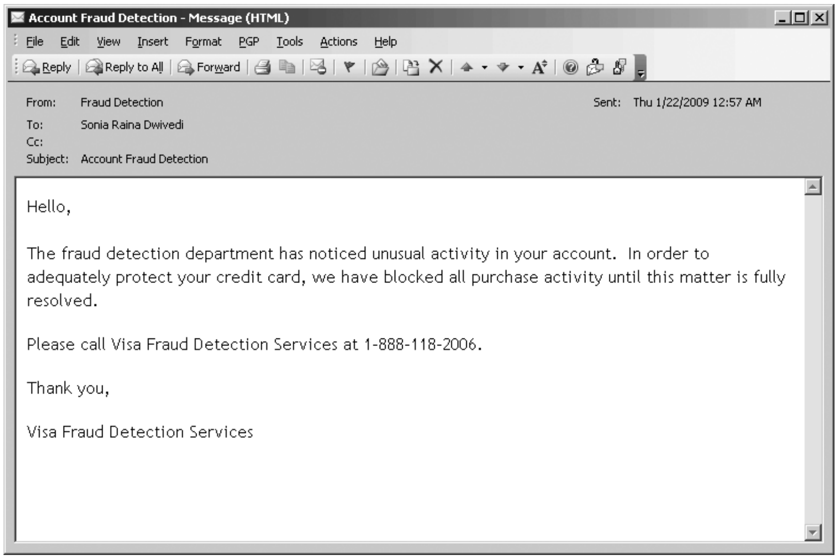
Because of the success of phishers and the amount of money they "earn" for doing almost nothing, phishing is big business, and it's getting larger. In fact, email phishing is just another form of the junk mail and advertisements received in physical mailboxes every day. For anyone who owns a home, receiving two or three letters a day from mortgage companies offering an "unbelievable" interest rate is almost standard.

VoIP phishing applies an old concept to a new technology. In most phishing emails, the target is asked to click a link, and doing so takes them to a bogus website that appears to be the legitimate one. For example, the user can be sent to a page that looks like the PayPal site but is actually a website controlled by an attacker. The bogus website will then ask the user for some type of information, such as a username, password, or some other user-specific information. Once attackers capture this information, they can then control the user's account without the user's knowledge. They are free to transfer money, trade stocks, or even sell users' social security information.

### *Spreading the Message*

VoIP phishing, also known as *vishing*, takes the same concept as email phishing but replaces the fake website with a fake phone number or even phone destination. For example, email phishing attacks may ask you to go to *www.visa.com* to conduct business concerning your Visa credit card; however, while the text will show up as *www.visa.com*, the actual destination might be a malicious website controlled by an attacker: *123.234.254.253/steal/money/from/people.html*. In VoIP phishing, attackers provide not the link to a malicious website but a legitimate-looking phone number, such as an 800, 888, or 866 number of the attackers' devising. Furthermore, to increase the appearance of validity with phone number buy-in services, attackers can attempt to buy a 800/888/866 number near the phone number block of the bank/institution they wish to impersonate. Given a direction or request to call an 800, 888, or 866 number, the end user may be more likely to trust it and make the telephone call. See Figure 7-1 for an example.

In addition to listing a phone number, attackers can be more sophisticated and add a malicious VoIP call icon to the email message. For example, many VoIP clients, such as Skype, allow icons to be placed in email messages or websites to initiate outgoing VoIP calls. Furthermore, the VoIP call icon can contain the logo of the company the attacker wishes to impersonate. Once the user clicks the logo, he will automatically call the number controlled by the attacker while believing that he is really calling the actual number of his credit card company. See Figure 7-2.


Account Fraud Detection - Message (HTML)
File Edit View Insert Format PGP Tools Actions Help
Reply | Reply to All | Forward

From: Fraud Detection
Sent: Thu 1/22/2009 12:57 AM
To: Sonia Raina Dwivedi
Cc:
Subject: Account Fraud Detection

Hello,

The fraud detection department has noticed unusual activity in your account. In order to adequately protect your credit card, we have blocked all purchase activity until this matter is fully resolved.

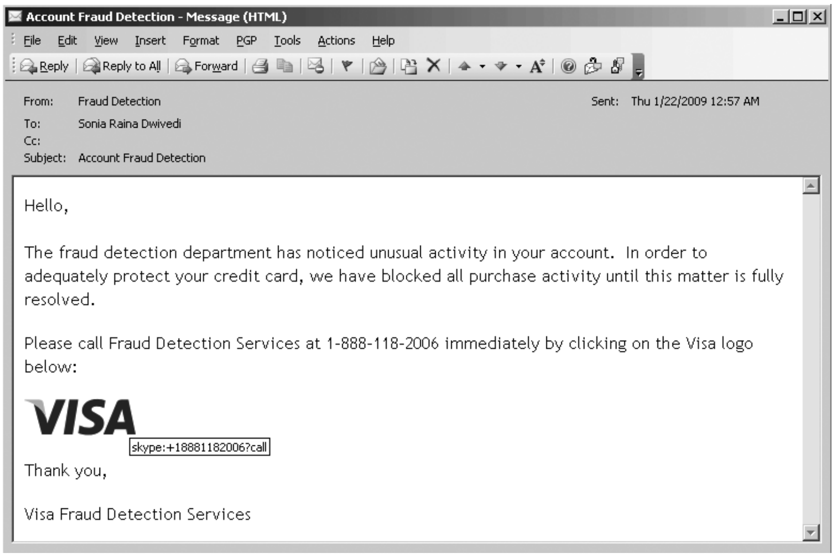
Please call Visa Fraud Detection Services at 1-888-118-2006.

Thank you,

Visa Fraud Detection Services

*Figure 7-1: VoIP phishing email*

Notice that the message shown in Figure 7-2 contains a recognizable and seemingly trustworthy company logo, such as Visa's, as well as text that says "Call Fraud Detection Services immediately." A user who clicks the logo will automatically call a number of the attacker's choice, which, obviously, is not actually Visa's. The exploit can occur with any VoIP client; however, this particular example has been customized for Skype. The reason an attacker would use Skype versus a more vulnerable VoIP client is the same reason why email phishers are fond of PayPal—there are more than 7 million registered users!


Account Fraud Detection - Message (HTML)
File Edit View Insert Format PGP Tools Actions Help
Reply | Reply to All | Forward
VISA

From: Fraud Detection
Sent: Thu 1/22/2009 12:57 AM
To: Sonia Raina Dwivedi
Cc:
Subject: Account Fraud Detection

Hello,

The fraud detection department has noticed unusual activity in your account. In order to adequately protect your credit card, we have blocked all purchase activity until this matter is fully resolved.

Please call Fraud Detection Services at 1-888-118-2006 immediately by clicking on the Visa logo below:

skype:+18881182006?call

Thank you,

Visa Fraud Detection Services

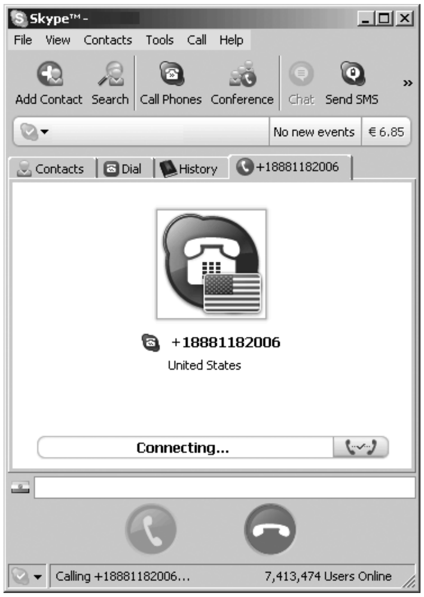
*Figure 7-2: VoIP phishing email with malicious VoIP call icon*

Among 7 million registered Skype users, one of them is bound to click that trusted icon and make the dangerous call. The HTML code for the malicious VoIP icon in Figure 7-2 is shown here:

```
<a href="skype:+18881182006?call">
<img src="http://attackers.ip.address/visa.jpg" style="border: none;"/>
</a>
```

Once the HTML file has been saved, it can be inserted as a signature file in the phisher's email client (in Microsoft Outlook, this is as simple as selecting **Insert** ▸ **Signature** ▸ **Use this file as template** ▸ **Browse** ▸ ***VoIP.Phish.Visa.htm***). The phisher can send millions of emails, and each of them will have the malicious VoIP icon via the signature file.

In the sample code, notice that the first item in bold is the attacker's 888 number. Because end users typically don't memorize the phone numbers of their credit card company, it would be difficult for an average person to determine if it is correct or not without checking the card itself, which many people will find too bothersome to do (especially if the user is worried about her account and wants to call the number as soon as possible). The second item shown in bold is the location of the Visa icon, which has been hosted on a server controlled by the attacker. End users who click the logo will been be taken to a phone/voicemail box controlled by the attacker, as shown in Figure 7-3.



+18881182006
United States

Connecting...

Calling +18881182006... 7,413,474 Users Online

*Figure 7-3: Result of user's clicking VoIP call icon*

### Receiving the Calls

In either of the scenarios just described, listing a phone number or providing a malicious VoIP call link, once the user makes the call, he will most likely enter a voicemail system that sounds exactly like the system of the intended target (the bank or credit card institution). After the user is prompted to enter his credit card number, PIN, and mother's maiden name for "verification" purposes by the automated system controlled by the attacker, the attacker has successfully carried out a VoIP phishing attack.

The attacker needs to ensure that when the user arrives at the bogus destination, the voice answer system, such as the IVR, resembles very closely the real destination's voice answer system. For example, every phish site for Visa, MasterCard, PayPal, Bank of America, Charles Schwab, Fidelity, or any other financial institution closely mirrors the real website. If a user went to a PayPal site and saw something remotely different, such as a different login page, misspelling, or just a different sequence of events to access her information, she might be tipped off that the site is bogus.

Similarly, VoIP phishers must ensure that the sequence of events, tone of voice, and prompts by the automated voice message service closely mirror those of the legitimate one. The bad news about this task it that it is fairly easy to accomplish. The Asterisk PBX is able to provide IVR services for users, and attackers can use this feature to create their own IVR system, ensure that it mirrors the "real" automated environment, and use it to answer calls. Asterisk is also able to auto-answer a phone number and provide an automated computer-generated voice in a variety of different tones. Furthermore, when users are prompted to enter their credit card number, PIN, or ZIP code, the attacker can set up an automated method to record this information with the Asterisk PBX, making the attack very simple and sustainable across a number of targets.

Now that we have shown how to create a VoIP phishing email easily, let's show how the automated call system can be set up. In this example, we will phish users, posing as a credit card company. Just as real credit card companies do, we will ask the user to enter his credit card information for verification purposes, including the credit card number and the user's ZIP code and four-digit PIN. Unlike real credit card companies, though, after attackers have gained the information they want, the call will disconnect, an event that will be blamed on high call volume.

Complete the following exercise to set up a mini–IVR-like system on the internal phone extension 867.4474 (To-Phish) using Asterisk PBX. The example here will simply show how Asterisk can be used to automatically answer phone calls; use Swift, a text-to-speech program for Asterisk, to speak to the user; ask the user for information such as a credit card number; and record that information and save it as a file.

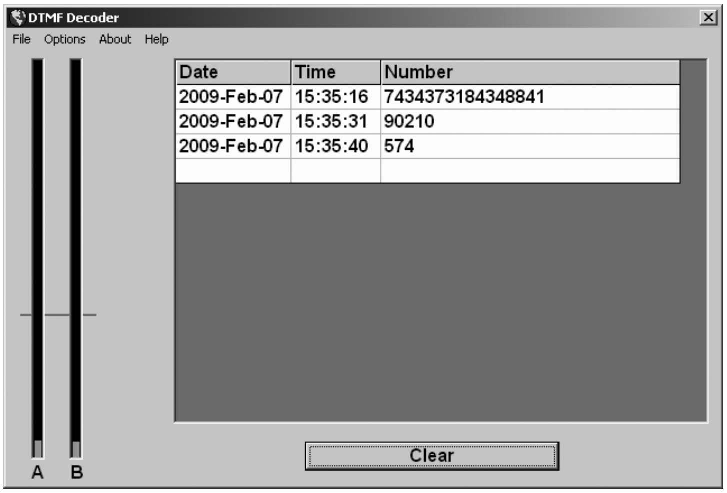
1. Log in to the Asterisk server.
2. Download Swift from *http://www.mezzo.net/asterisk/app_swift.html* and install it with the following commands:

   ```
   tar -xzr app_swif-release.tgz
   make install
   load app_swift.so
   ```

3. Once Swift has been installed correctly, add the following text to *extension.conf* (under the `[test]` realm):

   ```
    [test]
   exten => 8674474,1,Answer
   exten => 8674474,2,Wait(2)
   exten => 8674474,3,Monitor(wav,CreditCardPhish)
   exten => 8674474,4,Swift(Welcome to Visa Credit Card Services)
   exten => 8674474,5,Swift(Please enter your 16 digit credit card number)
   exten => 8674474,6,Swift(Please enter your zipcode)
   exten => 8674474,7,Swift(Please enter your 3-digit pin code)
   exten => 8674474,8,Swift(I'm sorry. Due to high call volume, the system
   cannot process your request. Please call again never)
   exten => 8674474,9,Swift(goodbye)
   exten => 8674474,10,Hangup
   ```

4. Next, using any phone registered to the Asterisk server, call 867.4474, as listed in the *extensions.conf* file.
5. When the system answers, type your credit card number, ZIP code, and three-digit PIN.
6. Once the information has been entered, Asterisk will record the information in two files located in */var/spool/asterisk/monitor*: *CreditCardPhish-in.wav* for the input sounds and *CreditCardPhish-out.wav* for the output sounds. The recording process is controlled by line 3, where the `Monitor` option is used to record the call. All sounds and key tones entered during the call will be recorded.
7. Once users have completed their calls, log in to the Asterisk server and copy all the recordings to a Windows operating system.
8. Convert the key tones recorded in the *.wav* files to actual text, numbers, or symbols.
   a. On the Windows operating system, download DTMF from *http://www.polar-electric.com/DTMF/Index.html.* DTMF is a tool that takes telephone audio key tones and displays them as the text, numbers, or symbols they represent.
   b. Open DTMF and play the *.wav* file recordings (*CreditCardPhish-in.wav* and *CreditCardPhish-out.wav*).
   c. Once the audio has been played and heard by DTMF, it will display the text, as shown in Figure 7-4.



| Date | Time | Number |
|---|---|---|
| 2009-Feb-07 | 15:35:16 | 7434373184348841 |
| 2009-Feb-07 | 15:35:31 | 90210 |
| 2009-Feb-07 | 15:35:40 | 574 |

*Figure 7-4: DTMF converts telephone key tones to text.*

Done! After sending the VoIP phishing email, the attacker has recorded the information entered by the victim.

## Making Free Calls

Making free calls from a PC to any landline or mobile phone in the United States or the United Kingdom is not really a security attack, but it is a nice little perk that will enable several other attacks in this chapter. For a few years, the major VoIP soft phones have provided free PC-to-PC calling but charge for calls from PCs to landlines and mobile phones, such as SkypeOut. Using Asterisk PBX, the X-Lite soft client, and VoIPBuster, free calls from a PC to a landline phone are now possible (but only for US or UK phone numbers). Here's how you set it up:

1. Create a VOIP account with VoIPBuster (*http://www.voipbuster.com/*), download the VoIPBuster client, and create a username and password that will be used in SIP session setup.
2. Once an account with VoIPBuster has been set up, log in to the Asterisk server and change directories to the Asterisk folder with **`cd /etc/asterisk`**.
3. Open the *sip.conf* file in */etc/asterisk* and add the following items at the end of the file. Make sure you replace the items in bold with your VoIPBuster username and password.

```
[voipbuster]
type=peer
host=sip.voipbuster.com
context=test
username=USERNAME
secret=PASSWORD
```

4. Open the *extensions.conf* file in */etc/asterisk* and add the following items in the test realm ([test]). Make sure you replace the items in italic with the number you want to call via your SIP client. Our example will be calling the number 415.118.2006.

```
[test]
exten => 100,Dial,(SIP/Sonia)
exten => 101,Dial,(SIP/Raina)
exten => 14151182006,Dial,(SIP/14151182006@voipbuster)
```

5. Using X-Lite or your favorite VoIP SIP client, point your VoIP soft phone to the Asterisk server. If using X-Lite, complete the following steps:
   a. Navigate to **SIP Account Settings**.
   b. Select **Properties**.
   c. Select the **Account** tab and enter your VoIPBuster username, VoIPBuster password, and domain (IP address of the Asterisk server).
6. Select **OK** and **Close**.

Done! By dialing 14151182006 on the X-Lite VoIP soft phone on your PC, you will make a call from the Asterisk PBX on your local network to VoIPBuster, which will then route the call to the landline or mobile phone you have chosen. Also, this allows the use of Asterisk for internal PC-to-PC calls as well, such as extensions 100 and 101 in *extensions.conf*, which are local VoIP client on the internal network.

It should be noted that neither Asterisk nor X-Lite must be used with VoIPBuster, because it also has a thick client that can make free phone calls for you; however, if you have an Asterisk PBX system for your internal calling, it is nice that you can use the same PBX for both internal VoIP calls as well as external calls. In order to use VoIPBuster directly for external calls, simply download its client and use its client interface.

## Caller ID Spoofing

Caller ID spoofing does exactly what its name implies: It changes the appearance of the source phone number of a telephone call. Caller ID spoofing can be innocent enough, allowing the kids who grew up with *69 to finally make phone calls and not feel bad about getting scared and hanging up at the last second; however, it can have many malicious applications as well. For example, the phone number of your bank can be spoofed, leading to another form of phishing attacks. Spoofing a bank number could allow attackers to call the phone number of everyone in the phone book and impersonate a trusted financial institution. Caller ID spoofing can also force someone to answer a call from someone he or she has been trying to avoid.

The reason Caller ID spoofing is possible is that implicit trust is placed on the source entity (the caller) during a phone call. For example, when a phone call is made, the source device, such as a VoIP soft phone, will send its source phone number to the destination as part of the data packet. Similar to how source IP addresses can be changed in TCP/IP headers, the source phone number can be changed by the outgoing device in a TCP/IP VoIP packet. In traditional phones, such as landlines or mobile devices, no user interface/option allows for this ability (for good reason); however, in the computer world, this is as simple as making a few edits to your soft phone/VoIP packet and placing the call. Spoofing values in TCP/IP packets is nothing new and is simply carried over to VoIP data packets.

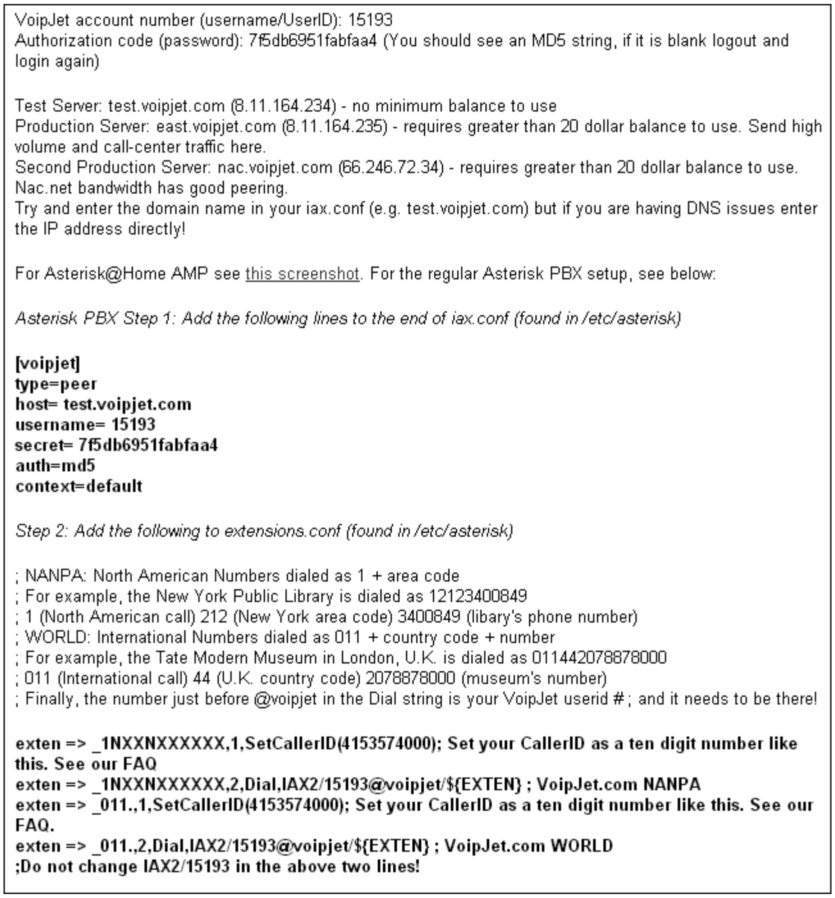
There are many ways to spoof Caller ID, including specialized calling cards, online calling services, or simply downloading specific software. A quick Internet search will lead to many methods for spoofing Caller ID; we are going to show four specific examples. The first example, which is the simplest (five quick steps), uses IAX with an IAX client and VoIPJet (an IAX VoIP provider). For those who prefer SIP clients, the second example uses a SIP client, such as X-Lite, an Asterisk server, and VoIPJet. The third example uses an online service. Finally, the fourth example shows how to perform Caller ID spoofing on an internal VoIP network, such as a Cisco or Avaya hard phone with Asterisk. It should be noted that spoofing your Caller ID is now defined as pre-texting, which is against the law and carries severe penalties (as noted by the 2006 Hewlett-Packard case).

### Example 1

As noted previously, the reason Caller ID spoofing works with iaxComm and VoIPJet is that the information provided by the calling entity is trusted. iaxComm offers the ability to change one's Caller ID number, as noted in step 2 in the next exercise. Because VoIPJet is a VoIP provider, it is taking information from a soft phone and converting that information to a PBX system for landline destinations. Because the soft phone (iaxComm) is not connecting directly to a PBX system, VoIPJet has no choice but simply to trust the information it receives in the TCP/IP VoIP packets. In this case, iaxComm is modifying the information before it is sent over the network, forcing VoIPJet and the final destination to display the spoofed number.

For this spoofing example, we will need to set up a VoIPJet account to spoof our Caller ID and an IAX client, such as iaxComm.

1. Download iaxComm from *http://iaxclient.sourceforge.net/iaxcomm/*.
2. Create a VoIPJet account by visiting *http://www.voipjet.com/*. The account grants you 25 cents' worth of calls for free.
3. Once a VoIPJet account has been set up, you will see an option called **Click here to view instructions on setting up Asterisk to send calls to VoIPJet**. Select that option and note the information to be used, as shown in Figure 7-5.



VoipJet account number (username/UserID): 15193
Authorization code (password): 7f5db6951fabfaa4 (You should see an MD5 string, if it is blank logout and login again)

Test Server: test.voipjet.com (8.11.164.234) - no minimum balance to use
Production Server: east.voipjet.com (8.11.164.235) - requires greater than 20 dollar balance to use. Send high volume and call-center traffic here.
Second Production Server: nac.voipjet.com (66.246.72.34) - requires greater than 20 dollar balance to use. Nac.net bandwidth has good peering.
Try and enter the domain name in your iax.conf (e.g. test.voipjet.com) but if you are having DNS issues enter the IP address directly!

For Asterisk@Home AMP see this screenshot. For the regular Asterisk PBX setup, see below:

*Asterisk PBX Step 1: Add the following lines to the end of iax.conf (found in /etc/asterisk)*

```
[voipjet]
type=peer
host= test.voipjet.com
username= 15193
secret= 7f5db6951fabfaa4
auth=md5
context=default
```

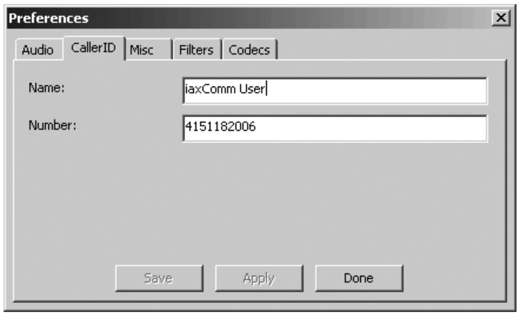
*Step 2: Add the following to extensions.conf (found in /etc/asterisk)*

```
; NANPA: North American Numbers dialed as 1 + area code
; For example, the New York Public Library is dialed as 12123400849
; 1 (North American call) 212 (New York area code) 3400849 (libary's phone number)
; WORLD: International Numbers dialed as 011 + country code + number
; For example, the Tate Modern Museum in London, U.K. is dialed as 011442078878000
; 011 (International call) 44 (U.K. country code) 2078878000 (museum's number)
; Finally, the number just before @voipjet in the Dial string is your VoipJet userid # ; and it needs to be there!

exten => _1NXXNXXXXXX,1,SetCallerID(4153574000); Set your CallerID as a ten digit number like
this. See our FAQ
exten => _1NXXNXXXXXX,2,Dial,IAX2/15193@voipjet/${EXTEN} ; VoipJet.com NANPA
exten => _011.,1,SetCallerID(4153574000); Set your CallerID as a ten digit number like this. See our
FAQ.
exten => _011.,2,Dial,IAX2/15193@voipjet/${EXTEN} ; VoipJet.com WORLD
;Do not change IAX2/15193 in the above two lines!
```

*Figure 7-5: VoIPJet account information*

4. Open iaxComm and with the following steps configure it to use VoIPJet:
   a. Select **Options** from the menu bar.
   b. Select **Preferences** and then the **CallerID** tab.
   c. On the **Number** line, enter the Caller ID number you wish to spoof from. See Figure 7-6. For this example, we will use 4151182006.



Name: iaxComm User
Number: 4151182006

*Figure 7-6: CallerID tab in iaxComm*

d. Select **Apply** ▸ **Save** ▸ **Done**. (Exit the menu by clicking the **X** in the upper right corner.)

e. Select **Options** from the menu bar.

f. Select **Accounts**.

g. Select **Add**.

h. Enter the VoIP information received from VoIPJet in Figure 7-5: Account Name (**`VoIPJet`**), Host (**`test.voipjet.com`**), Username (**`15193`**), Password (**`7f5db6951fabfaa4`**).

i. Select **Save**, exit the menu, and then select **Done**.

Done! You have now registered your iaxComm client to VoIPJet. The next step is to dial any ten-digit phone number, beginning with the number 1 (e.g., 14158675309). Type the number in the **Extension** text box on iaxComm. Once the call takes place, the Caller ID number set in the **Preferences** section of the client will appear on the remote phone.

### Example 2

In order to spoof Caller ID using a SIP client, you must use an Asterisk PBX system with the VoIPJet account. Complete the following steps to spoof Caller ID by connecting the X-Lite SIP client to an Asterisk server and connecting the Asterisk server to VoIPJet.

1. Create a VoIPJet account by visiting *http://www.voipjet.com/*. The account grants you 25 cents' worth of calls for free.
2. Once an account with VoIPJet has been set up, you will see an option called **Click here to view instructions on setting up Asterisk to send calls to VoipJet**. Select that option and note the information to be used in the *iax.conf* and *extensions.conf* files, as shown previously in Figure 7-5.
3. Change directories to the Asterisk folder with the command **`cd /etc/asterisk`**.
4. Copy the IAX information given to you by VoIPJet directly into the *iax.conf* file. Notice that the information from VoIPJet, shown in Figure 7-5, mirrors the items added to the *iax.conf* file. Also, you will probably have to log out and then log back in to get the MD5 checksum needed on the `secret=` line. Here is an example of the information entered into *iax.conf*:

```
[voipjet]
type=peer
host= test.voipjet.com
username= 15193
secret= 7f5db6951fabfaa4
auth=md5
context=default
```

5. Copy the extension information given to you by VoIPJet directly into the *extensions.conf* file under the test realm (`[test]`). Unlike *iax.conf*, you don't need everything given to you by VoIPJet to complete the proof of concept in this example, just the lines shown below. Additionally, make sure you replace the items in bold with the phone number you wish to spoof from. For this example, we will be spoofing from 415.118.2006 to any 10-digit number that is dialed with a prefix of 1 (as shown by the `_1NXXNXXXXXX` line):

```
exten => _1NXXNXXXXXX,1,SetCallerID(4151182006)
exten => _1NXXNXXXXXX,2,Dial,IAX2/15193@voipjet/${EXTEN}
exten => _011.,1,SetCallerID(4151182006)
exten => _011.,2,Dial,IAX2/15193@voipjet/${EXTEN}
```

6. Using a SIP client, such as X-Lite, between your client and the Asterisk server requires an extra step. Open the *sip.conf* file and enter the following information, which will specify a SIP client to register with your Asterisk server:

```
[Sonia]
type=friend
host=dynamic
username=Sonia
secret= 123voiptest
context=default
```

7. Using X-Lite or your favorite VoIP SIP client, point your VoIP soft phone to the Asterisk server. If using X-Lite, complete the following steps:
   a. Navigate to **SIP Account Settings**.
   b. Select **Properties**.
   c. Select the **Account** tab and enter the Username (**`Sonia`**), Password (**`123voiptest`**), and Domain (***`IP address of the Asterisk server`***).
   d. Select **OK** and **Close**.

Done! You have now registered your Asterisk server to VoIPJet (using IAX) and your X-Lite client to the Asterisk server (using SIP). The next step is to dial any 10-digit phone number, beginning with the number 1 (e.g., 14158675309), on the X-Lite SIP client. The Caller ID information will be retrieved from *extensions.conf* (item in bold in the step 5) on the Asterisk server. Once the call takes place, the number after the `SetCallerID` line will appear on the remote phone.

### Example 3

The next method of spoofing your Caller ID is quite simple. As stated previously, there are many methods of spoofing a Caller ID, including the use of services provided on websites like *http://www.fakecaller.com/*. By the time this book is released, this link might no longer work, but there are probably ten more just like it. Regardless, while fakecaller.com allows you to spoof Caller ID, it allows you only to insert text to repeat back to the user. Actual conversations cannot take place using this service; however, the proof of concept is demonstrated well with the website.

Complete the following steps to spoof your Caller ID with fakecaller.com. Note that the service sends call information to a third party.

1. Visit *http://www.fakecaller.com/*.
2. Type the number you wish to call in the **Number to dial** text box.
3. Type the spoofed number, such as 4158675309, in the **Number to display on Caller ID** text box.
4. Type the name, such as *HackmeAmadeus*, in the **Name on Caller ID** text box. Note that this may not be displayed.
5. Select the type of **Voice**, male or female and age, for the call.
6. Select the message you wish to repeat when the target picks up the phone, such as "I'm Rick James, bitch!"
7. Select **Make the call**.

Done! In a few seconds, the number shown in step 2 will receive a call, appearing from the number on step 3. The text shown in step 6 will be spoken to the user.

### Example 4

The next method of spoofing your Caller ID targets an internal network using VoIP with SIP. For example, you may want to spoof your Caller ID with outbound calls not to landlines or mobile phones but rather to your cubicle-mate sitting right next to you. If the environment uses Cisco or Avaya hard phones that are SIP-enabled, spoofing the Caller ID on an internal VoIP network is also possible.

Complete the following steps to spoof your Caller ID on your internal VoIP network. The targeted phone extension is 2222, the real phone extension is 1111, and the spoofed phone extension is 1108. Asterisk will be used to mimic the setup between the hard phone sitting on your desk and the Cisco CallManager or Avaya Call Server. A soft client will also be used to connect to the Asterisk server to execute the spoofing.

1. Unplug the Ethernet jack from the hard phone on your desk.
2. On your Asterisk server, open the *sip.conf* file and enter the username and password information for your real phone extension. This will enable the Asterisk server to register to Cisco CallManager or Avaya Call Server, instead of to the hard phone on your desk. Note that the spoofer's real phone extension, pass code, and the spoofed number all need to be

entered correctly, as shown in the bold text. For example, if the VoIP phone on the desk has the extension number of 1111 and the passcode is 1111, then those values must enter in this file, as well as the extension you wish to spoof from (in the `callerid` line):

```
 [Spoof]
type=friend
host=dynamic
username=1111
secret=1111
context=default
callerid=1108
```

3. On your Asterisk server, open the *sip.conf* file and enter the following information, which will enable a SIP client (such as X-Lite) to register with your Asterisk server:

```
[Sonia]
type=friend
host=dynamic
username=Sonia
secret=123voiptest
context=default
```

4. Edit `extension` in the *extensions.conf* file and add the following information under the test realm (`[test]`). Notice that when extension 2222 is dialed, the Caller ID value will be set to 1108, as noted in the first line here.

```
exten => 2222,1,SetCallerID(4151182006)
exten => 2222,2,Dial,SIP/1112@Spoof/${EXTEN}
```

5. Using X-Lite or your favorite VoIP SIP client, point your VoIP soft phone to the Asterisk server. If you're using X-Lite, complete the following steps:
   a. Navigate to **SIP Account Settings**.
   b. Select **Properties**.
   c. Select the **Account** tab and enter the Username (**`Sonia`**), Password (**`123voiptest`**), and Domain (***`IP address of the Asterisk server`***).
   d. Select **OK** and **Close**.

Done! You have now registered your Asterisk server to Cisco CallManager or Avaya Call Server and your X-Lite client to the Asterisk server (using SIP). The next step is to dial the four-digit phone extension of 2222 on the X-Lite SIP client. The Caller ID information will be retrieved from *extensions.conf* (items in bold in steps 2 and 3) from the Asterisk server. Once the call has been placed, the number after the `CallerID` and/or the `SetCallerID` line will appear on the remote phone.

As you can see, Caller ID spoofing is quite simple, no matter which of the four demonstrated methods is used. The ability to spoof Caller ID has more impact than a practical joke or to subvert *69, however. For example, credit card companies often send new credit cards in the mail and require users to use their home phone number to activate the card. An angry neighbor, perhaps one who has cleaned up after the neighbor's cat or is tired of listening to dogs barking all night, can steal her neighbor's mail and activate a credit card by spoofing the Caller ID she is calling from.

Another attack involves listening to someone else's voicemail from his mobile phone. In order to listen to voicemail on their mobile phones, most users select the phone's voicemail icon. This action actually calls their own number, which puts them into the voicemail system. Often, users do not use a password on their account, thinking that the voicemail box can be accessed only by someone holding the physical phone. If the user has made this mistake, an attacker can spoof the user's Caller ID, call the mobile phone, and get direct access to the target's voicemail system without being prompted for a password.

## Anonymous Eavesdropping and Call Redirection

Man-in-the-middle attacks have plagued networks for many years. Tools from Dsniff/fragrouter to Cain & Abel help show how network communication methods are not secure. Using the same model, telephone communication via VoIP can fall into the same problem space. While Layer 2 man-in-the-middle attacks using ARP packets are by far the easiest way to eavesdrop on a call, access to the correct network space is required. Unfortunately, there are a few ways to eavesdrop without using ARP poisoning—using common phishing attacks in combination with call redirection.

The first kind of this attack is a targeted attack, involving Caller ID spoofing. The attacker essentially creates a three-way call between the credit card company and the target, staying on the line as a passive listener and recording the content. The attacker spoofs his Caller ID number as the one listed on the back of a credit card or on the credit card company's website. Once the number has been spoofed, the attacker calls the target on one connection. The target, believing that the call is coming from the credit card company, answers the call thinking it is a trusted entity. Once the target answers the call, the attacker can send an automated computer voice informing him of supposed unusual activity on his account and asking him to verify his information. While the message is playing to the target on one connection, the attacker opens another connection with the real credit card company. Once the credit card company answers the call, the attacker can then connect (three-way call or conference) both the target and credit card company while remaining on the line. Before doing anything else, most credit card companies use an automated computer voice to verify credit card numbers. Once the conference has been enabled, the target is then asked by the real credit card company to verify his information by typing or speaking his credit card number, PIN, and the card's expiration date. The attacker secretly remains on the call and records all the information.

Complete the following steps to perform this attack using X-Lite.

1. Instead of repeating steps, complete steps 1 thru 8 from “Example 2” on page 142; however, in step 5, replace 4151182006 with the number on the back of your credit card.
2. Open X-Lite and select the **AC** button, which should then turn yellow and show text that states **Auto-conference enabled**. This button will automatically create a conference between the two lines used by X-Lite.
3. Using line 1 on X-Lite, call the target. This will be using the Caller ID value from step 5 in the earlier section. When the target answers the phone, play a pre-recorded audio file that states, “This is an automated message. We have noticed unusual activity in your account. Please remain on the line to verify your information.” A poor man’s approach to recording the message is to use Windows Narrator, which is described in detail in the next section of this chapter.
4. Using line 2 on X-Lite, call the credit card company. Once the credit card company picks up the call, X-Lite immediately conferences all the lines together (the Auto-Conference option was enabled in step 2). The target will then be listening to the real credit card company and be prompted for verification information.
5. On X-Lite, click the **Record** button. All information from the target to the credit card company will now be recorded by the attacker and can be used to compromise the target’s account.

The second method of performing this attack takes not a targeted approach but a wider approach for its target. This attack was first mentioned by Jay Shulman at Black Hat 2006. The attacker sends a phishing email similar to the one shown previously in this chapter. When an end user calls the number shown in the phishing email, the attacker opens a second connection to the actual credit card company. Instead of answering the call directly, the attacker connects the end user with the real credit card company; however, the attacker remains on the line. When the user is asked by the credit card company to verify her information by entering or speaking her credit card number, PIN, and the card’s expiration date, the attacker, having remained on the call, captures the information.

## Spam Over Internet Telephony

Remember the old days when you could just select and delete all the spam messages in your inbox? How about when you could just go to your Junk email folder and simply delete its contents with just one click? Now think of having more than a hundred voicemail messages (or the maximum capacity of your voicemail box) on your mobile phone. Could you delete all of them with just a few clicks on your phone? Furthermore, what would you do when legitimate users who are trying to leave you a message are not able to leave you one, such as “My flight from O’Hare got canceled because someone saw a cloud 400 miles away from the airport, so pick me up from SJC at 9 PM instead of SFO at 5 PM"? How disruptive would these issues be to your life compared with the 300 email messages from the Crown Prince of Nigeria?

The idea of SPIT is nothing new, as telemarketers already use automated technology to call home users to sell products and goods. Furthermore, many organizations will provide this service for a small charge, such as *http://www.call-em-all.com/*, which allows a spammer to send more than 1,000 people a pre-recorded voicemail for under $100. However, with VoIP, not only can hundreds of pre-recorded messages be sent out to any phone or voicemail system in the country, these messages can also be free and hard to trace, which makes the National Do Not Call Registry a lesser mitigation strategy. While everyone loves their favorite Republican, Democrat, or independent political candidate calling them on Election Day, would they enjoy receiving those messages every day from an anonymous seller?

In actuality, an anonymous spammer may be better than what could be done with the true abuse of SPIT. For financial gain, an attacker could mimic the automated fraud detection service that credit card companies often use. When the credit card company detects an unusual charge, an automated voice call executes to the phone number listed for the account holder. The message usually tells the account holder that some aberrant activity has been detected and he should call the credit card company right away. However, an attacker can create a similar fraud detection voice call but ask the person to call a number of her choice. For example, the attacker's automated message could be:

> "Hello, this is an automated message from Visa Fraud Detection Services. We have noticed unusual activity in your account and ask that you call 1.800.118.2006 immediately to resolve this issue. This message will now repeat.
>
> Hello, this is an automated message from Visa Fraud Detection Services. We have noticed unusual activity in your account and ask that you call 1.800.118.2006 immediately to resolve this issue. Thank you."

The following sections show a few ways to perform SPIT.

### SPIT and the City

The ability to send pre-recorded calls over VoIP is quite easy. With VoIP infrastructure, standard messaging format can be used. Open PBX systems, such as Asterisk, can be used to blast pre-recorded messages to individual phone numbers in mass quantity. Asterisk allows users to make a single call file and send it manually. The call file can then be repeatedly sent to several different phone numbers over a short period of time.

Complete the following steps to send spam messages over VoIP infrastructure:

1. Record the spam message. This can be accomplished using a variety of methods; for this proof of concept, we will use a pre-recorded message in *.mp3* format. Using any voice recorder, record the spam message and save it to a *.mp3* file (e.g., *SPAM.mp3*).

2. After the file has been saved, load it to the following directory on your Asterisk server: */var/lib/asterisk/mohmp3/SPAM.mp3*. If you don't have time to record a spam message, use any music *.mp3* file for this example.
3. Create an extension sequence to call the target and play the *.mp3* file when the phone is answered.
   a. Edit */etc/asterisk/extensions.conf* by adding the following lines under the test realm `[test]`, which will create an extension and reference the *SPAM.mp3* message recorded:

   ```
   [test]
   exten => s,1,Answer
   exten => s,2,MP3Player(/var/lib/asterisk/mohmp3/SPAM.mp3)
   exten => s,3,Hangup
   ```

4. To complete the proof of concept, we will be using the free account created earlier with VoIPBuster. Please complete that section of this chapter before proceeding to the next step. In summary, be sure to visit *http://www.voipbuster.com/*, create an account, and add the following information to your *sip.conf* file (where ***`USERNAME`*** and ***`PASSWORD`*** are the information your provided to VoIPBuster):

   ```
   [voipbuster]
   type=peer
   host=sip.voipbuster.com
   context=test
   username=USERNAME
   secret=PASSWORD
   ```

5. Create the call file itself. The call file will be used to manually send a pre-recorded message using Asterisk.
   a. Change directories to */var/spool/asterisk/tmp*.
   b. Open a text editor, such as vi, and create a call file called *SPAM.Test.call*.

      The first line will list the targeted phone number to send your spam to, which is indicated by the channel information. The channel information will use the VoIPBuster account created earlier. For example, the first line will be listed as `SIP/1-xxx-xxx-xxxx@voipbuster`, where *`xxx-xxx-xxxx`* should be replaced by the 10-digit phone number of the targeted number (e.g., `SIP/14151182006@voipbuster`). If the targeted phone is 415.118.2006, the channel line will look like the following:

   ```
   Channel: SIP/14151182006@voipbuster
   ```

c. Add the rest of the items below, which include the max retries, wait time, and priority, to make the call file work:

```
MaxRetries: 5
RetryTime: 300
WaitTime: 45
Context: test
Extension: s
Priority: 1
```

6. To test the call file to ensure that everything worked, restart the Asterisk server, which ensures that the updated *extensions.conf* file has been loaded:

```
/etc/init.d/asterisk/ restart
```

7. Copy the newly created call file to Asterisk's outgoing folder. Asterisk checks this folder periodically to send outbound calls. Within a few moments of your moving the file, Asterisk will call 415.118.2006 and play the pre-recorded *.mp3* message to the user when she answers the phone:

```
mv /var/spool/asterisk/tmp/SPAM.Test.call /var/spool/asterisk/outgoing
```

Done! You have now sent the *SPAM.mp3* file to your targeted user.

If the call was made successfully, then the real nastiness can begin. As you may have noticed, there is nothing unique about the call file except the phone number listed on the first line. A simple script can be created that changes the 10-digit phone number of the target to any value the spammer wishes. Furthermore, the script can be written in a way to create a unique call file for each number between 415.000.0000 and 415.999.9999. Once these call files have been moved to the outgoing folder and sent by Asterisk, it can then send the pre-recorded *SPAM.mp3* file to all the phone numbers in San Francisco (415 is the area code for San Francisco). Furthermore, the attacker could use his VoIPJet account instead of VoIPBuster and set the Caller ID value to something trusted, such as the local fire department number. This would make the calls appear to be originating from a trusted source, allowing the spammer to SPIT on all the phones in a major city.

### Lightweight SPIT with Skype/Google Talk

Another way to SPIT on users is to use Skype, Google Talk, or the handful of other VoIP clients that support the voicemail feature. Skype and Google Talk offer a feature that allows a voicemail message to be sent to other Skype/Google Talk users. Similar to sending advertisement email to users, this feature can be abused by Skype/Google Talk users. The feature allows a voicemail to be sent to any contact in your contact list. Unlike bulk email, which allows a single email to be sent to several thousands users, Skype and Google Talk do not support bulk voicemail. An attacker would have to send a voicemail to each target one by one, thus limiting the feasibility of this type of SPIT activity given that volume is a big factor when one is trying to advertise products to users via spam. Regardless, to SPIT on Skype/Google Talk users, a phisher can send a voicemail that sounds as if it is from a legitimate credit card company. In fact, with PayPal being a high-profile target of email phishers, and the fact that eBay owns both PayPal and Skype, a voicemail from “PayPal” to a Skype account citing unauthorized activity and requesting immediate action is probably the next wave of attacks. A sample Skype phish attempt may have the following speech:

> “Dear Customer: We have noticed unusual activity in your account and ask that you call 1.800.118.2006 immediately to resolve this issue. The activity in question seems to abusing both your PayPal and eBay accounts at this time. Thank you, PayPal Trust and Safety.”

Carry out the following steps to complete a proof of concept of SPIT with Skype:

1. Download Skype from *http://www.skype.com/* or Google Talk from *http://www.google.com/talk/*.
2. Acquire Skype Voicemail, which can be purchased for US$6.00, or Google Talk Voicemail, which is free.
3. Open Notepad and copy the previous phishing text into a new file.
4. Open Windows Sound Recorder (**Start ▸ Programs ▸ Accessories ▸ Sound Recorder**).
5. Open Windows Narrator (**Start ▸ Programs ▸ Accessibility ▸ Narrator**).
6. Click Sound Recorder’s **Record** button.
7. When Narrator begins to speak words, give the Notepad file the focus. This step records the phishing text into a computer voice, mimicking the automated calls made by credit card companies.
8. Click Sound Recorder’s **Stop** button after Narrator finishes the phishing text. Save the file as *SPIT.wav*.
9. To use Skype and/or Google Talk to SPIT:
   a. Right-click the user to whom you wish to send a SPIT voicemail.
   b. Wait for the user’s voicemail box to start recording.
   c. Play the *SPIT.wav* file from your machine.

Done! You have just sent a spam voicemail mail using computer-automated text to a targeted VoIP user.

As you may have noticed, the example shows an unsophisticated method of spamming VoIP users. As with every other section of this chapter, the proof of concept is to show how easily SPIT can be performed, but not to show the recipe for disaster. A real SPIT methodology would improve the previous example by using a better computer-automated voice (such as one produced by Asterisk Festival) and sending bulk voicemails with a single audio file (using scripting or some other automated delivery method).

## Summary

As you have no doubt noticed from this chapter, many unconventional attacks are possible with VoIP infrastructure. The descriptions of many of these attacks in this chapter have shown the most severe cases, which allow any user to download the Asterisk PBX system and within a few moments play games on trusted devices in our homes and offices (landlines and mobile phones, as well as VoIP phones). VoIP technology has a long way to go in terms of trust boundaries and security guarantees, because abuse of the system is not actively defended against or secured. History tells us that when abuse is allowed and can lead to financial gain, such as with email technologies, attackers will not hesitate to take advantage of the opportunity. Unfortunately for the rest of us, the trust of items we once felt very secure about can no longer be guaranteed, whether that is the Caller ID, an account representative from your credit card company, or simply a voicemail.