

Voice over IP

VoIP (In) Security



Presented by Darren Bilby
NZISF 14 July 2005

Security-Assessment.com – Who We Are

- NZ's only pure-play security firm
- Largest team of security professionals in NZ
- Offices in Auckland, Wellington and Sydney
- Committed to research and improving our industry

- Specialisation in multiple security fields
 - Security assessment
 - Security management
 - Forensics / incident response
 - Research and development



What is VoIP?

- **Voice over Internet Protocol**
- **“A method for taking analog audio signals, like the kind you hear when you talk on the phone, and turning them into digital data that can be transmitted over the Internet. ”**
- **Also known as:**
 - **Voice over Packet (VoP)**
 - **IP Telephony (IPT)**



VoIP Trends

- **VOIP becoming more popular and will increase in future**
- **Many ISPs and Telco's starting to offer VoIP services**
- **Like most other phone calls, it is presumed to be confidential**
- **Original protocols designed by telephone people with trusted networks in mind**



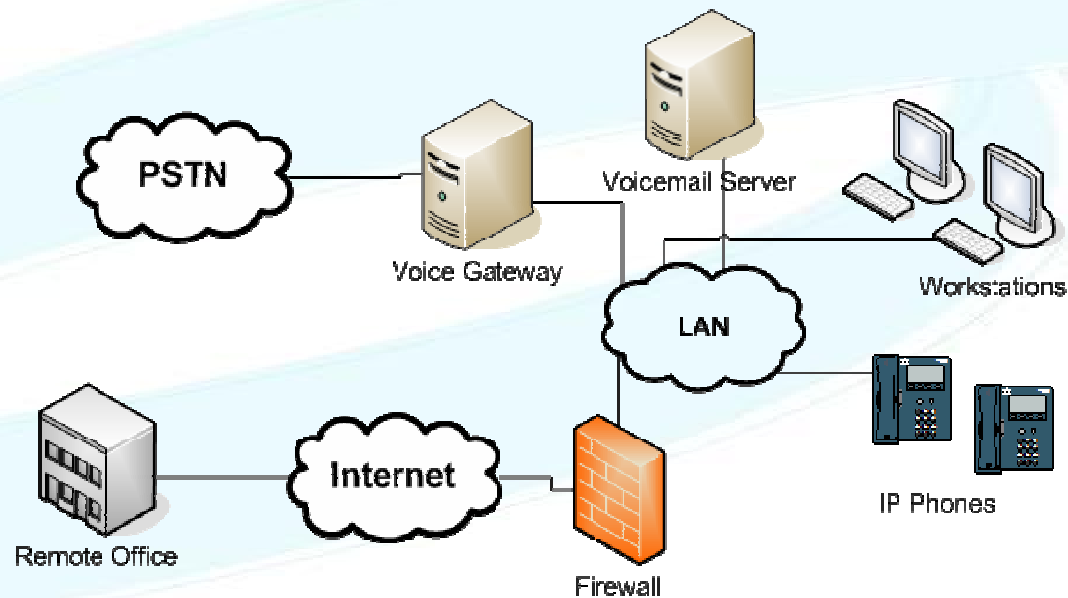
Different Types of VoIP

- There are many different implementations of VoIP:
 - MSN
 - Firefly
 - Skype
 - Office Phone Replacements
 - Push to Talk
 - Ihug Connect
 - Slingshot iTalk
- **Different technologies, but most of these do not have security built-in.**



Components of a VoIP Implementation

- Client
- Voice Gateway
- Support Servers – Voicemail, Management Servers



VoIP Clients



- **Hard Phone**
- **Soft Phone**
- **Analog Telephone Adaptor (ATA)**



Protocols and Acronyms

Protocols and Acronyms

- **Signaling Protocol**
 - Create, modify, and terminate sessions with participants
 - Conferences
 - Proxies
 - Authentication
- **Transport Protocol**
 - Manages the actual voice data



Protocols and Acronyms

- **ITU H.323**
 - One of the earliest sets of VoIP standards
 - Handles voice, video, and data conferencing
 - Some limitations, but most VoIP traffic utilises this today
- **Session Initiation Protocol (SIP)**
 - Signaling protocol
 - RFC 3261
 - Currently most favored protocol for new systems
- **Realtime Transport Protocol (RTP/RTCP)**
 - Used for media transfer by other protocols
 - Fast, scaleable and efficient
 - RTCP manages the call
 - RTP is the voice data



Protocols and Acronyms

- **SCCP (Skinny)**
 - Cisco signaling and control protocol
 - Open standard
- **IAX/IAX2**
 - Signaling and control protocol
 - Designed by Asterisk open source project
 - Handles NAT and Firewalls cleanly
- **MGCP (Media Gateway Control Protocol)**
 - Signaling and control protocol
 - Reduce traffic between gateways



Why is VoIP Security a Problem?

- Eavesdropping and Recording Phone Calls
- Track Calls
- Stealing Confidential Information
- Modifying Phone Calls
- Making Free Phone Calls
- Faking Caller ID
- Board Room Bugging
- Spam over IP Telephony (SPIT)
- Another Network Entry Point



The Problems We See With VoIP

- Insecure Servers
- Insecure Clients
- Insecure Protocols
- Insecure Protocols on Insecure Networks
- Badly Written Protocols
- Implementation Flaws

There is nothing new under the sun!



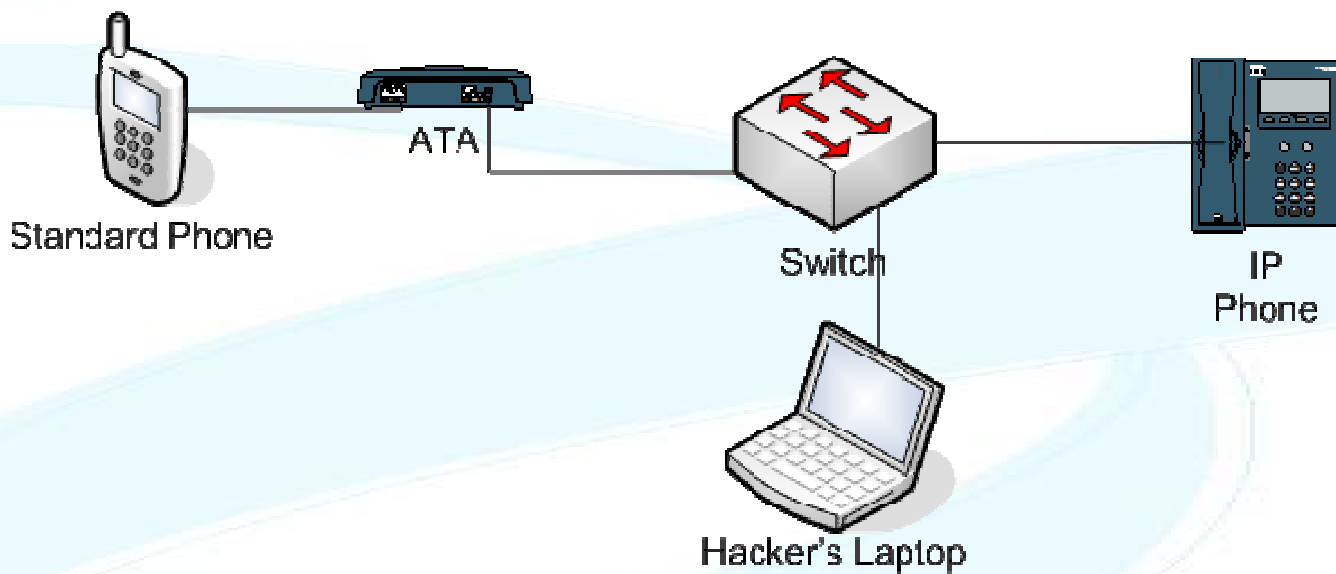
VoIP Security Scenarios

Scenario 1 – Industrial Information Gathering

- Employee uses the VOIP network to listen to the managing director's phone calls
- Gains access to personal details
- Forwards information about business deals to competitors



Demo



- Cain - <http://www.oxid.it>
- Ettercap – <http://ettercap.sourceforge.net>
- Ethereal – <http://www.ethereal.com>
- Vomit - <http://vomit.xtdnet.nl>



New ARP Poison Routing

WARNING !!!

APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted also. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

IP address	MAC	IP address	MAC
192.168.0.4	00D05908C07B	10.10.10.2	000D61C9D2AF
192.168.0.20	000BEA8000BC	192.168.0.66	00055D8028D4
192.168.0.66	00055D8028D4	192.168.0.20	000BEA8000BC
10.10.10.2	000D61C9D2AF		

OK

Cancel



The screenshot displays the 'airtight' application window. The interface includes a menu bar (File, View, Configure, Tools, Help), a toolbar with various icons, and a tabbed interface with the following tabs: Protected Storage, Network, Sniffer, LSA Secrets, Cracker, Traceroute, CCDU, and Wireless. The main area contains a table with the following data:

Started	Closed	IP1 (Codec)	IP2 (Codec)	Status	File	Size
12/04/2005 - 11:23:48	12/04/2005 - 11:23:59	192.168.0.66:49152 (P...	192.168.0.4:17764 (PC...		RTP-20050411232414348.wav	291326 bytes

At the bottom of the application, there is a status bar with icons for Hosts, APR, APR-DNS, APR-SSH-1, APR-HTTPS, Routing, Passwords, and VoIP. The URL <http://www.oxid.it> is displayed in the bottom left corner.



sipcapture.ethereal - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: + Expression... Clear Apply

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	203.22.251.220	192.168.1.5	IAX2	Text, source call# 1458, timestamp 21654539ms subclass 0
2	0.000414	192.168.1.5	203.22.251.220	IAX2	IAX, source call# 30343, timestamp 21654539ms ACK
3	0.073683	203.22.251.220	192.168.1.5	IAX2	Text, source call# 1458, timestamp 21654623ms subclass 0
4	0.073875	192.168.1.5	203.22.251.220	IAX2	IAX, source call# 30343, timestamp 21654623ms ACK
5	3.752547	192.168.1.5	192.168.1.254	DNS	Standard query A iptel.org
6	4.095239	192.168.1.254	192.168.1.5	DNS	Standard query response A 195.37.77.99
7	4.105281	192.168.1.5	195.37.77.99	SIP/SD	Request: INVITE sip:darrenbi@iptel.org, with session description
8	4.450753	195.37.77.99	192.168.1.5	SIP	Status: 407 Proxy Authentication Required
9	4.457416	192.168.1.5	195.37.77.99	SIP	Request: ACK sip:darrenbi@iptel.org
10	4.457443	192.168.1.5	195.37.77.99	SIP/SD	Request: INVITE sip:darrenbi@iptel.org, with session description
11	4.816035	195.37.77.99	192.168.1.5	SIP	Status: 100 trying -- your call is important to us
12	5.022024	195.37.77.99	192.168.1.5	UDP	Source port: 5060 Destination port: 5060
13	5.317021	195.37.77.99	192.168.1.5	SIP	Status: 180 Ringing
14	5.451757	203.22.251.220	192.168.1.5	IAX2	Text, source call# 1458, timestamp 21660001ms subclass 0
15	5.452171	192.168.1.5	203.22.251.220	IAX2	IAX, source call# 30343, timestamp 21660001ms ACK
16	8.127168	205.188.2.87	192.168.1.5	AIM	Oncoming Buddy: 240842380
17	8.253551	192.168.1.5	205.188.2.87	TCP	1052 > 5190 [ACK] seq=0 Ack=115 win=65420 [CHECKSUM INCORRECT
18	13.654077	195.37.77.99	192.168.1.5	SIP/SD	Status: 200 ok, with session description
19	13.662691	192.168.1.5	195.37.77.99	SIP	Request: ACK sip:darrenbi@222.152.49.128:5060;nat=yes
20	13.682138	192.168.1.5	195.37.77.99	RTP	Payload type=ITU-T G.711 PCMA, SSRC=3875315064, Seq=1, Time=9.
21	13.682182	192.168.1.5	195.37.77.99	RTP	Payload type=ITU-T G.711 PCMA, SSRC=3875315064, Seq=2, Time=9.
22	13.688586	195.37.77.99	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=3, Time=6.
23	13.702088	192.168.1.5	195.37.77.99	RTCP	Sender Report
24	13.702134	192.168.1.5	195.37.77.99	RTP	Payload type=ITU-T G.711 PCMA, SSRC=3875315064, Seq=3, Time=9.
25	13.703658	195.37.77.99	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=4, Time=8.
26	13.721125	192.168.1.5	195.37.77.99	RTP	Payload type=ITU-T G.711 PCMA, SSRC=3875315064, Seq=4, Time=9.
27	13.724574	195.37.77.99	192.168.1.5	RTCP	Sender Report
28	13.729203	195.37.77.99	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=5, Time=9.
29	13.741245	192.168.1.5	195.37.77.99	RTP	Payload type=ITU-T G.711 PCMA, SSRC=3875315064, Seq=5, Time=9.
30	13.746945	195.37.77.99	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=6, Time=1.
31	13.761303	192.168.1.5	195.37.77.99	RTCP	Sender Report
32	13.761367	192.168.1.5	195.37.77.99	RTP	Payload type=ITU-T G.711 PCMA, SSRC=3875315064, Seq=6, Time=9.
33	13.764466	195.37.77.99	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=7, Time=1.
34	13.784496	195.37.77.99	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=8, Time=1.
35	13.803156	195.37.77.99	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=9, Time=1.
36	13.826731	195.37.77.99	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=10, Time=1.
37	13.845461	195.37.77.99	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=11, Time=1.
38	13.885827	195.37.77.99	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=12, Time=1.
39	13.892375	195.37.77.99	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=13, Time=1.
40	13.905048	195.37.77.99	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=14, Time=1.

File: sipcapture.ethereal 234 KB UU: | P: 1042 D: 1042 M: U

File Edit View Go Capture Analyze Statistics Help

Filter: + Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Details
1	0.000000	203.22.1.1	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=1, Time=0.000000
2	0.000414	192.168.1.5	203.22.1.1	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=2, Time=0.000414
3	0.073683	203.22.1.1	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=3, Time=0.073683
4	0.073875	192.168.1.5	203.22.1.1	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=4, Time=0.073875
5	3.752547	192.168.1.5	203.22.1.1	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=5, Time=3.752547
6	4.095239	192.168.1.5	203.22.1.1	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=6, Time=4.095239
7	4.105281	192.168.1.5	203.22.1.1	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=7, Time=4.105281
8	4.450753	192.168.1.5	203.22.1.1	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=8, Time=4.450753
9	4.457416	192.168.1.5	203.22.1.1	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=9, Time=4.457416
10	4.457443	192.168.1.5	203.22.1.1	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=10, Time=4.457443
11	4.816035	192.168.1.5	203.22.1.1	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=11, Time=4.816035
12	5.022024	192.168.1.5	203.22.1.1	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=12, Time=5.022024
13	5.317021	192.168.1.5	203.22.1.1	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=13, Time=5.317021
14	5.451757	203.22.1.1	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=14, Time=5.451757
15	5.452171	192.168.1.5	203.22.1.1	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=15, Time=5.452171
16	8.127168	203.22.1.1	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=16, Time=8.127168
17	8.253551	192.168.1.5	203.22.1.1	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=17, Time=8.253551
18	13.654077	192.168.1.5	203.22.1.1	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=18, Time=13.654077
19	13.662691	192.168.1.5	203.22.1.1	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=19, Time=13.662691
20	13.682138	192.168.1.5	203.22.1.1	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=20, Time=13.682138
21	13.682182	192.168.1.5	203.22.1.1	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=21, Time=13.682182
22	13.688586	195.37.77.99	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=22, Time=13.688586
23	13.702088	192.168.1.5	195.37.77.99	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=23, Time=13.702088
24	13.702134	192.168.1.5	195.37.77.99	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=24, Time=13.702134
25	13.703658	195.37.77.99	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=25, Time=13.703658
26	13.721125	192.168.1.5	195.37.77.99	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=26, Time=13.721125
27	13.724574	195.37.77.99	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=27, Time=13.724574
28	13.729203	195.37.77.99	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=28, Time=13.729203
29	13.741245	192.168.1.5	195.37.77.99	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=29, Time=13.741245
30	13.746945	195.37.77.99	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=30, Time=13.746945
31	13.761303	192.168.1.5	195.37.77.99	RTCP	Sender Report
32	13.761367	192.168.1.5	195.37.77.99	RTP	Payload type=ITU-T G.711 PCMA, SSRC=3875315064, Seq=31, Time=13.761367
33	13.764466	195.37.77.99	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=32, Time=13.764466
34	13.784496	195.37.77.99	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=33, Time=13.784496
35	13.803156	195.37.77.99	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=34, Time=13.803156
36	13.826731	195.37.77.99	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=35, Time=13.826731
37	13.845461	195.37.77.99	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=36, Time=13.845461
38	13.885827	195.37.77.99	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=37, Time=13.885827
39	13.892375	195.37.77.99	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=38, Time=13.892375
40	13.905048	195.37.77.99	192.168.1.5	RTP	Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=39, Time=13.905048

Ethereal: RTP Stream Analysis

Forward Direction | Reversed Direction

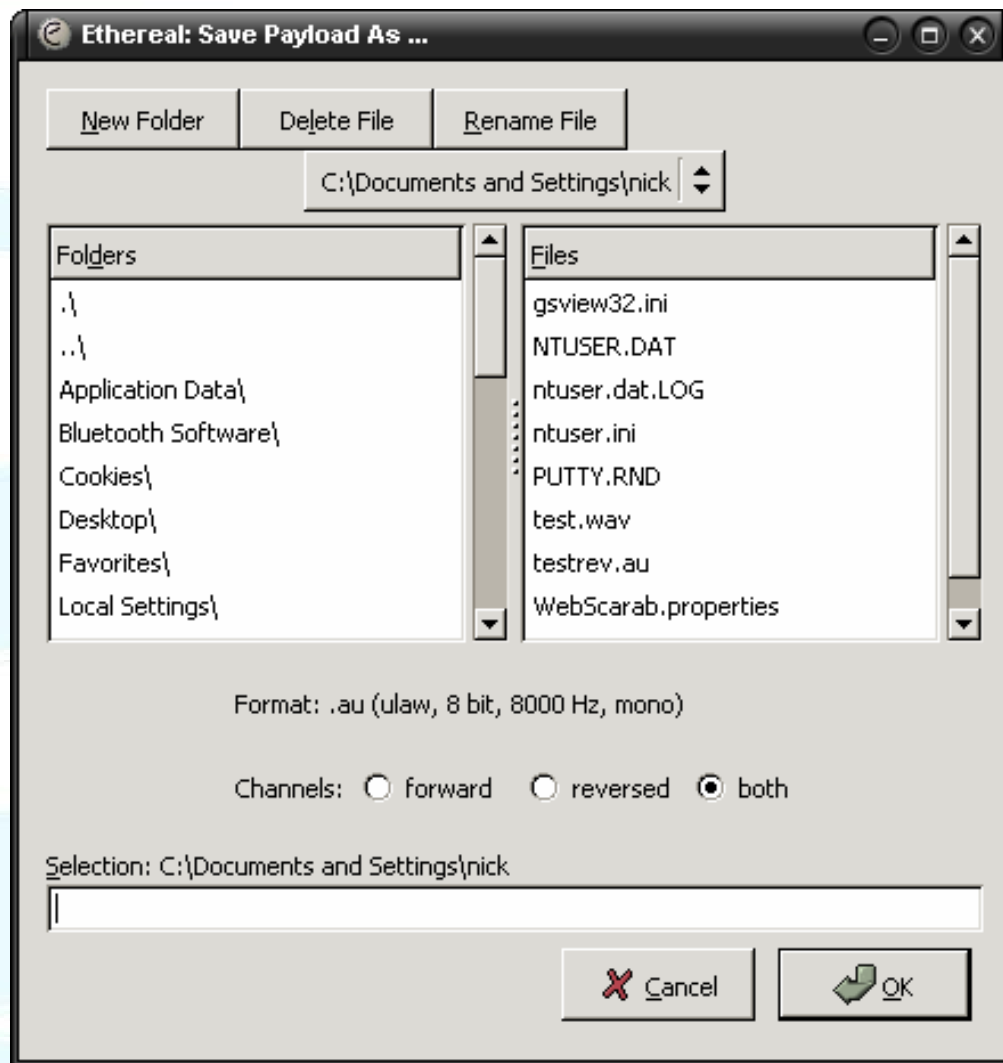
Analysing stream from 195.37.77.99 port 46428 to 192.168.1.5 port 8000 SSRC = 2419731127

Packet	Sequence	Delay (s)	Jitter (s)	Marker	Status
22	3	0.000000	0.000000		[Ok]
25	4	0.015072	0.000308		[Ok]
28	5	0.025545	0.000635		[Ok]
30	6	0.017742	0.000737		[Ok]
33	7	0.017521	0.000846		[Ok]
34	8	0.020030	0.000795		[Ok]
35	9	0.018660	0.000829		[Ok]
36	10	0.023575	0.001000		[Ok]
37	11	0.018730	0.001017		[Ok]
38	12	0.040366	0.002227		[Ok]
39	13	0.006548	0.002928		[Ok]
40	14	0.012673	0.003203		[Ok]
41	16	0.041341	0.003087		Wrong sequence nr.
42	17	0.019690	0.002913		[Ok]
43	18	0.018738	0.002810		[Ok]
44	19	0.021644	0.002827		[Ok]

Max delay = 0.099230 sec at packet no. 436
 Total RTP packets = 644 (expected 654) Lost RTP packets = 10 Sequence errors = 10

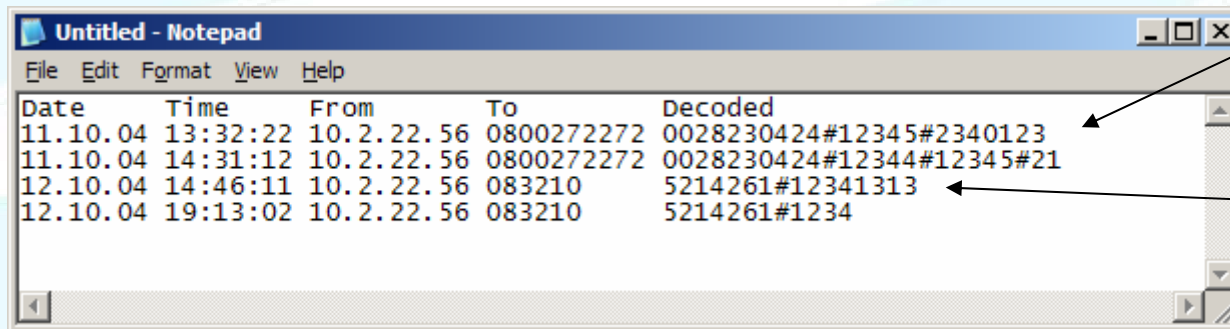
Save payload... Save as CSV... Refresh Jump to Next non-Ok Close

File: sipcapture.ethereal 234 KB UUI: P: 1042 D: 1042 M: U



Scenario 2 – The Fraud

- Employee uses ARP redirection in a large office to record all voice conversations
- Leaves it recording and logging for a week
- Then uses DTMF decoder to get access to other employees bank details, voice mailboxes etc



The screenshot shows a Notepad window titled "Untitled - Notepad" with a menu bar (File, Edit, Format, View, Help). The text content is as follows:

Date	Time	From	To	Decoded
11.10.04	13:32:22	10.2.22.56	0800272272	0028230424#12345#2340123
11.10.04	14:31:12	10.2.22.56	0800272272	0028230424#12344#12345#21
12.10.04	14:46:11	10.2.22.56	083210	5214261#12341313
12.10.04	19:13:02	10.2.22.56	083210	5214261#1234

Phone banking

Voice Mail



Scenario 3 – The Industrial Spy

- Evil Russian hacker is hired by a competitor to gain knowledge of business strategies.
- Hacker sends secretary a link to FunnyGame.exe, pretending to be an associate.
- Hacker sets boardroom IP phone in speakerphone mode, and calls a phone he controls thus recording boardroom meetings.



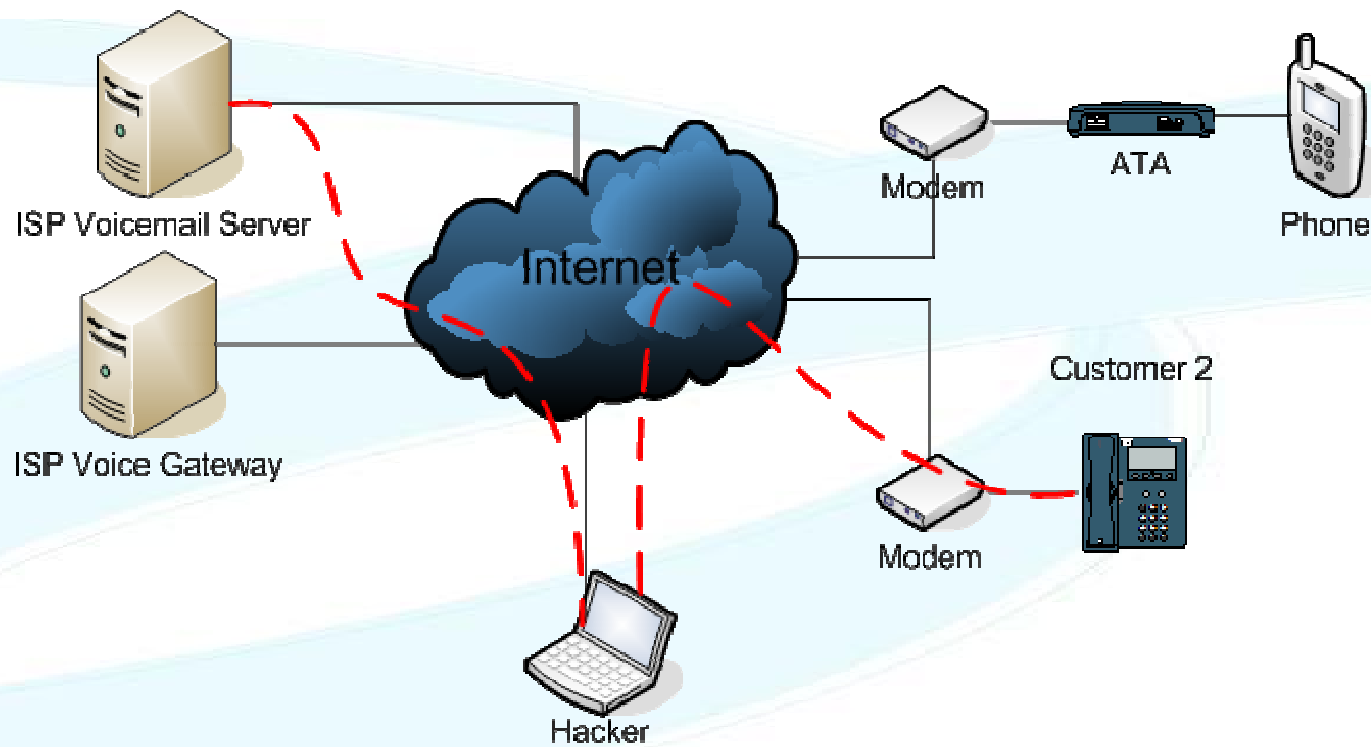
Scenario 4 – Hacking Phones with IE

- Phones are standard IP devices
 - HTTP, Telnet, SNMP
- There are vulnerabilities in these devices
- Password security

- Hacker scans the Internet looking for vulnerable phones
- Hacker then uses the phones to call 0900 numbers which she gets paid for



Demo



Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://10.10.10.66/

D-Link
Building Networks for People

Prompt

Enter username and password for "VoIP Gateway" at http://10.10.10.66


User Name:
[]

Password:
[]

Use Password Manager to remember this password.

OK Cancel

Waiting for 10.10.10.66...



D-Link DVG-1120S

- Config IP
- Device Information
- Proxy DNS
- Telephony Configuration
 - SIP Configuration
 - Server
 - User Agent
 - Peer to Peer
 - ACR Configuration
 - IP Filter
 - Routing
 - Bridge Mode
 - DHCP Configuration
 - NAT Configuration
 - SNMP Trap Configuration
 - SNMP IP Management Addr
 - Administration Management
- Monitor
- Firmware Update
- Factory Reset
- Save & Restart System

SIP Configuration - Server

Server FQDN	disabled
IP Address	192 . 168 . 0 . 4
Domain Name	
Port	5060
Service Domain	
URL Format	SIP-URL
User Parameter Phone	disabled
Timer T2	4 sec

Initial Unregister	enabled
Register Mode	CA_register
Register Expiration	3600 sec
Session Expires	180 sec
Min-SE	180 sec
Session Expires Refresher	uac

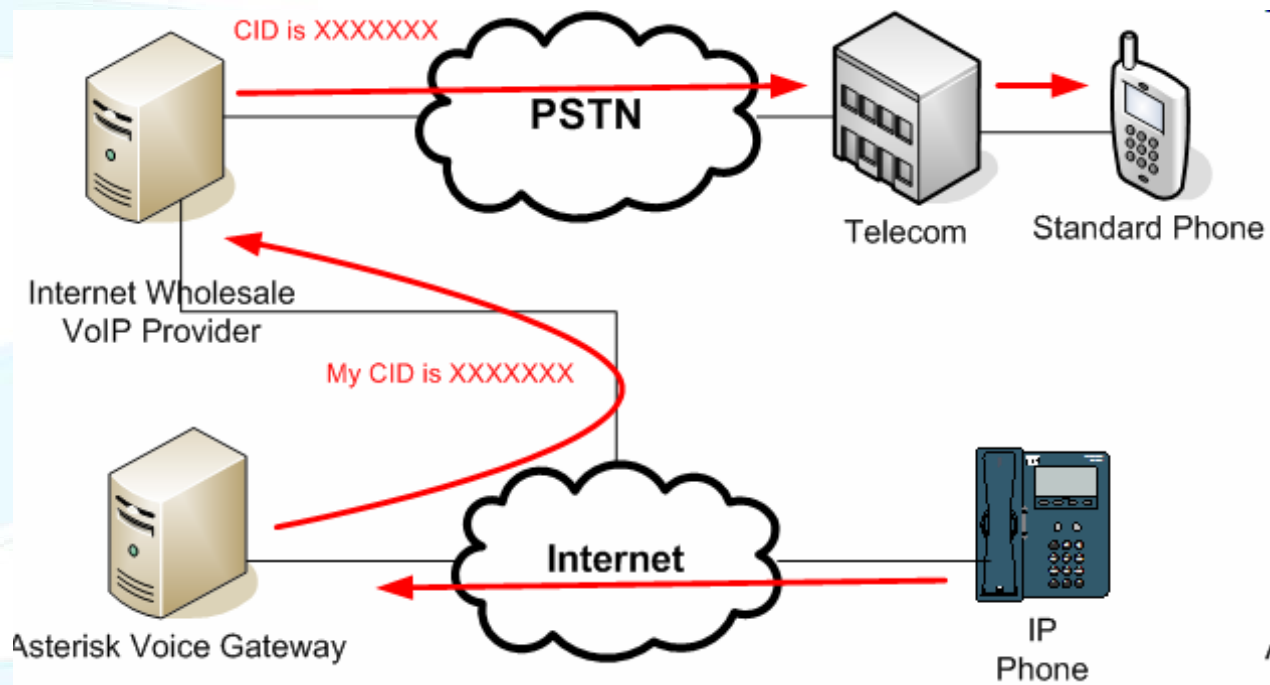
Codec Priority & Packet Interval			
G.711a-law	no-use	20	ms
G.711u-law	1st	20	ms
G.723.1	no-use	30	ms

Scenario 5 - Caller ID Spoofing

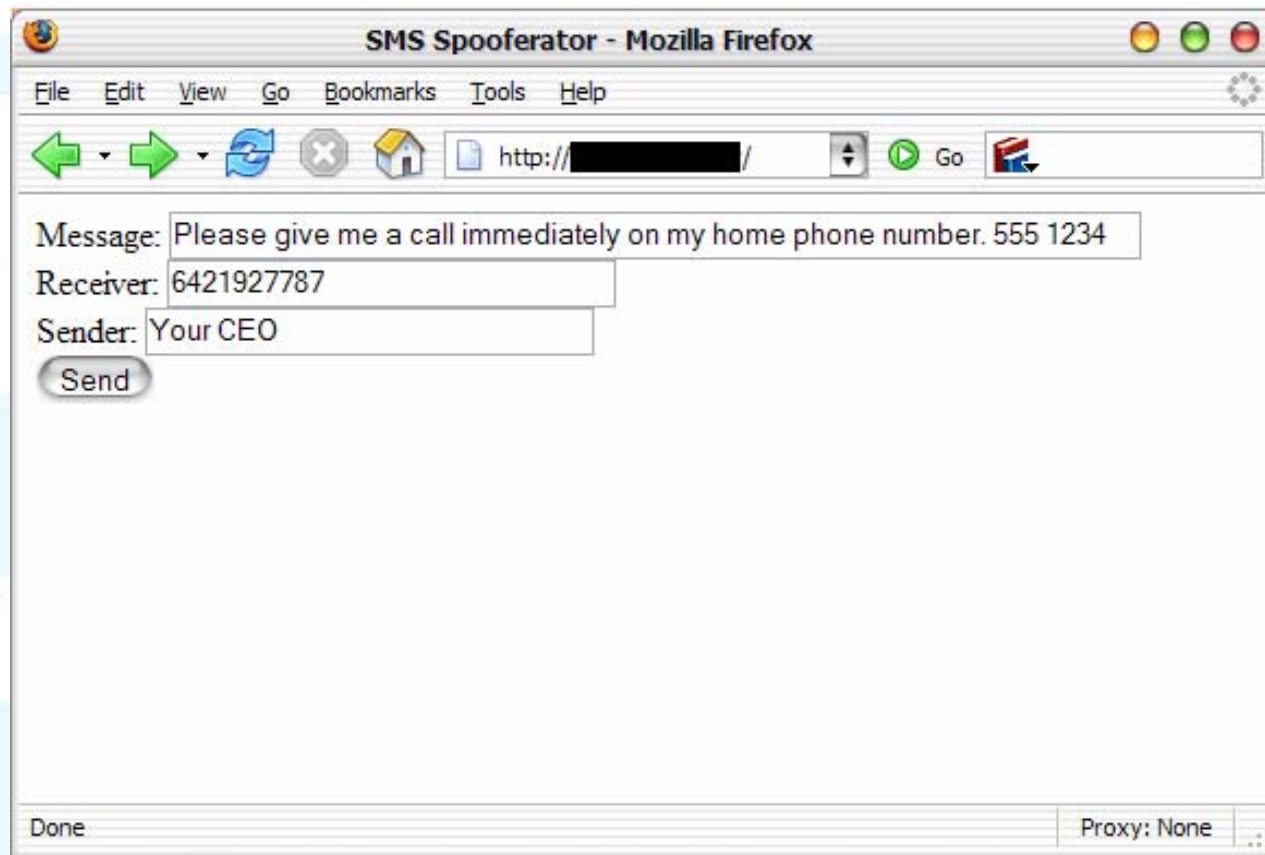
- While most good systems have changed, CID is still used as authentication
- Do you respond differently to internal calls?
- Call the helpdesk from the CIO's cell phone



Caller ID Demo



SMS Spoofing



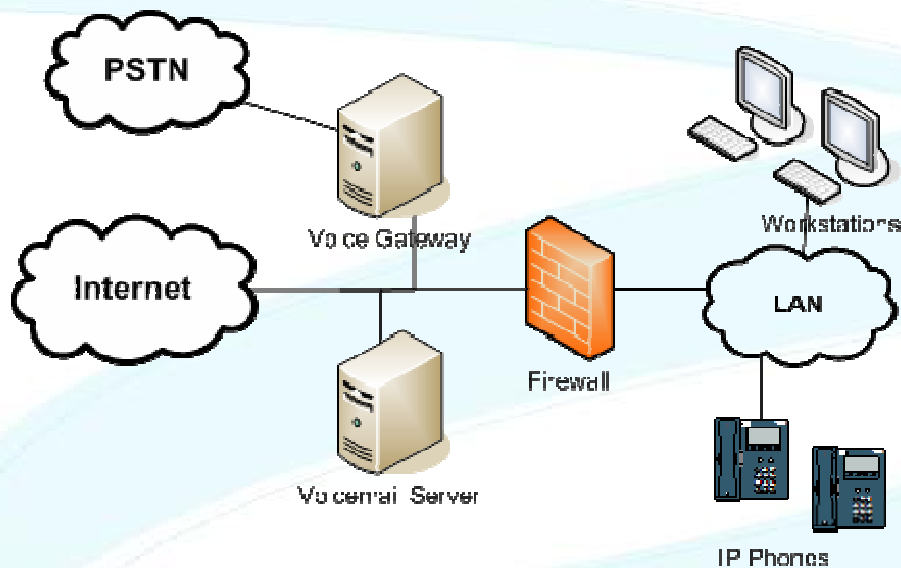
Okay... So How Do We Secure It?

- **Secure the Devices**
- **Network Segregation**
- **Encrypt the Traffic**
- **Intrusion Detection**



Secure the Devices

Secure the Devices



- Don't expose anything to the Internet that doesn't need to be!
- Patch and secure VoIP servers
- Patch phones
- Train your telephony staff in security practice

- This is a really bad idea!



Got Patches?

- **July 12 2005 - Cisco CallManager 3.3 and earlier, 4.0, and 4.1 are vulnerable to DoS attacks, and or arbitrary code being executed.**
- **July 7 2005 – Multiple vendor weakness in SIP Notify handling. Denial of Service (DoS)**
- **March 23 2005 – Grandstream BudgeTone DoS**
- **March 8 2005 – Ustar ATA remote access vulnerability**

- **Has the vendor had independent security testing done?**



Network Segregation

Threats to the LAN

- CAM Overflow
- ARP Poisoning
- VLAN Hopping
- Spanning Tree Attacks
- DHCP Rogue Server
- DHCP Starvation
- CDP Attacks
- HSRP Attacks

Layer 2 is a dangerous place to live!!!



Network Segregation

Problem: Malicious devices can sniff voice traffic



Use switches



Hacker can use ARP redirection or MAC overflow to turn switch into HUB



Use separate Voice and Data VLANS – Management overhead



Put a HUB in the phone



Now we can't VLAN



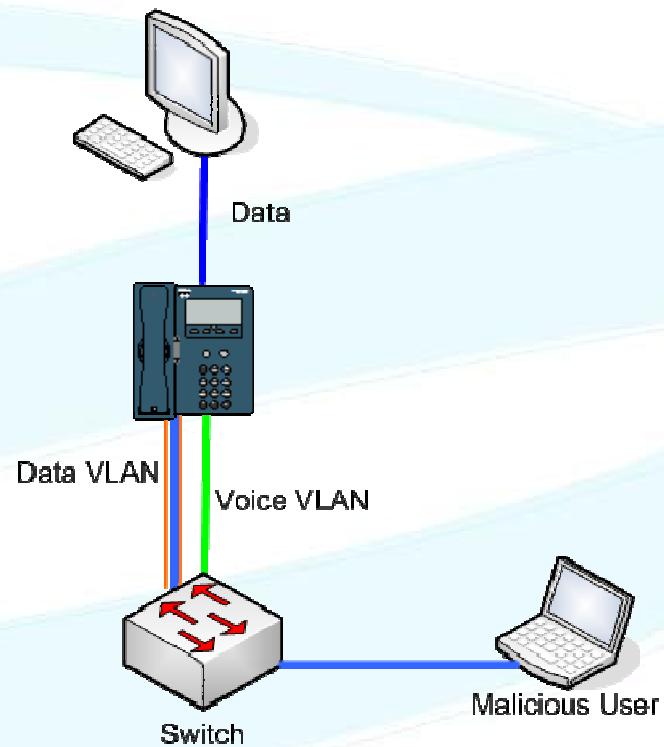
Make phone smarter, teach it about VLAN's



Hacker can now attack any VLAN from his phone port. But safe from remote attackers



Network Segregation



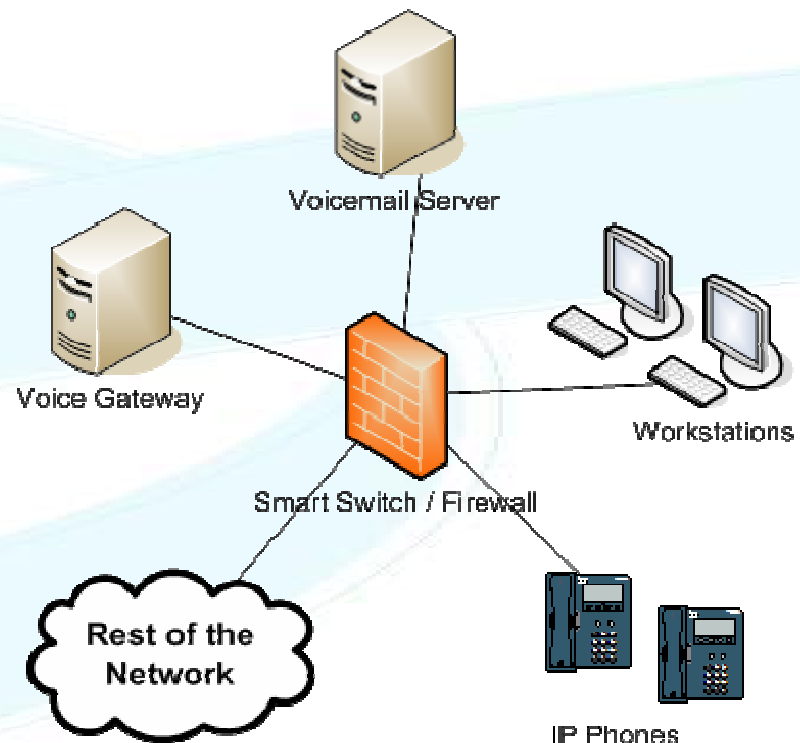
Network Segregation

- Try to stop malicious connections to your network
 - Disable switch ports not in use
 - Restrict access to switch by MAC address
 - Implement Sticky MAC
- All have management overhead and are not really secure



Network Segregation

- SIP Firewalls
- Firewalls, Routers and Smart Switches
- Use Voice VLAN
- Implement VLANs securely!
- Only allow the required traffic from one interface to another
- Reduce DoS risk
- Integrated solutions eg Cisco



Encrypt the Traffic

Encrypt the Traffic

- **Wrap an insecure protocol in a secure one**
 - **IPSEC**
 - **Other VPN**
- **Use a secure protocol**
 - **Secure Call Setup eg SIP TLS**
 - **SRTP – Cisco designed protocol for encrypting RTP traffic**



SRTP - Secure Real-time Transport Protocol

- **RTP/RTCP extension**
- **End to End**
- **Designed by Cisco**
- **IETF RFC 3711**
- **Adds**
 - **Confidentiality (AES128)**
 - **Message authentication (HMAC-SHA1)**
 - **Replay protection**
- **Doesn't effect compression or QoS**
- **Scales well**



Encryption Requires Authentication

- **SRTP Does not define authentication**
 - Pre Shared Keys
 - Custom SIP headers
 - MIKEY (Multimedia Internet KEYing)
 - Certificates preloaded on phones



SRTP – Can I Use It?

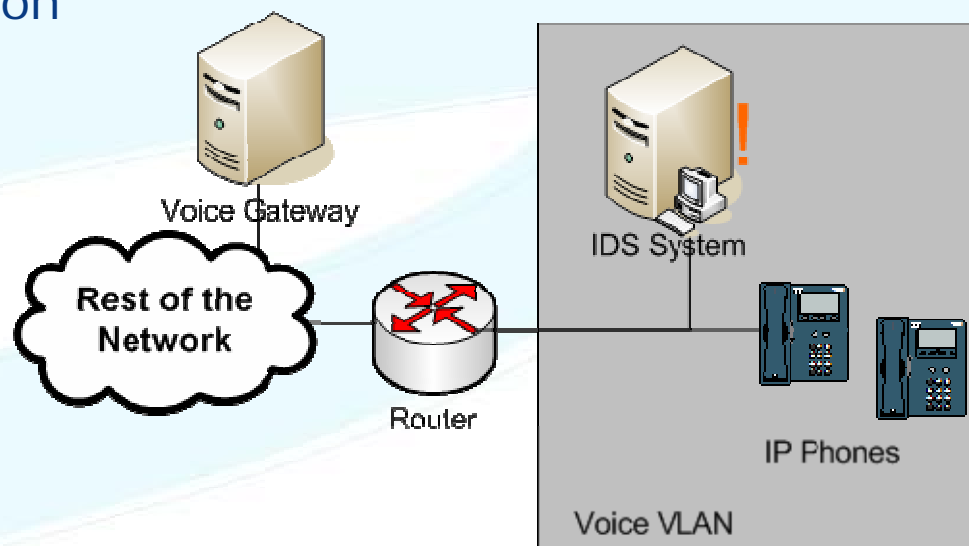
- **Currently known support by Sipura, Zultys, Avaya and Cisco**
- **Cisco support on Call Manager 4.0**
- **Currently only high end phones 7940, 7960 and 7970**



Intrusion Detection

Intrusion Detection

- Benefits of VLAN
 - IDS monitoring can be accurate
 - Very limited traffic on the network
- ARP Inspection at a minimum



Securing VoIP Summary

- **Secure Phones and Management Devices**
- **Segregate your network using VLANs and firewalls**
- **Only buy devices that support SRTP and push your vendors for support**
- **Use Intrusion Detection where possible**
- **Consider VoIP security overhead before deciding**



Good Sites For Learning More

- Some good links for learning more about VoIP
 - Voip-Info.org <http://www.voip-info.org>
 - VoP Security <http://www.vopsecurity.org>
 - Cain and Abel <http://www.oxid.it>
 - Vomit <http://vomit.xtdnet.nl/>
 - VoipSA <http://www.voipsa.org>

Questions?

darren@security-assessment.com