Phone System Testing

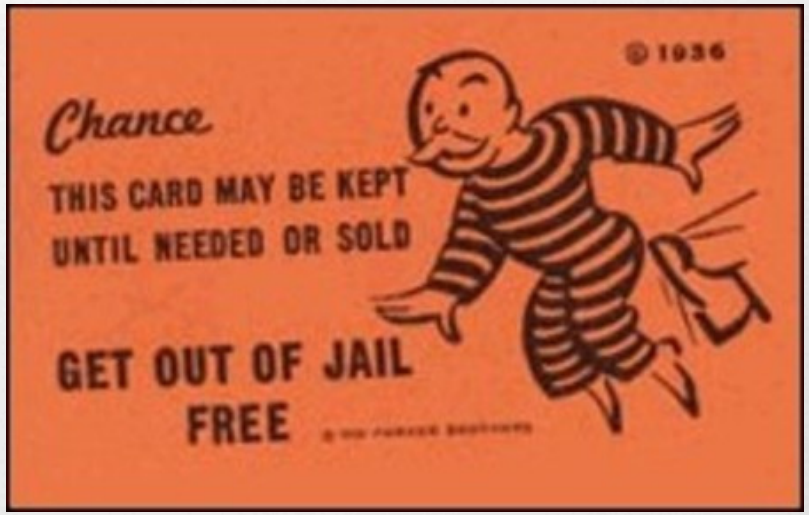
AND OTHER FUN TRICKS

Snide / Owen @LinuxBlog

github.com/PhreakMe/DC25 (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.



This is for educational purposes only

Introduction

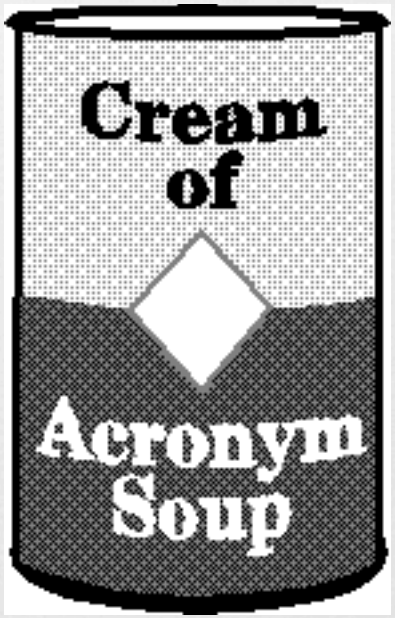
- History / Evolution
- Anatomy
- How to test
- Issue Types
- Fun Stuff

About Me

Presentations

Fun

Moved to US in 2000.




BORN IN THE 80'S RAISED IN THE 90'S
WE ARE THE LAST GENERATION THAT LEARNED TO PLAY IN THE STREET, WE ARE THE PIONEERS OF WALKMANS AND CHAT ROOMS, WE WERE THE LAST TO RECORD SONGS OFF THE RADIO ON CASSETTES. WE LEARNED HOW TO PROGRAM THE VCR BEFORE ANYONE ELSE, WE GREW UP WATCHING SAVED BY THE BELL, THE FRESH PRINCE OF BEL AIR AND MARTIN, WE TRAVELED IN CARS WITH NO SEAT BELTS OR AIRBAGS, WE LIVED WITHOUT CELL PHONES, WE WROTE LETTERS, WE GREW UP WITHOUT PROFILES AND LIKES AND BATHROOM MIRROR PICTURES ...
WE HAD THE BEST OF THE BEST OF ALL TIMES
anonews


NOT SURE IF I MISS THE 90'S
OR JUST MISS BEING A KID
assaliah / 9GAG


MULTIPLAYER
IN THE 90's.

Blocking Someone In
The 90's

How many of you remember your childhood home phone number?

So who uses Phones?

What industries?

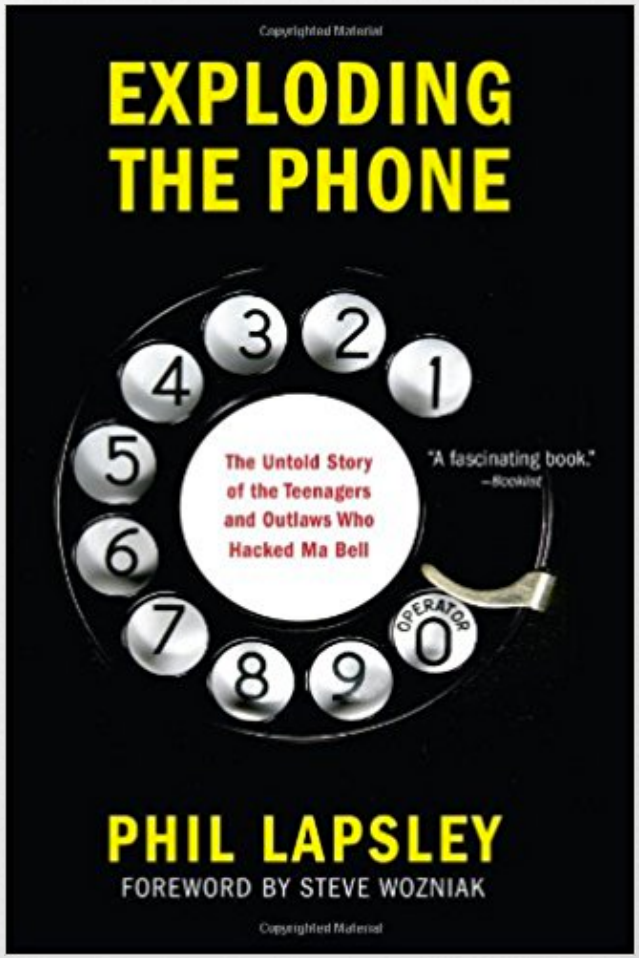
Particularly interesting:

- Banking/finance
- Healthcare
- Insurance
- Utilities
- Government
- Military.

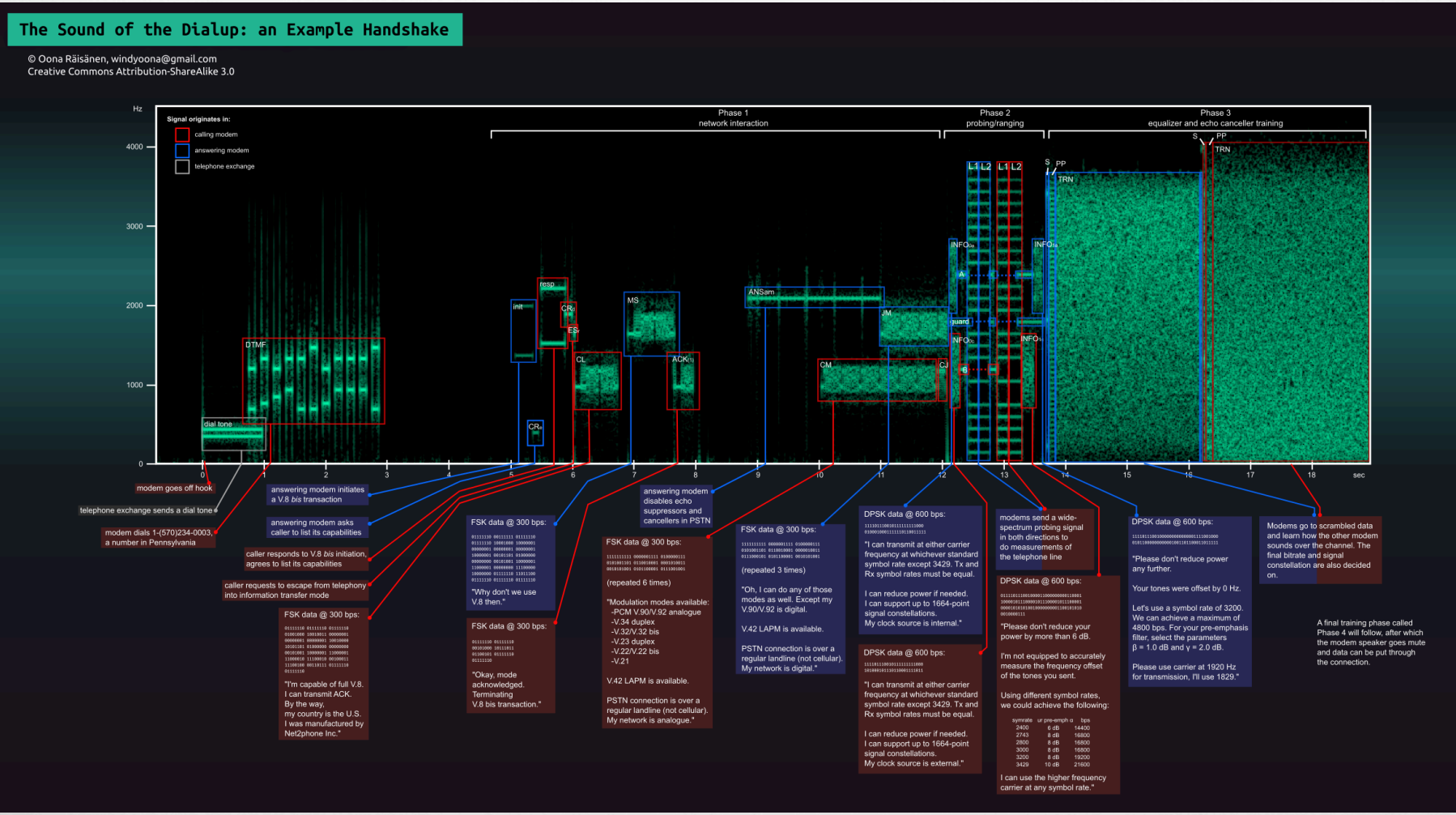
History

Sorry, Wrong number DC23

Exploding The Phone (2013)



History



https://en.wikipedia.org/wiki/Dial-up_Internet_access

History

- 1996 ICQ, NetMeeting, SMS (UK)
- 1997 AIM
- 1998 Yahoo Messenger
- 1999 MSN Messenger & Asterisk
- 2001 TeamSpeak & MMS
- 2002 Yahoo Messenger Chat
- 2003 Skype Released - MySpace
- 2004 Facebook
- 2005 YouTube
- 2007 iPhone

Recent History

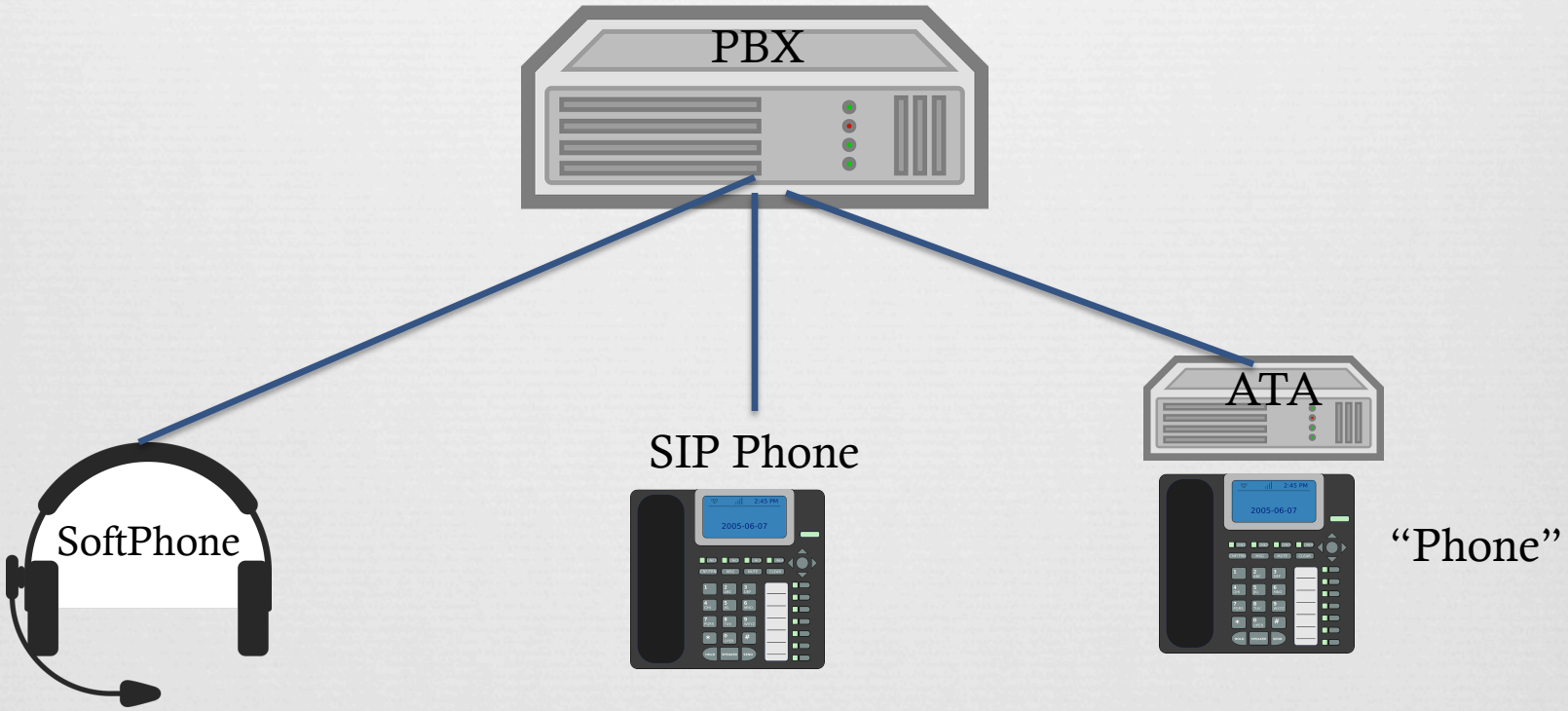
- Hangouts
- FB Messenger
- Signal
- Screen Sharing
- LiveStreaming
- WhatsApp
- SnapChat
- Kik
- etc etc.

PBX's

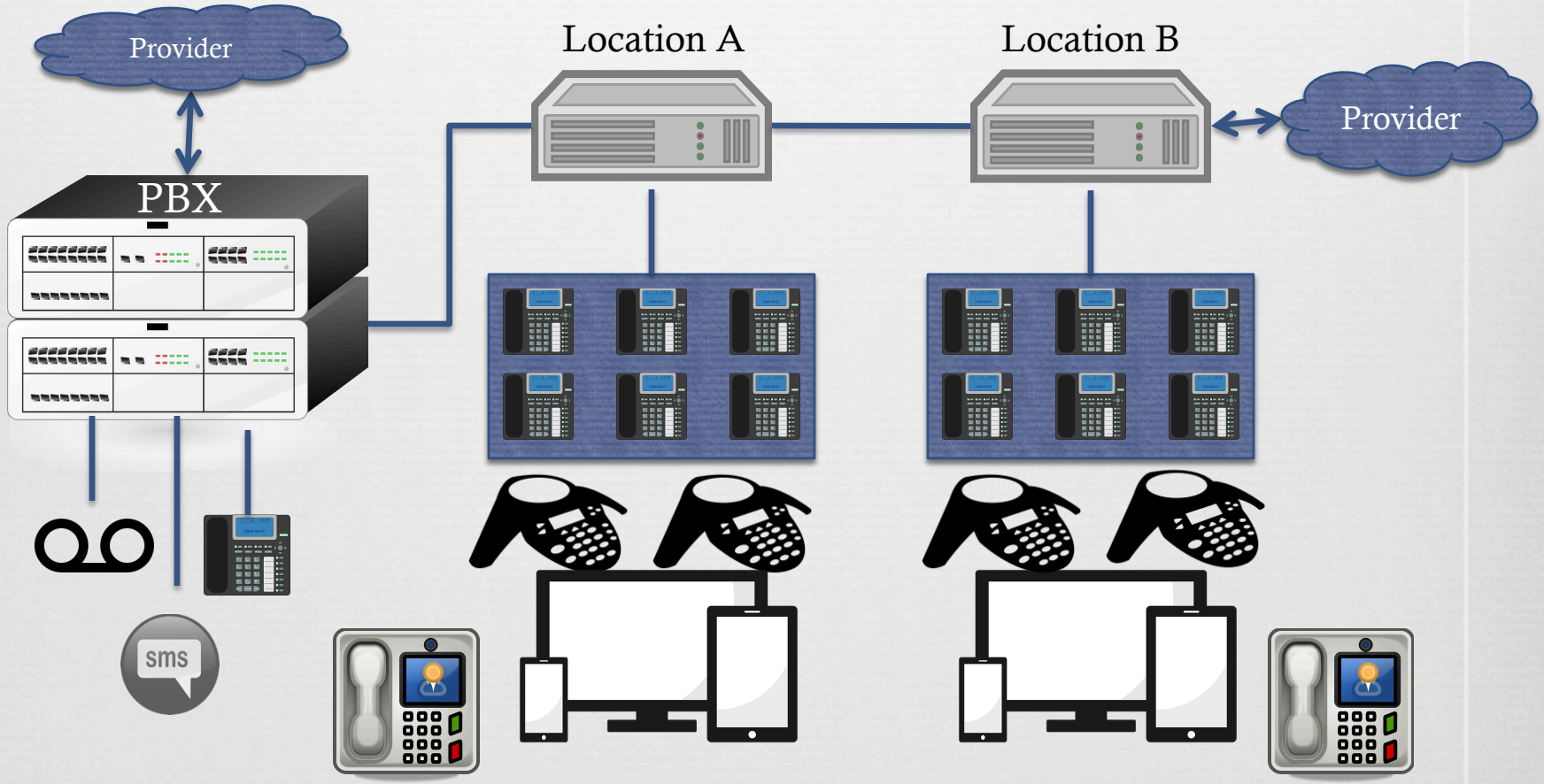
Why do people run PBX's?

- Reduce Costs
- Cheap Calling
- "Apps"
  - Voicemail
  - IVR's
  - Conferencing
  - Directories

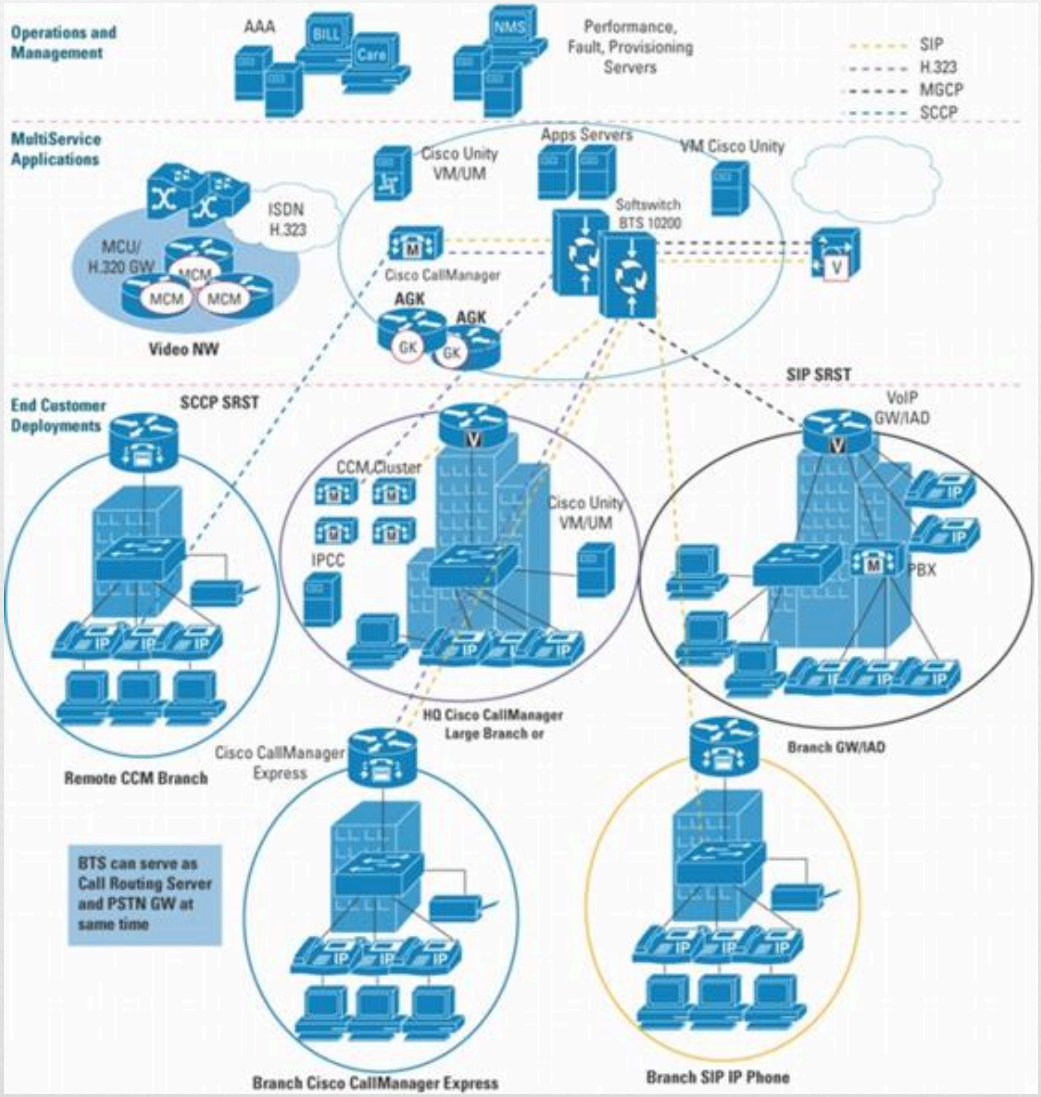
Basic Deployment



Common Deployment



Large

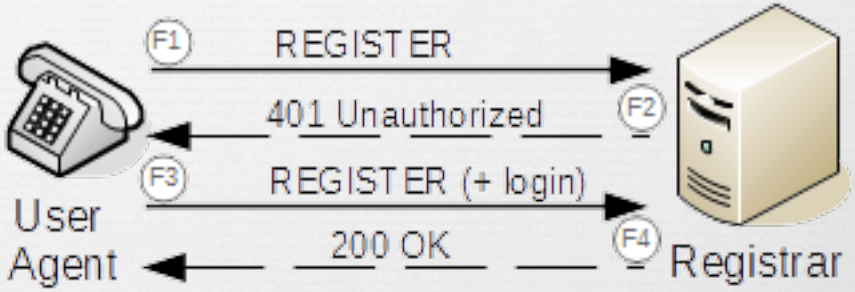

Operations and Management
AAA
BILL
Care
NMS
Performance, Fault, Provisioning Servers
SIP
H.323
MGCP
SCCP
MultiService Applications
Cisco Unity VM/UM
Apps Servers
VM Cisco Unity
Softswitch BTS 10200
ISDN H.323
MCU/ H.320 GW
MCM
MCM
MCM
Video NW
Cisco CallManager
AGK
AGK
GK
GK
SIP SRST
End Customer Deployments
SCCP SRST
VoIP GW/IAD
CCM Cluster
Cisco Unity VM/UM
IPCC
PBX
HQ Cisco CallManager Large Branch or
Branch GW/IAD
Cisco CallManager Express
Remote CCM Branch
BTS can serve as Call Routing Server and PSTN GW at same time
Branch Cisco CallManager Express
Branch SIP IP Phone

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
- Skype

Common Protocols

- SIP
- H.323
- IAX
- RTP
- XMPP



https://en.wikipedia.org/wiki/Session_Initiation_Protocol

Codecs

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

```
*CLI> core show codecs
Disclaimer: this command is for informational purposes only.
       It does not indicate anything about your configuration.
     ID  TYPE     NAME DESCRIPTION
-------------------------------------------------------------------------------
  100001 audio     g723 (G.723.1)
  100002 audio      gsm (GSM)
  100003 audio     ulaw (G.711 u-law)
  100004 audio     alaw (G.711 A-law)
  100011 audio     g726 (G.726 RFC3551)
  100006 audio    adpcm (ADPCM)
  100019 audio     slin (16 bit Signed Linear PCM)
  100007 audio    lpc10 (LPC10)
  100008 audio     g729 (G.729A)
  100009 audio    speex (SpeeX)
  100016 audio  speex16 (SpeeX 16khz)
  100010 audio     ilbc (iLBC)
  100005 audio g726aal2 (G.726 AAL2)
  100012 audio     g722 (G722)
  100021 audio   slin16 (16 bit Signed Linear PCM (16kHz))
  300001 image     jpeg (JPEG image)
  300002 image      png (PNG image)
  200001 video     h261 (H.261 Video)
  200002 video     h263 (H.263 Video)
  200003 video    h263p (H.263+ Video)
  200004 video     h264 (H.264 Video)
  200005 video    mpeg4 (MPEG4 Video)
  400001  text      red (T.140 Realtime Text with redundancy)
  400002  text     t140 (Passthrough T.140 Realtime Text)
  100013 audio   siren7 (ITU G.722.1 (Siren7, licensed from Polycom))
  100014 audio  siren14 (ITU G.722.1 Annex C, (Siren14, licensed from Polycom))
  100017 audio  testlaw (G.711 test-law)
  100015 audio     g719 (ITU G.719)
  100028 audio  speex32 (SpeeX 32khz)
  100020 audio   slin12 (16 bit Signed Linear PCM (12kHz))
  100022 audio   slin24 (16 bit Signed Linear PCM (24kHz))
  100023 audio   slin32 (16 bit Signed Linear PCM (32kHz))
  100024 audio   slin44 (16 bit Signed Linear PCM (44kHz))
  100025 audio   slin48 (16 bit Signed Linear PCM (48kHz))
  100026 audio   slin96 (16 bit Signed Linear PCM (96kHz))
  100027 audio  slin192 (16 bit Signed Linear PCM (192kHz))
```

DTMF

Dual Tone Multi Frequency

Can be easily generated

	1209 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

http://www.genave.com/dtmf.htm
https://en.wikipedia.org/wiki/Dual-tone_multi-frequency_signaling

How?

Step 1) Figure out what you're testing

Testing

Scope

- Blackbox / Whitebox?

Info Gathering

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

Quad Core 1.6GHz
2GB Ram
16GB Onboard Flash
Gigabit Ethernet
Wifi

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

Lack of SSL/TLS for SIP

General Lack of Auth Controls

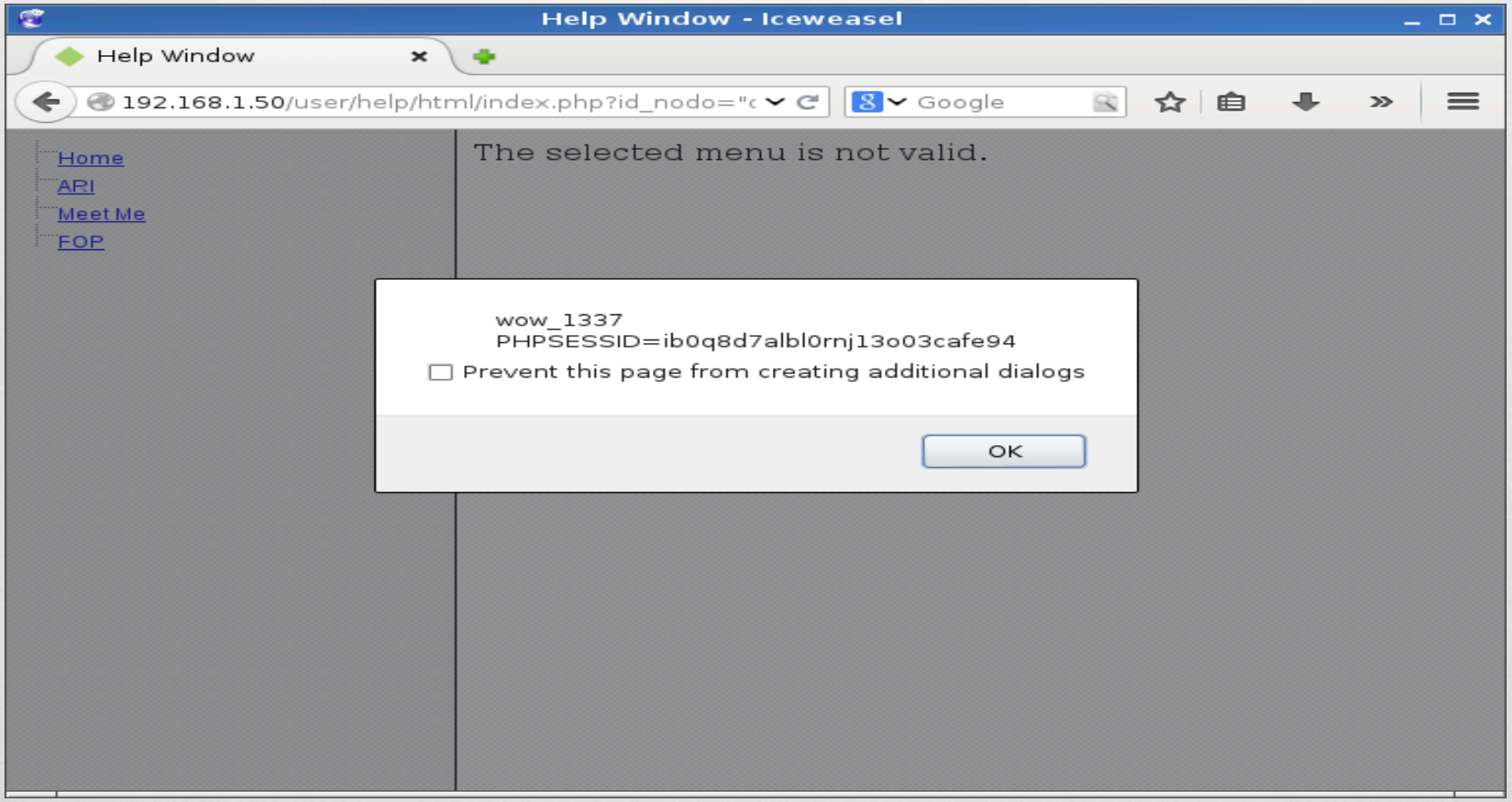
Registration Hi-Jacking

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP
192.168.1.161:60872;branch=z9hG4bK-524287-1---031c4a1857fab377;received=192.
168.1.161;rport=60872
From: <sip:user@192.168.1.50>;tag=9358e342
To: <sip:user@192.168.1.50>;tag=as1a862888
Call-ID: 84254ODViMjY3ZjVmMTU3NzhkYmRhZjNhNmY0ZTk0OThkOTQ
CSeq: 1 REGISTER
Server: Asterisk PBX 11.13.1~dfsg-2+deb8u2
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO,
PUBLISH, MESSAGE
Supported: replaces, timer
WWW-Authenticate: Digest algorithm=MD5, realm="asterisk", nonce="26d841dc"
Content-Length: 0
```

https://wiki.asterisk.org/wiki/display/AST/Secure+Calling+Tutorial

A3: Cross-site Scripting

Somewhat covered by injection



401 Authorization Required - Iceweasel

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

192.168.1.50/maint/modules/home/index.php

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

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

Sum of #	Gained Access			
Row Labels	Admin	None	User	Grand Total
High	**31**	**11**		**42**
Exec Code Overflow	31			31
XSS		11		11
Low	**45**	**469**	**348**	**862**
Bypass		11		11
Dir. Trav.		58		58
Dos & Priv			4	4
DoS +Info		30		30
DoS Exec Code		8	19	27
DoS Exec Code Overflow		29	16	45
DoS Exec Code Overflow Bypass			35	35
DoS Overflow		56		56
DoS Overflow Mem. Corr.		19		19
Exec Code		36		36
Exec Code +Priv		4		4
Exec Code Dir. Trav.			33	33
Exec Code File Inclusion			19	19
Exec Code Overflow		94	130	224
Exec Code Sql		14	53	67
Info		102		102
Overflow		2		2
Priv	45	3		48
Sql			39	39
(blank)		3		3
Medium	**29**	**170**		**199**
Bypass		36		36
DoS +Info		16		16
DoS Exec Code Overflow		21		21
DoS Overflow		26		26
Exec Code Overflow	29	50		79
Info		20		20
XSS		1		1
Grand Total	**105**	**650**	**348**	**1103**

A9: Components with Known Vulnerabilities

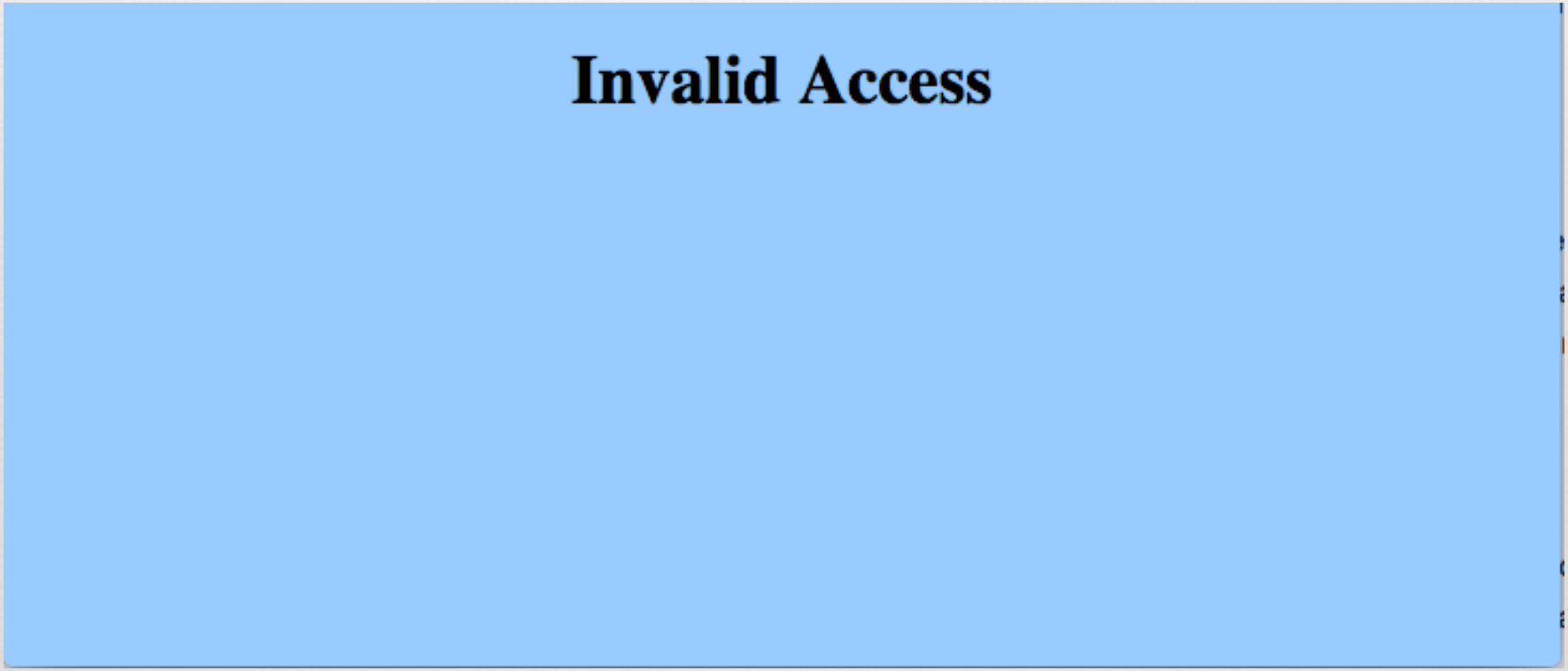
Cisco ATA186-I2-A Analog Telephone Adapter - ...
$110.00
ServerSupply.com
Free shipping

Cisco ATA186-I1 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

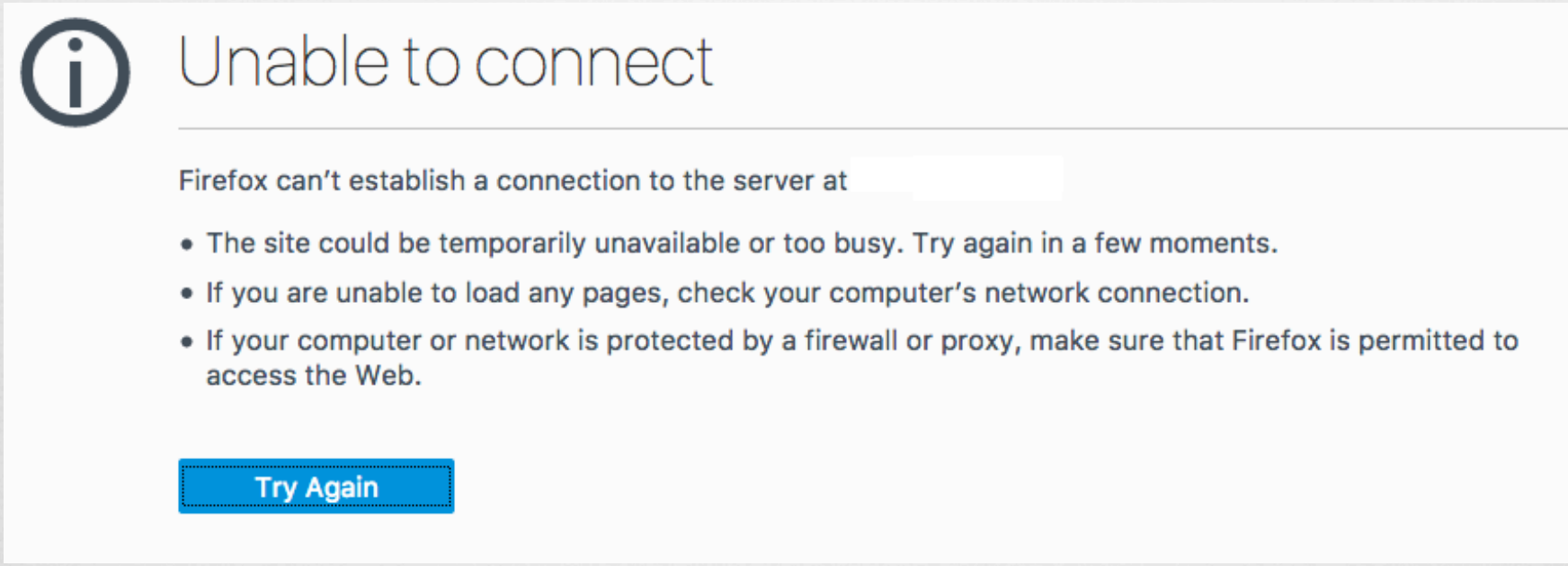
A9: Components with Known Vulnerabilities



A9: Components with Known Vulnerabilities

TftpURL:		CfgInterval:	86400
EncryptKey:	•	EncryptKeyEx:	00000000000000000000
Dhcp:	0	StaticIP:	
StaticRoute:		StaticNetMask:	
UID0:		PWD0:	
UID1:		PWD1:	
GkOrProxy:		UseLoginID:	0
LoginID0:		LoginID1:	
AltGk:	0	AltGkTimeOut:	0
SIPRegInterval:	120	MaxRedirect:	5
SIPRegOn:	1	NATIP:	0.0.0.0
SIPPort:	5060	MediaPort:	16384
OutBoundProxy:	0	NatServer:	0
NatTimer:	0x00000000	MsgRetryLimits:	0x00000000
SessionTimer:	0x00000000	SessionInterval:	1800
MinSessionInterval:	1800	DisplayName0:	0
DisplayName1:	0	LBRCodec:	0
AudioMode:	0x00140014	RxCodec:	1
TxCodec:	1	NumTxFrames:	2
CallFeatures:	0xffffffff	PaidFeatures:	0xffffffff
CallerIdMethod:	0x00019e60	FeatureTimer:	0x00000000
FeatureTimer2:		Polarity:	

A9: Components with Known Vulnerabilities



A9: Components with Known Vulnerabilities

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

Milestone	Definition	Date
End-of-Life Announcement Date	The date the document that announces the end of sale and end of life of a product is distributed to the general public.	March 30, 2010
End-of-Sale Date	The last date to order the product through Cisco point-of-sale mechanisms. The product is no longer for sale after this date.	September 28, 2010
Last Ship Date: HW	The last-possible ship date that can be requested of Cisco and/or its contract manufacturers. Actual ship date is dependent on lead time.	December 27, 2010
End of Routine Failure Analysis Date: HW	The last-possible date a routine failure analysis may be performed to determine the cause of hardware product failure or defect.	September 28, 2011
End of New Service Attachment Date: HW	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.	September 28, 2011
End of Service Contract Renewal Date: HW	The last date to extend or renew a service contract for the product.	December 24, 2014
Last Date of Support: HW	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.	September 30, 2015

http://www.cisco.com/c/en/us/products/unified-communications/ata-180-series-analog-telephone-adaptors/end_of_life_notice_c51-585199.html

A9: Components with Known Vulnerabilities

- How does this apply?

A10 - Underprotected APIs

AGI
ARI
WebRTC
wss://
UserAgents

OWASP Mapping

A1: Injection	1: Security Misconfiguration
A2: Broken Authentication and Session Management	2: Broken Authentication and Session Management
A3: Cross-site Scripting	3: Injection
A4: Broken Access Control	4: Using Components with Known Vulnerabilities
A5: Security Misconfiguration	5:Broken Access Control
A6: Sensitive Data Exposure	6: Insufficient Access Protection
A7: Insufficient Access Protection	7: Sensitive Data Exposure
A8: Cross-Site Request Forgery (CSRF)	8: XSS
A9: Using Components with Known Vulnerabilities	9: Underprotected API's
A10: Under Protected API's	10: CSRF

Using Asterisk

vagrant up

Console

AGI

```
contrib-jessie*CLI> core show help core show
```

```
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

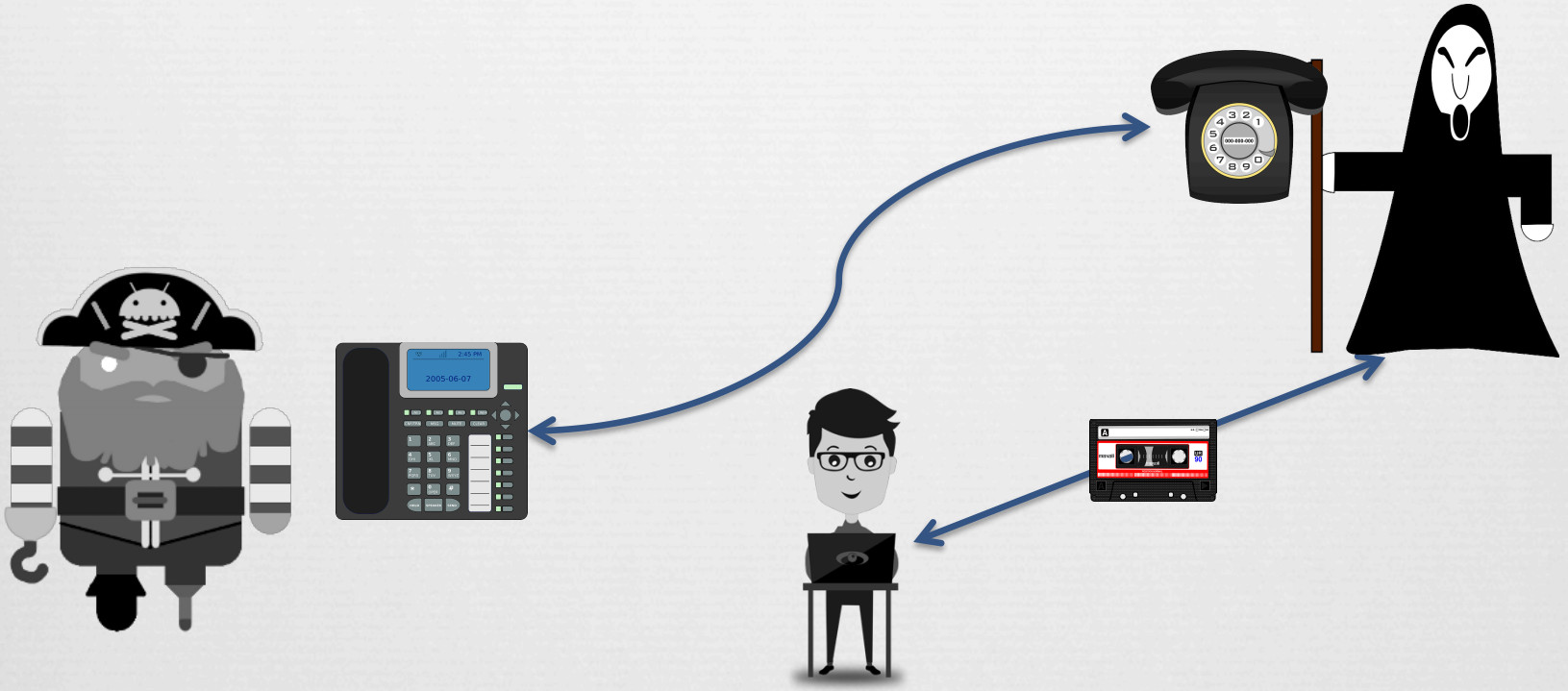
Vectors

Two Vectors

A. Fat Finger Squat

B. Spoofed Target Vish

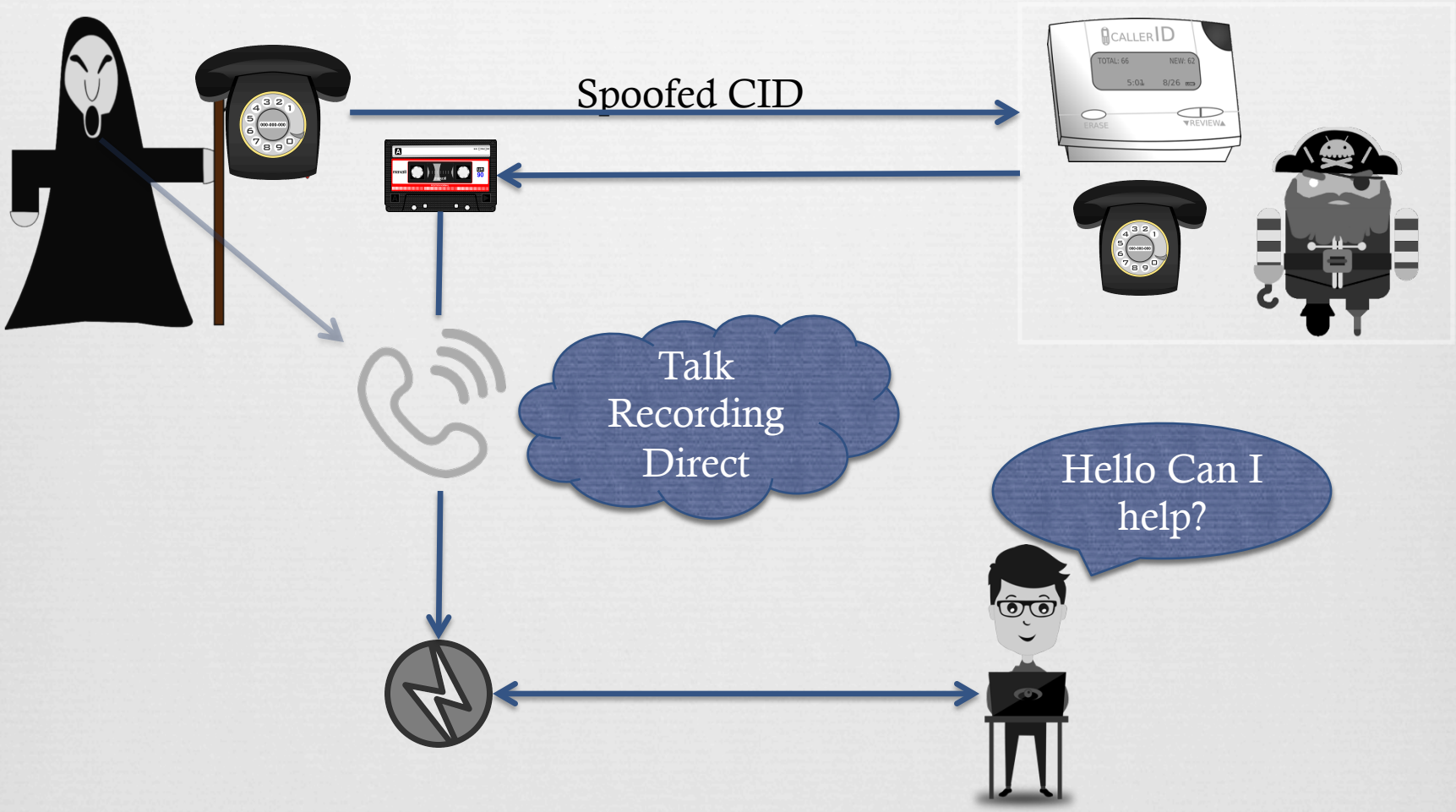
Vector A - Fat Finger Squat



Vector A

Demo Time

Vector B – Spoofed Target Vish



Result

Left with a Recording

- What does that contain?

What's that Sound?

Software
- DTMF Decoding

Software
- Online (dialabc)

Hardware Decoder with ATA or line out

Tones Found

Tone	Start Offset [ms]	End Offset [ms]	Length [ms]
1	845 ± 15	965 ± 15	120 ± 30
5	1,056 ± 15	1,177 ± 15	120 ± 30
7	1,267 ± 15	1,388 ± 15	120 ± 30
0	1,448 ± 15	1,569 ± 15	120 ± 30
2	1,659 ± 15	1,780 ± 15	120 ± 30
3	1,871 ± 15	1,991 ± 15	120 ± 30
4	2,052 ± 15	2,173 ± 15	120 ± 30
0	2,263 ± 15	2,384 ± 15	120 ± 30
0	2,444 ± 15	2,565 ± 15	120 ± 30
0	2,655 ± 15	2,776 ± 15	120 ± 30
3	2,857 ± 15	2,987 ± 15	120 ± 30

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

Phreak Me

github.com/phreakme

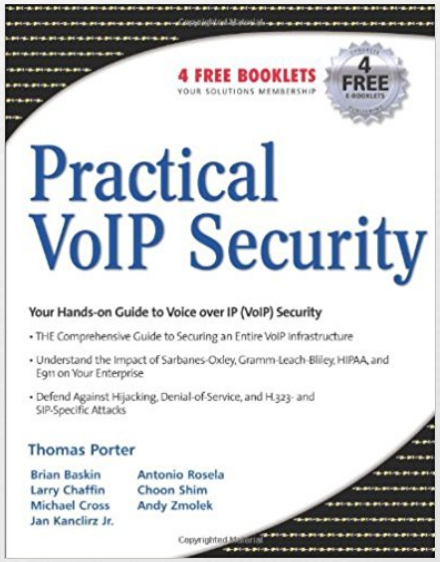
- Overview
- RTFM

- More Changes to come

Additional Resources

Books:

Practical VoIP Security



Presentations

Fatih Ozavci – VoIP Wars

Jason Ostrom - VoIP Hopping the Hotel

https://voipsa.org/Resources/tools.php

Wrap Up