Phone System Testing
AND OTHER FUN TRICKS

Snide / Owen
@LinuxBlog
github.com/PhreakMe (Latest Slides & Code)
Mandatory Disclaimer

The opinions expressed in this presentation and on the following slides are solely those of the presenter. There is no guarantee on the accuracy or reliability of the information provided herein.

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

This is for educational purposes only
Introduction

- History / Evolution
- Anatomy
- How to test
- Issue Types
- Fun Stuff
About Me

Moved to US in 2000.

Presentations

Fun
How many of you remember your childhood home phone number?
So who uses Phones?

What industries?

Particularly interesting are:
    banking/finance
    Healthcare
    Insurance
    Utilities
    Government
    Military.
History

Sorry, Wrong number DC23

Exploding The Phone (Book) 2013.
History

The Sound of the Dialup: an Example Handshake

https://en.wikipedia.org/wiki/Dial-up_Internet_access
<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1996</td>
<td>ICQ, NetMeeting, SMS (UK)</td>
</tr>
<tr>
<td>1997</td>
<td>AIM</td>
</tr>
<tr>
<td>1998</td>
<td>Yahoo Messenger</td>
</tr>
<tr>
<td>1999</td>
<td>MSN Messenger &amp; Asterisk</td>
</tr>
<tr>
<td>2001</td>
<td>TeamSpeak &amp; MMS</td>
</tr>
<tr>
<td>2002</td>
<td>Yahoo Messenger Chat</td>
</tr>
<tr>
<td>2003</td>
<td>Skype Released - MySpace</td>
</tr>
<tr>
<td>2004</td>
<td>Facebook</td>
</tr>
<tr>
<td>2005</td>
<td>YouTube</td>
</tr>
<tr>
<td>2007</td>
<td>iPhone</td>
</tr>
</tbody>
</table>
Recent History

- Hangouts
- FB Messenger
- Signal
- Screen Sharing
- LiveStreaming
- WhatsApp
- SnapChat
- Kik
- etc etc.
PBX’s

Why do people run PBX’s?
• Reduce Costs
• Cheap Calling
• "Apps"
  • Voicemail
  • IVR’s
• Conferencing
• Directories
Basic Deployment

PBX

SoftPhone

SIP Phone

ATA

“Phone”
Common Deployment
Large
More Tech

- Call Monitoring
- Voicemail
- Transcribing
- Call center / Queue
- Ring Groups
- Call Backs
- Portals
- Reporting and Analytics

- Translations
- Voice
- Biometrics
- 2FA
- Mobile
- Forwarding
- BYOD
- Apps
- Softphones / Skype
DTMF

Dual Tone Multi Frequency

Can be easily generated

http://www.genave.com/dtmf.htm
Common Protocols

- SIP
- RTP
- XMPP
- IAX
Codecs

- G.711 - ITU-T
  - PCM
  - Alaw
  - Ulaw
- G.711.0
- G.711.1
- g.722
- GSM
How?

Step 1) Figure out what you’re testing
Testing

Scope
  Blackbox / Whitebox?

Info Gathering
Testing

Info Gathering

• OSINT
  • Grab Phone Numbers from Web / Directories.
  • Look for patterns

• Port Scans
• Shodan
• Use the Web
• Whois has information too!
Externally Testing

Testing Via POTS
- Regular Phone. Sit and press buttons
- Modems and AT commands
- Soft Phones
  - Any of the major ones
  - Ekiga, Twinkle ETC.
- Automatable / Scriptable
  - SipCLI
  - Sip.Js & JSSip
  - MJSip
- Use a PBX
My Testing Setup

OrangePi 2E

Decent Specs

Portable
Software

Armbian

Asterisk

Scripting Utilities

More on this Later!
Types of Issues 2017

A1: Injection
A2: Broken Authentication and Session Management
A3: Cross-Site Scripting (XSS)
A4: Broken Access Control
A5: Security Misconfiguration
A6: Sensitive Data Exposure
A7: Insufficient Attack Protection
A8: Cross-Site Request Forgery (CSRF)
A9: Using Components with Known Vulnerabilities
A10: Under protected APIs
A1: Injection

Injection Points: Web, Voice, SIP, DTMF

Result:
  XSS
  SQL
  Buffer Overflows
  Log Contamination
A2: Broken Authentication & Session Management

Mostly Authentication
Lack of SSL/TLS for SIP

https://wiki.asterisk.org/wiki/display/AST/Secure+Calling+Tutorial
A3: Cross-site Scripting
Somewhat covered by injection
A4: Broken Access Control

http://example.com/app/accountInfo?
acct=notmyacct

Given that example, this can be translated into a bad configuration.

Either Extensions or AGI Script / App
A5: Security Misconfiguration

- Pretty common
- SIP allowguest – Default = yes
- 4 Digit passwords for SIP Clients
- Conferencing
- Default passwords
- Weak Passwords
- Misconfigured Dial plans & AGI’s
A6: Sensitive Data Exposure

• Voicemail
• Conference Calls
• Information not available elsewhere
  • Similar to the User/Password combination enumeration
• Corp Directories
  • Full Names, E-Mails
  • Schedules, out of office
A7: Missing Function Level Access Control

- Caller ID Spoof
- User logs in, tries username / pass, fails tries another.
- Systems like voicemail that allow userid, password separate and prompt for username again is an issue
- Potential with misconfigurations, if put back into another context.
- Reasonable Use
A8: Cross-Site Request Forgery (CSRF)

• Vendors
• Web portals and configuration pages are often vulnerable
• In from a phone sense not directly applicable
A9: Components with Known Vulnerabilities
A9: Components with Known Vulnerabilities

- Cisco ATA 186 Analog Telephone Adapter - ... $110.00
  ServerSupply.com
  Free shipping

- Cisco ATA 186-1 I ATA 186 Analog Phone Adapter ...
  $69.99
  NetworkTigers

- Cisco Ata 186 Analog Telephone Adaptor $39.99
  eBay

Cisco ATA 186 Analog Telephone Adapter - Cisco
www.cisco.com › ... › Data Sheets and Literature › Data Sheets ▼
Apr 8, 2004 - The Cisco ATA 186 Analog Telephone Adaptor is a handset-to-Ethernet adaptor that turns...
A9: Components with Known Vulnerabilities
# A9: Components with Known Vulnerabilities

<table>
<thead>
<tr>
<th>TftpURL:</th>
<th>CfgInterval: 86400</th>
</tr>
</thead>
<tbody>
<tr>
<td>EncryptKey:</td>
<td>EncryptKeyEx: 0000000000000000000000000000000000000000000000000000000000000000</td>
</tr>
<tr>
<td>Dhcp: 0</td>
<td>StaticIP:</td>
</tr>
<tr>
<td>StaticRoute:</td>
<td>StaticNetMask:</td>
</tr>
<tr>
<td>UID0:</td>
<td>PWD0:</td>
</tr>
<tr>
<td>UID1:</td>
<td>PWD1:</td>
</tr>
<tr>
<td>GkOrProxy:</td>
<td>UseLoginID: 0</td>
</tr>
<tr>
<td>LoginID0:</td>
<td>LoginID1:</td>
</tr>
<tr>
<td>AltGk: 0</td>
<td>AltGkTimeOut: 0</td>
</tr>
<tr>
<td>SIPRegInterval:</td>
<td>MaxRedirect: 5</td>
</tr>
<tr>
<td>SIPRegOn: 1</td>
<td>NATIP: 0.0.0.0</td>
</tr>
<tr>
<td>SIPPort: 5060</td>
<td>MediaPort: 16384</td>
</tr>
<tr>
<td>OutBoundProxy:</td>
<td>NatServer: 0</td>
</tr>
<tr>
<td>NatTimer: 0x00000000</td>
<td>MsgRetryLimits: 0x00000000</td>
</tr>
<tr>
<td>SessionTimer: 0x00000000</td>
<td>SessionInterval: 1800</td>
</tr>
<tr>
<td>MinSessionInterval: 1800</td>
<td>DisplayName0: 0</td>
</tr>
<tr>
<td>DisplayName1: 0</td>
<td>LBRCodec: 0</td>
</tr>
<tr>
<td>AudioMode: 0x00140014</td>
<td>RxCodec: 1</td>
</tr>
<tr>
<td>TxCodec: 1</td>
<td>NumTxFrames: 2</td>
</tr>
<tr>
<td>CallFeatures: 0xffffffff</td>
<td>PaidFeatures: 0xffffffff</td>
</tr>
<tr>
<td>CallerIdMethod: 0x00019e60</td>
<td>FeatureTimer: 0x0000000000</td>
</tr>
<tr>
<td>FeatureTimer2: 0x0000000000</td>
<td>Polarity: 0x0000000000</td>
</tr>
</tbody>
</table>
A9: Components with Known Vulnerabilities

Unable to connect

Firefox can’t establish a connection to the server at

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer’s network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Try Again
# A9: Components with Known Vulnerabilities

## Table 1. End-of-Life Milestones and Dates for the Cisco ATA 186 Analog Telephone Adaptor

<table>
<thead>
<tr>
<th>Milestone</th>
<th>Definition</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-of-Life Announcement Date</td>
<td>The date the document that announces the end of sale and end of life of a product is distributed to the general public.</td>
<td>March 30, 2010</td>
</tr>
<tr>
<td>End-of-Sale Date</td>
<td>The last date to order the product through Cisco point-of-sale mechanisms. The product is no longer for sale after this date.</td>
<td>September 28, 2010</td>
</tr>
<tr>
<td>Last Ship Date: HW</td>
<td>The last-possible ship date that can be requested of Cisco and/or its contract manufacturers. Actual ship date is dependent on lead time.</td>
<td>December 27, 2010</td>
</tr>
<tr>
<td>End of Routine Failure Analysis Date: HW</td>
<td>The last-possible date a routine failure analysis may be performed to determine the cause of hardware product failure or defect.</td>
<td>September 28, 2011</td>
</tr>
<tr>
<td>End of New Service Attachment Date: HW</td>
<td>For equipment and software that is not covered by a service-and-support contract, this is the last date to order a new service-and-support contract or add the equipment and/or software to an existing service-and-support contract.</td>
<td>September 28, 2011</td>
</tr>
<tr>
<td>End of Service Contract Renewal Date: HW</td>
<td>The last date to extend or renew a service contract for the product.</td>
<td>December 24, 2014</td>
</tr>
<tr>
<td>Last Date of Support: HW</td>
<td>The last date to receive service and support for the product. After this date, all support services for the product are unavailable, and the product becomes obsolete.</td>
<td>September 30, 2015</td>
</tr>
</tbody>
</table>

A9: Components with Known Vulnerabilities

• How does this apply?
A10 - Underprotected APIs

AGI
ARI
WebRTC
wss://
<table>
<thead>
<tr>
<th>OWASP Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A1: Injection</strong></td>
</tr>
<tr>
<td><strong>A2: Broken Authentication and Session Management</strong></td>
</tr>
<tr>
<td><strong>A3: Cross-site Scripting</strong></td>
</tr>
<tr>
<td><strong>A4: Broken Access Control</strong></td>
</tr>
<tr>
<td><strong>A5: Security Misconfiguration</strong></td>
</tr>
<tr>
<td><strong>A6: Sensitive Data Exposure</strong></td>
</tr>
<tr>
<td><strong>A7: Insufficient Access Protection</strong></td>
</tr>
<tr>
<td><strong>A8: Cross-Site Request Forgery (CSRF)</strong></td>
</tr>
<tr>
<td><strong>A9: Using Components with Known Vulnerabilities</strong></td>
</tr>
<tr>
<td><strong>A10: Under Protected API’s</strong></td>
</tr>
</tbody>
</table>
Using Asterisk

vagrant up

Soft Phone
Console
AGI

```
contrib-jessie*CLI> core show help core show help
contrib-jessie*CLI> core show help core show help
Usage: core show help [topic]
When called with a topic as an argument, displays usage information on the given command. If called without a topic, it provides a list of commands.
```

https://wiki.asterisk.org/wiki/display/AST/Asterisk+13+Command+Reference
Scenario
Vectors

Two Vectors
A. Fat Finger Squat
B. Spoofed Target Vish
Vector A - Fat Finger Squat
Vector B – Spoofed Target Vish

Spoofed CID

Talk Recording Direct

Hello Can I help?
Vector A

Demo Time
Result

Left with a Recording
- What does that contain?
What’s that Sound?

Software
- DTMF Decoding
- Online (dialabc)

Hardware Decoder with ATA or line out

http://dialabc.com/sound/detect/index.html
Phreak Me

PhreakMe (github.com/phreakme)

• Overview
• Last Years Changes
• More Changes to come
Wrap Up

Thank you for your patience