Voice over IP

What You Don't Know Can Hurt You

by Darren Bilby

security-assessment.com

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

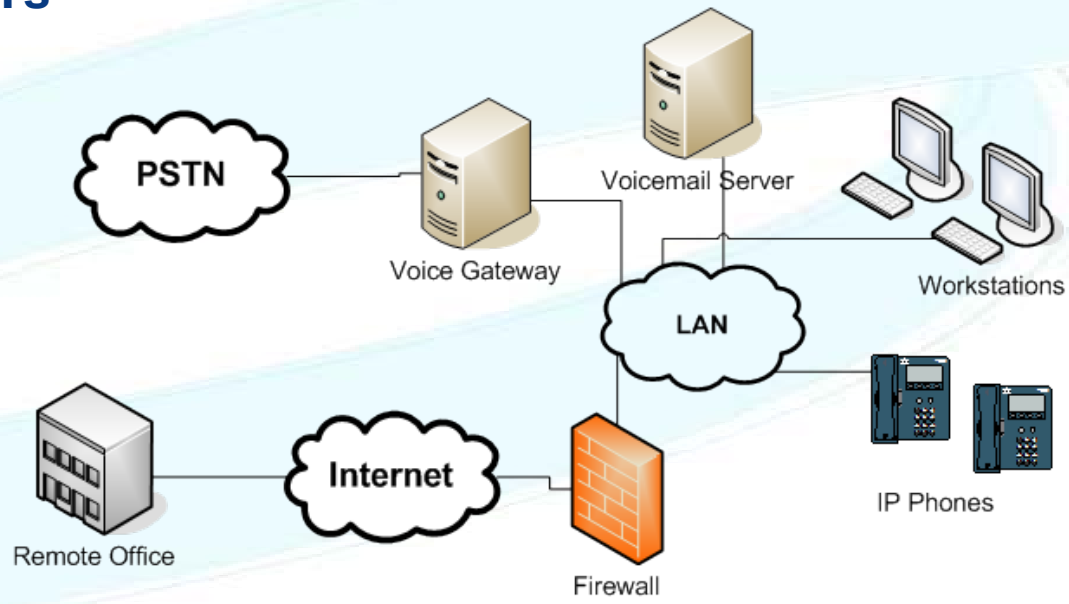
- VOIP becoming more popular and will increase in future
- Many ISPs and Telco's starting to offer VoIP services
- Like most other phone calls, it is presumed to be confidential
- Designed by telephone people with trusted networks in mind

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, Proxies, Management Servers



VoIP Clients

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

Protocols and Acronyms

security-assessment.com

Protocols and Acronyms

- Signaling Protocol
  - Create, modify, and terminate sessions with participants
  - Conferences
  - Proxies
  - Authentication

- Transport Protocol
  - Actually sends the 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?

- Pranks
- Eavesdropping and Recording Phone Calls
- Track Calls
- Stealing Confidential Information
- Modifying Phone Calls
- Making Free Phone Calls
- Board Room Bugging
- Sending Spam

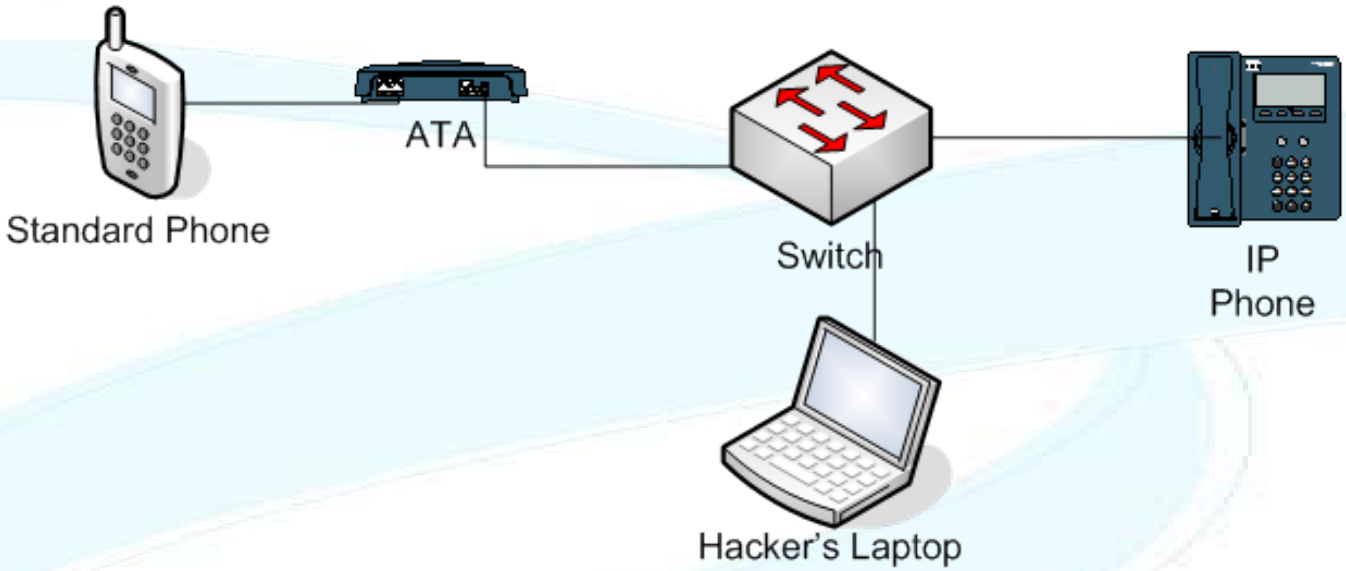
VoIP Security Scenarios

security-assessment.com

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

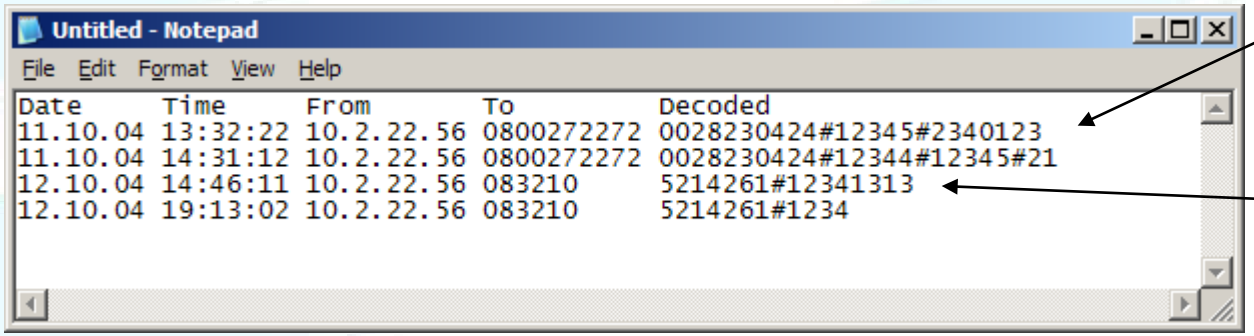
Demo



- **Cain**
  - **http://www.oxid.it/**
- **Voice over Misconfigured IP Telephony (Vomit)**
  - **http://vomit.xtdnet.nl/**

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



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

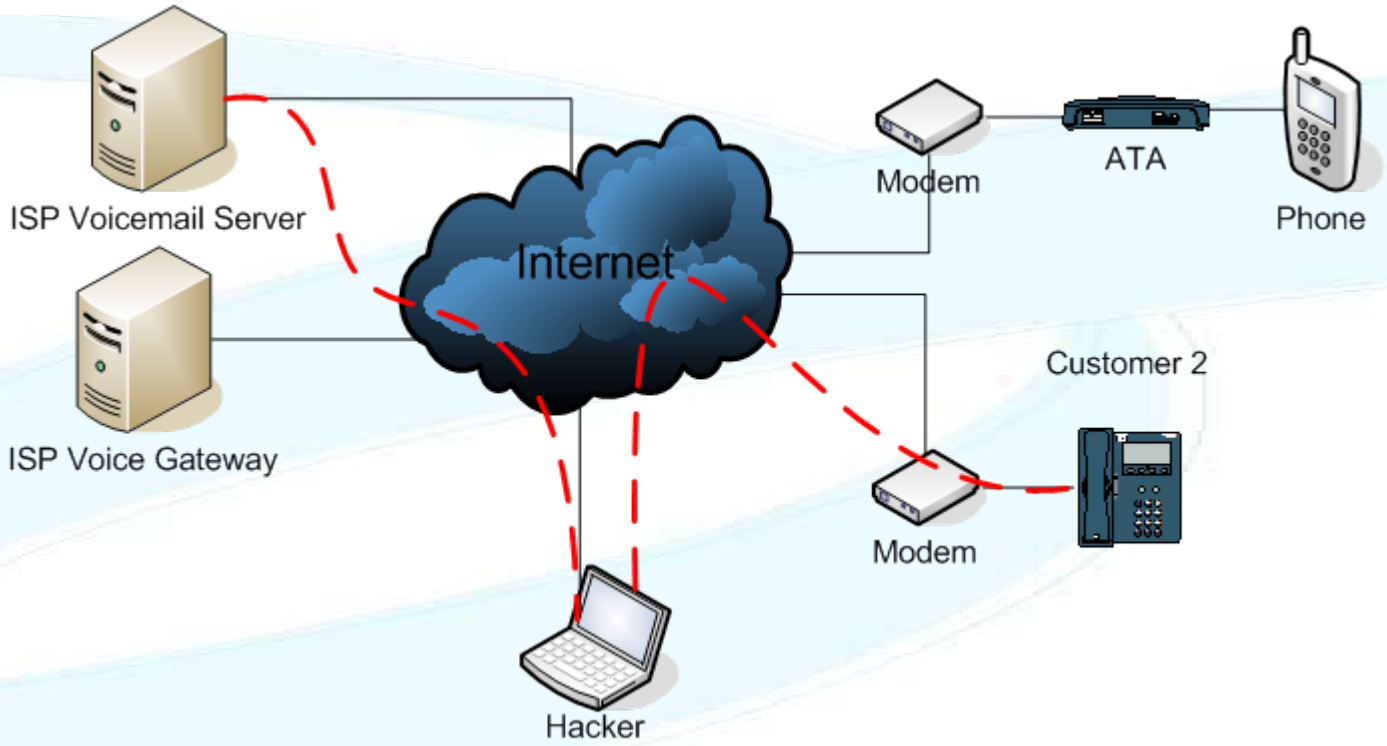
- Evil Russian hacker is hired by a competitor to gain knowledge of business strategies.
- Hacker sends secretary a link to FunnyGame.exe, pretending to be an associate.
- Hacker sets boardroom IP phone in speakerphone mode, and calls a phone he controls thus recording boardroom meetings.

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



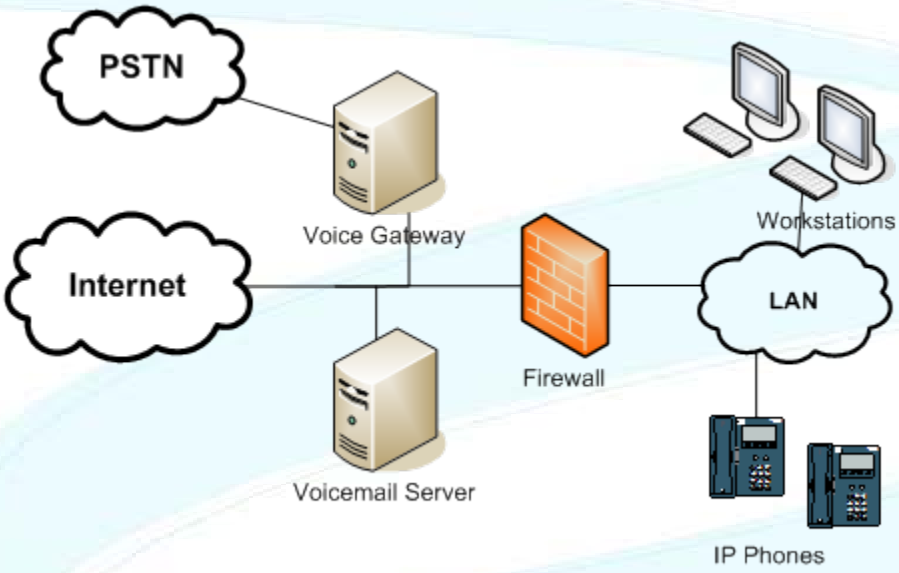
Okay… So How Do We Secure It?

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

Secure the Devices

security-assessment.com

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!

Network Segregation

security-assessment.com

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

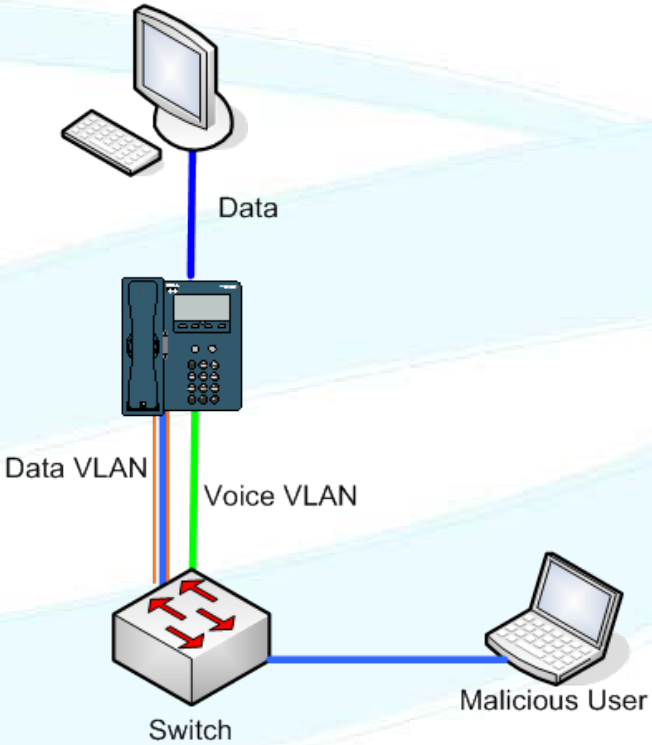
↓

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

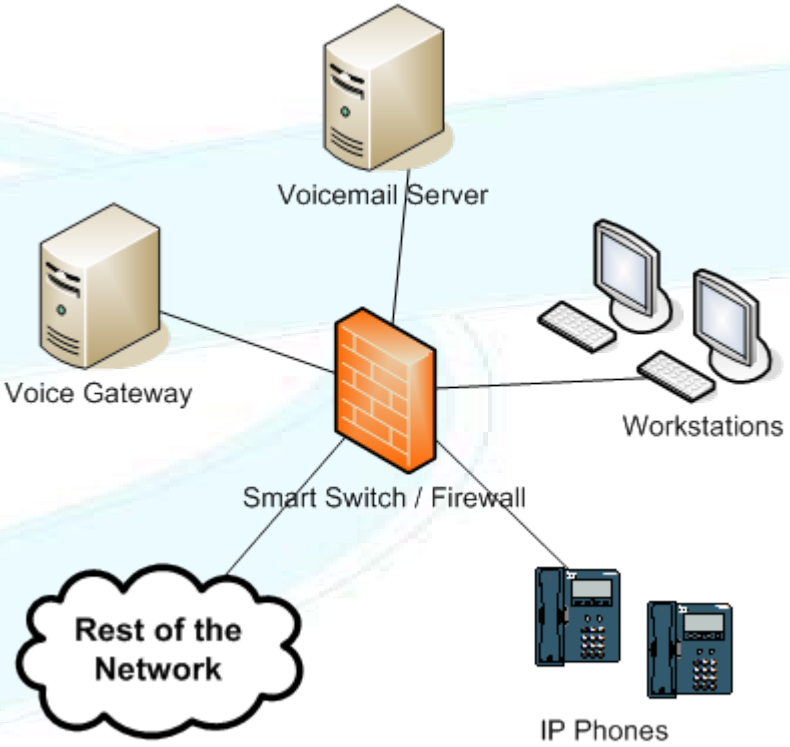
- Try to stop malicious connections to your network
  - Disable switch ports not in use
  - Restrict access to switch by MAC address
  - Implement Sticky MAC

- All have management overhead and are not really secure

Network Segregation

- Firewalls, Routers and Smart Switches
- Use Voice VLAN
- Only allow the required traffic from one interface to another
- Reduce DoS risk

- Integrated solutions eg Cisco



Encrypt the Traffic

security-assessment.com

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 <u>not</u> define authentication
  - Pre Shared Keys
  - Custom SIP headers
  - MIKEY (Multimedia Internet KEYing)
  - Certificates preloaded on phones

SRTP – Can I Use It?

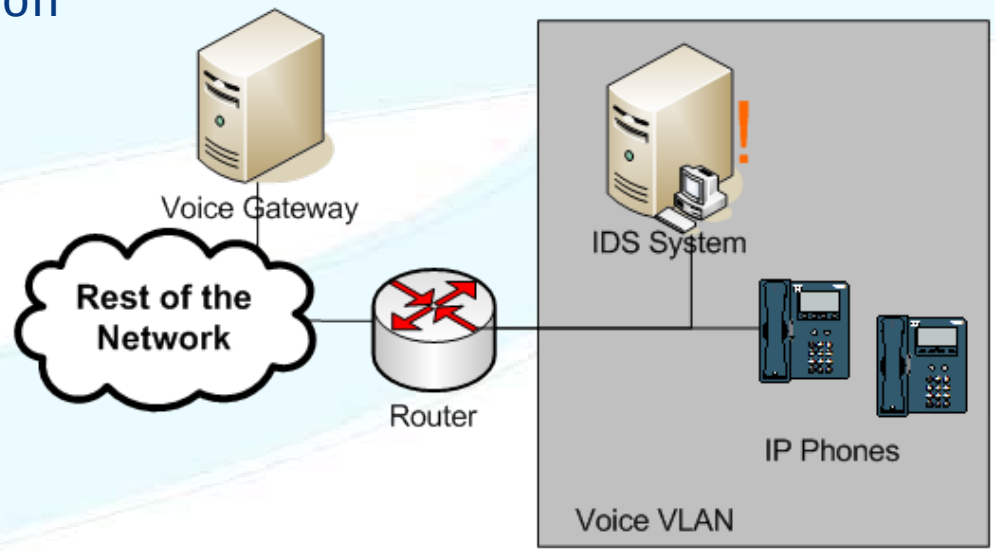
- Currently known support by Sipura, Zultys, Avaya and Cisco
- Cisco support on Call Manager 4.0
- Currently only high end phones 7940, 7960 and 7970

Intrusion Detection

security-assessment.com

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

Other VoIP Issues

security-assessment.com

Other VoIP Issues - Caller ID Spoofing

- **CID is often used for authentication**
  - **Voicemail systems**
- **Makes social engineering a lot easier**

- **But, high barrier to entry:**
  - **Access to direct connection with Telco eg E1**
  - **Access to misconfigured VoIP provider**
- **Multiple companies are now offering caller ID spoofing:**

- CovertCall	- PI Phone
- Star38	- Us Tracers
- Camophone	- Telespoof

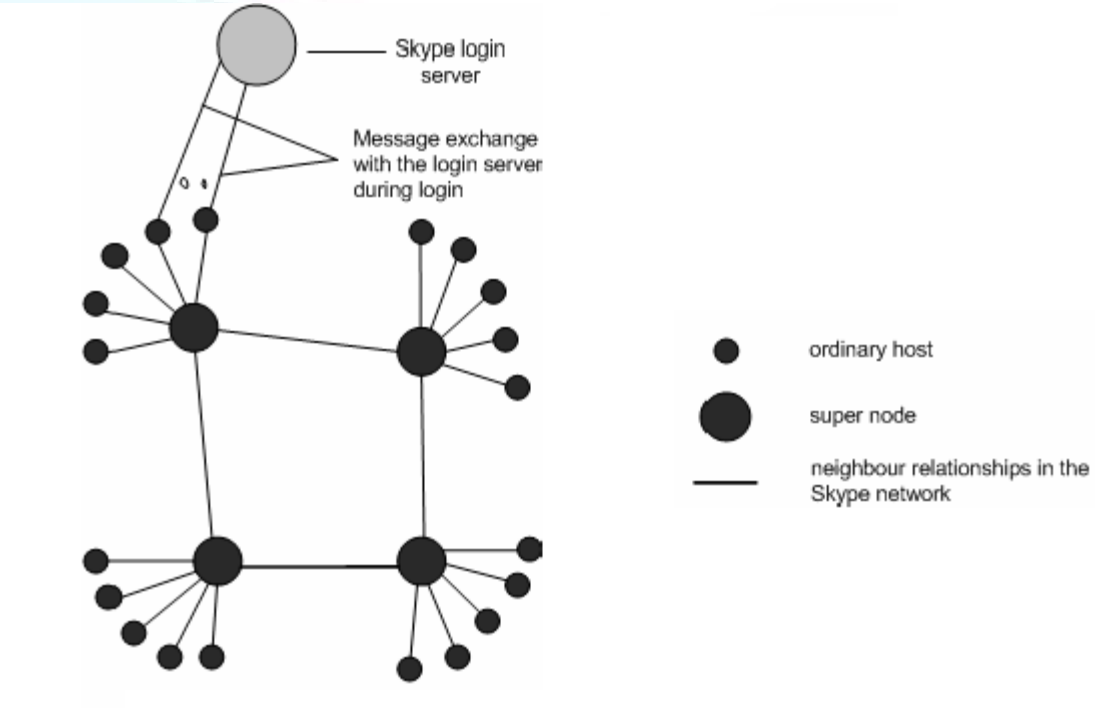
Skype

security-assessment.com

Other VoIP Issues - Skype

- Proprietary VOIP system for calls over the Internet
- Free and simple to use
- Developed by the creators of KaZaA
- NAT and Firewall traversal
- File transfer

Other VoIP Issues - Skype



Ref: "An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol“
Salman A. Baset and Henning Schulzrinne

Skype Security Concerns

- Claims AES 128bit encryption - unverifiable
- Skype may have the ability to decrypt all voice traffic
- Same developers as KaZaA, known for spyware
- Cannot stop client becoming a Supernode
- Client allows file transfer, even through firewalls, an access path for malicious code, information leakage
- Client can update itself automatically

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/