

VoIP Security Issues: a review

Peter Cox
CEO UM Labs Ltd
peter@um-labs.com

September 2009

Agenda

- About the speaker
- Some definitions
- 3 minute introduction to VoIP
- VoIP Threat Taxonomy
- Real-life examples
- Vendor comparisons
- Detecting attacks
- Addressing the problem
- Questions and answers





Peter Cox

- Founder and CEO of UM Labs Ltd
 - Developer of VoIP Security and encryption products
 - Regular speaker on VoIP Security Topics
 - In-depth VoIP Security Workshops
- Co-founder of Borderware Technologies Inc
- 25 Years experience in Internet protocols and security



Some Definitions

- Voice over IP (VoIP)
 - Voice and video telephony over IP networks
 - Corporate grade service (excludes interpersonal services such as Skype)
 - Standards based or proprietary
- Signalling Protocols
 - Protocols responsible for call setup and related functions
- Media Protocols
 - Protocol responsible for transporting voice or video stream



The growth of VoIP

- Most Voice over IP (VoIP) systems start as replacements for legacy phone systems
- Virtually all corporate telephony products are built on VoIP

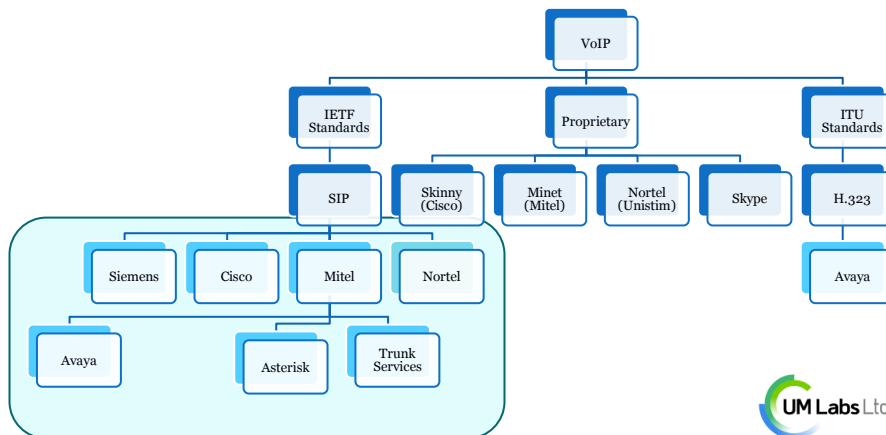
| | |
|---------|---------|
| Avaya | Mitel |
| Alcatel | Nortel |
| Cisco | Siemens |
| Etc.... | |

- VoIP offers much more than any legacy phone system



VoIP Protocol Family tree

- Signalling Protocols



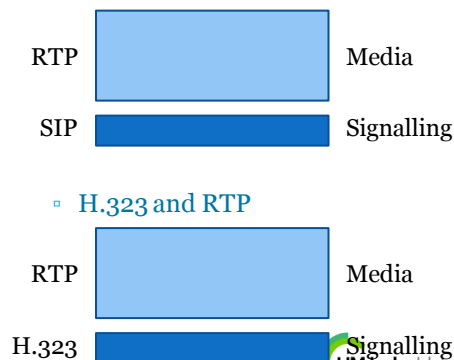
Signalling and Media

- Standard phone systems (TDM) separate signalling and media
- Basic rate ISDN lines provide “2B+D” (2 x 64K “bearer” channels 1 x 16K “delta” channel)
- B channels carry media (2 voice calls on a standard basic rate ISDN)
- D channel carries signalling
 - Call setup
 - Call termination
 - Management functions



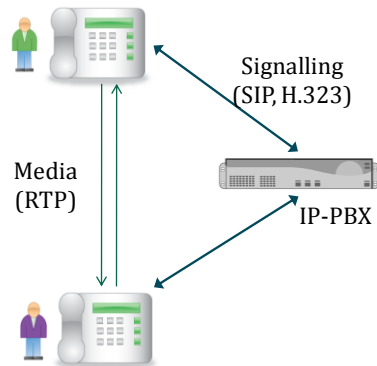
VoIP continue the Signalling Media Split

- TDM uses channel separation
 - e.g. ISDN Basic Rate
- VoIP uses protocol separation
 - SIP and RTP
 - H.323 and RTP



IP Infrastructure exploits Media Signalling Separation

- Signalling and Media *may* follow different Network paths
- Signalling always flows via the IP-PBX
- Media options:
 - Peer to Peer
 - Via PBX
 - Via some other device
- Advantage: Significantly shorter media path, better voice quality, lower network loads
- Disadvantages: Significant security challenges



VoIP Threat Taxonomy

Content

- Threats affecting VoIP Content
- Call monitoring & eavesdropping
- Unwanted calls

Application

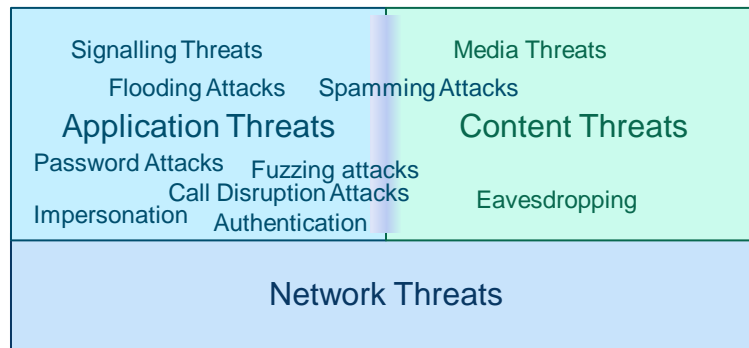
- Threats against protocols & applications
- Flooding attacks
- Call disruption attacks

IP Network

- IP Network level threats common to all network applications



VoIP Threat Classification



SIP Security Threats

| Threat | Potential Impact | Scope |
|-----------------------|---|------------------------|
| Registration Flood | Service degradation, complete loss of service | Entire System |
| Deregistration Attack | Service loss | Targeted phones |
| Call Flooding | Service degradation, user irritation | Targeted phones |
| Call Disruption | Calls terminated, calls can't complete | Targeted phones |
| Unauthorised calls | Toll fraud | Entire system |
| Call Hijacking | Calls re-directed, direct financial loss | Targeted calls |
| Protocol misuse | Failure of targeted devices | Any targeted component |

- These threats are *not* addressed by standard Firewall technologies



Content Threats

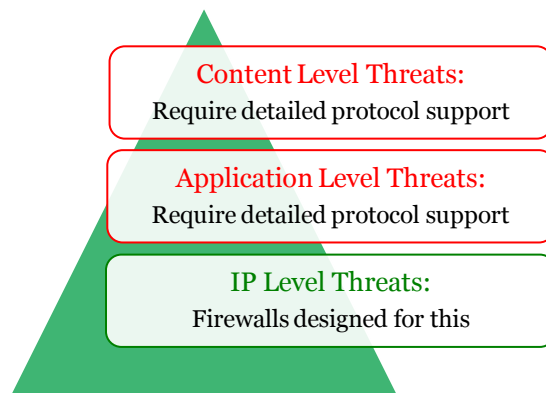
| Threat | Potential Impact | Scope |
|---------------------------------|--|----------------|
| Unauthorised call monitoring | Loss of confidentiality, direct financial loss | Entire System |
| RTP Injection (replacing media) | Loss of confidentiality, direct financial loss | Targeted calls |
| Unwanted calls (VoIP Spam) | Service degradation, user irritation | Entire system |

- These threats are *not* addressed by standard Firewall technologies



Limitations of Standard Security Technologies

- Standard (general purpose) Firewalls do not address the complete set of security threats



SIP Registration

- REGISTER requests associate a phone's network identity with a name or number
- Enables the PBX to route calls
- **Optionally** authenticates the phone
- REGISTER requests can originate from anywhere
- Many attack options



REGISTER Request

```
REGISTER sip:voipcode.org SIP/2.0
Via: SIP/2.0/UDP 192.168.19.12:5060;branch=z9hG4bK1d1bc13a8c075154cde
Max-Forwards: 70
To: <sip:fred@voipcode.org>
From: <sip:fred@voipcode.org>;tag=1916793
Call-ID: SL-tpucghjy-41543ff7@192.168.19.12
CSeq: 10131 REGISTER
Expires: 3600
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER
Contact: <sip:fred@192.168.19.12>
User-Agent: SIP Library: Unix V1.1 Build: May 14 2007, 17:44:30
Content-Length: 0
```



De-Registration Attacks

- REGISTER requests include an expiry
- Lifetime in seconds or registration
- Phone must re-register before that time

```
REGISTER sip:voipcode.org SIP/2.0
Via: SIP/2.0/UDP 172.16.60.2:5060;branch=z9hG4bK21c623c10ac3ce23bb2
Max-Forwards: 70
To: <sip:3123@voipcode.org>
From: <sip:3123@voipcode.org>;tag=2221664
Call-ID: SL-lncmphna-434bb7fb@172.16.60.2
CSeq: 16606 REGISTER
Expires: 3600
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER
Contact: <sip:3123@172.16.60.2>
User-Agent: SIP Library: Solaris V1.1 Build: May 29 2007, 16:04:39
Content-Length: 0
```

De-registration

- A phone can de-register by setting expiry to zero
- Informs the PBX that phone is unavailable
- No calls will be routed to that device
 - Useful when a soft-phone is shutdown

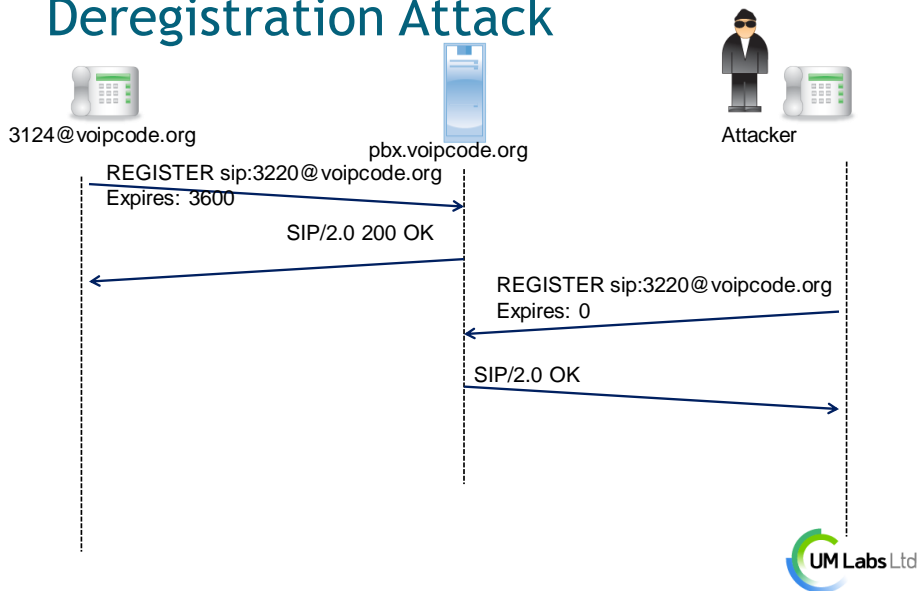
```
REGISTER sip:voipcode.org SIP/2.0
Via: SIP/2.0/UDP 172.16.60.2:5060;branch=z9hG4bK21c623c10ac3ce23bb2
Max-Forwards: 70
To: <sip:3123@voipcode.org>
From: <sip:3123@voipcode.org>;tag=2221664
Call-ID: SL-lncmphna-434bb7fb@172.16.60.2
CSeq: 16606 REGISTER
Expires: 0
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER
Contact: <sip:3123@172.16.60.2>
User-Agent: SIP Library: Solaris V1.1 Build: May 29 2007, 16:04:39
Content-Length: 0
```

De-Registration Attack

- Most SIP application servers or PBXs do not check the source of a registration
- Attacker can fake a De-registration
- Needs only user name/number and domain



Deregistration Attack



VoIP Authentication

- The SIP standard (RFC 3261) defines an *optional* authentication service
- Many implementers (and some vendors) do not understand its importance
- Many SIP installations have incomplete or no authentication

- Problem not limited to SIP
- Nortel CS1000 installations running Unistim do not authenticate phones

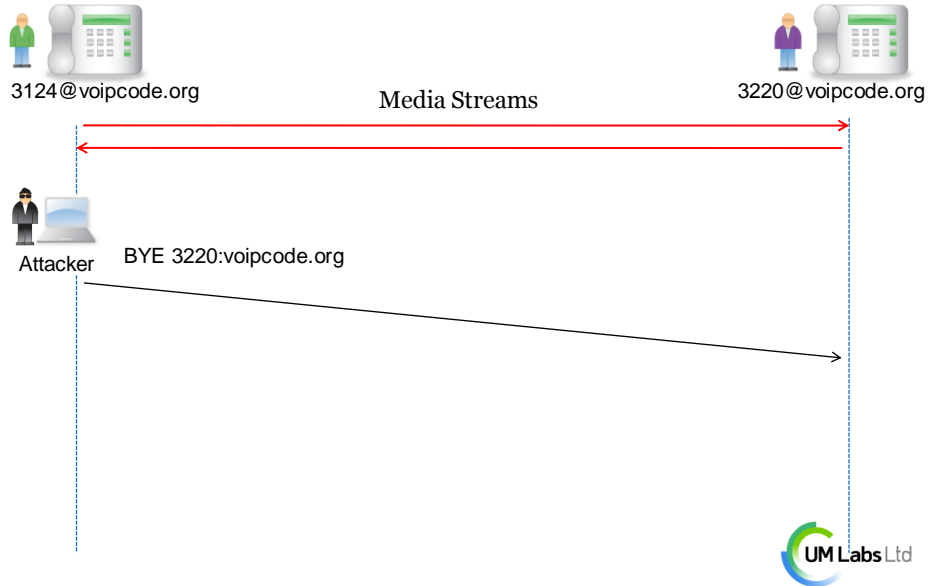


SIP BYE

- SIP BYE request terminates an active call
- Normally sent by 1st phone to hang up at end of call
- May be sent by PBX
- Attackers can misuse BYE to terminate calls



Call Termination Attack



Dissecting a Bye Attack (1)

- Call from PBX to Extension 3220



▫ Normal Termination

```

BYE sip:413@192.168.4.75:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.4.28:5060;branch=z9hG4bK28107c34;rport
From: "Sales Desk" <sip:3124@192.168.4.28>;tag=as466c284f
To: <sip:3220@192.168.4.8:5060>;tag=4ab274367f880505i0
Call-ID: 456e14f3615c4fa714a164920de4702a@192.168.4.28
CSeq: 103 BYE
User-Agent: Branch Office PBX
Max-Forwards: 70
Content-Length: 0
  
```

Dissecting a Bye Attack (2)

- Call from PBX to Extension 413



▫ BYE Attack

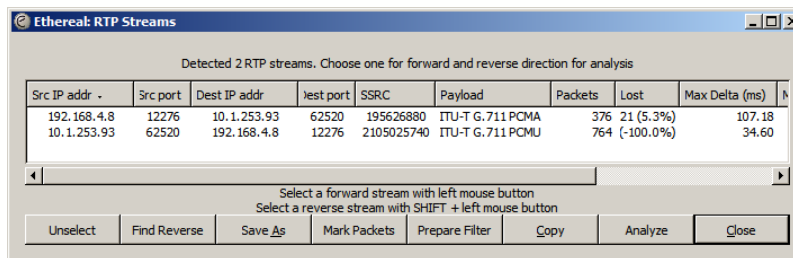
```

BYE sip:victim@1.2.3.4 SIP/2.0
Via: SIP/2.0/UDP 192.168.4.28:5060;branch=z9hG4bK3028e41a
Max-Forwards: 70
To: <sip:123@random.com>
From: <sip:attacker@hostile.org>;tag=e0ae24c56f1952bf10
Call-ID: 26adb57535734f41413514ac09fc043d@192.168.4.28
CSeq: 102 BYE
Expires: 240
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER
Contact: <sip:456@6.7.8.9>
Content-Length: 0
  
```

psLtd

Eavesdropping / Unlawful Monitoring

- Monitor and record the call...
 - The old fashioned way using packet sniffers and other tools:



Eavesdropping / Unlawful Monitoring

- Monitor and record the call...
 - The easy way, point and click wire-tapping from anywhere on the net....
 - See <http://siptap.voipcode.org>

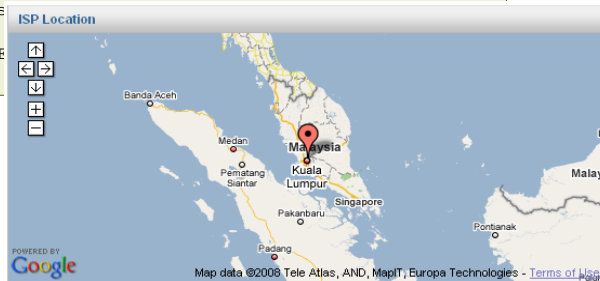
| Time | Caller | Recipient | Call ID | Duration (secs) | Audio Stream | Status |
|-----------------|---------------------------------|---------------------------------|--|-----------------|--------------|--------|
| Sep 09 12:13:02 | sip:401@sip-services-europe.com | sip:202@sip-services-europe.com | b04bdabd1245de1e@192.168.19.30 | 7 | Play | N |
| Sep 09 12:14:02 | sip:401@172.16.60.3 | sip:904@mouselike.org | 664f78ac3d3754832d41027d279d0e1c@172.16.60.3 | 15 | Play | N |
| Sep 09 12:14:43 | sip:401@sip-services-europe.com | sip:214@sip-services-europe.com | 4b3b0bda153344e@192.168.19.30 | 647 | Play | N |
| Sep 09 12:14:43 | sip:401@sip-services-europe.com | sip:202@sip-services-europe.com | f389acfeb8250c92@192.168.19.30 | 8 | Play | N |

Are the threats real?

- UM Labs Systems regularly targeted by attackers attempting to make calls to PSTN
- No Authorisation for these calls
- Toll-Fraud, mostly to UK numbers
- Attackers are obviously:
 - Scanning the Internet for VoIP Systems
 - Identifying location of those systems
 - Targeting numbers that are likely to succeed

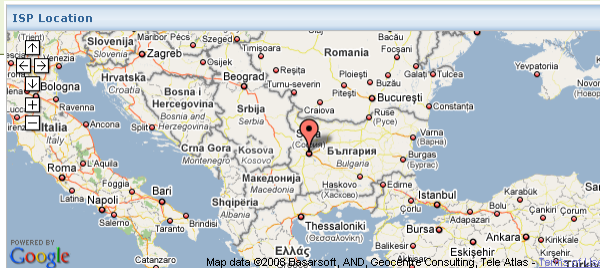
Toll Fraud Example

```
Dec 03 01:54:32 962 bytes received from 124.217.230.238:29848 via TCP
INVITE sip:525551690000@217.154.219.168 SIP/2.0
Via: SIP/2.0/TCP
124.217.230.238;branch=1110001001100110010010000000111
Max-Forwards: 100
From: <sip:5199362832664@217.154.219.168>;tag=36270123734
To: <sip:525551690000@217.154.219.168>
Call-ID: ef85a02b11110010111000001010011111011100
CSeq: 1 INVITE
Contact: <sip:c444cf@124.217.230.238>
Content-Type: application/sdp
Content-Length: 200
Allow: ACK, BYE, CANCEL, MESSAGE
User-Agent: X-Lite release
```



Probe for Information

```
Dec 10 21:15:14 401 bytes received from 213.130.74.72:5060 via UDP
OPTIONS sip:100@217.154.219.168 SIP/2.0
Via: SIP/2.0/UDP 127.0.0.1:5060;branch=z9hG4bK-2461510689;rport
Content-Length: 0
From: "114"<sip:114@1.1.1.1>; tag=6439396164626138313363340131313035343232343138
Accept: application/sdp
User-Agent: Auidocodes-Sip-Gateway
To: "114"<sip:114@1.1.1.1>
Contact: sip:100@127.0.0.1:5060
CSeq: 1 OPTIONS
Call-ID: 632046747554930111593954
Max-Forwards: 70
```



Threats have a high potential cost

VoIP toll fraud attack racks up a \$82K bill in two days

A recent report from the Australian press relates the story of a Perth company where hackers made 11,000 calls via the company's VoIP running up a bill of AU\$ 120,000 (\$82,500) . This figure ranks this incident among the most expensive of documented toll-fraud attacks.

<http://tinyurl.com/a9qjb9>

INVITE of death, does this spell doom for VoIP?

The last couple of weeks have seen two significant VoIP vulnerability reports.

The second vulnerability, with the comparatively mundane name of SIP Digest authentication relay attack, is technically much more complex. An attacker could use this technique to make calls via a commercial service provider at the victim's expense.

<http://tinyurl.com/byq3mj>

Further Information on VoIP Security Threats

UM Labs Website

- www.um-labs.com

VoIP Threats Podcast

- 10 minute demo of common threats
- www.tinyurl.com/2s42jr

UM Labs workshops

- One-day review
- Two-day in-depth workshop



Vendor Comparison

CISCO SUBNET The independent voice of Cisco customers

NetworkWorld.com > Community > Brad Reese on Cisco

Log in Post Register

Search Community / blogs: Search

Outrageously shocking: More than 100 Cisco, Avaya and Nortel VoIP security holes discovered

Submitted by [Brad Reese](#) on Wed, 04/02/2008 - 7:54pm.

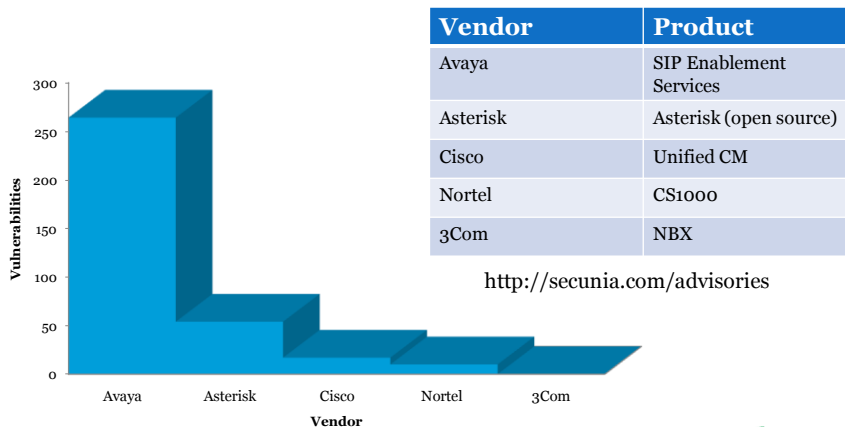
It is **shocking and outrageous** that there are more than **100 security holes** in VoIP products from Cisco, Avaya and Nortel.

The flaws were discovered by VoIP security solutions vendor [VoIPshield](#), which revealed the vulnerabilities to the public today.

<http://www.networkworld.com/community/node/26574>



Vendor Comparison: Total Secunia Vulnerabilities



Detecting Attacks

Easy to detect attacks

- Registration flooding
- Call flooding
- Call Termination attacks
- Denial of service attacks
- RTP Injection attacks

Stealth attacks

- Call eavesdropping
- Toll fraud (until you get the bill)

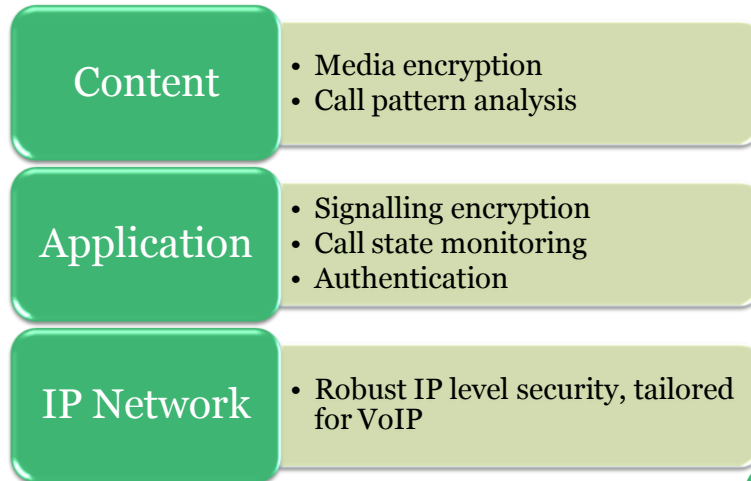


Countering the threats

- Countering VoIP threats requires specialist security controls
 - Complexity of VoIP applications and protocols
 - Impact of identified threats
 - Broad scope of applications
- These controls are beyond the scope of standard security products (firewalls)
- Controls require a specialist security gateway



Designing a VoIP Security Gateway

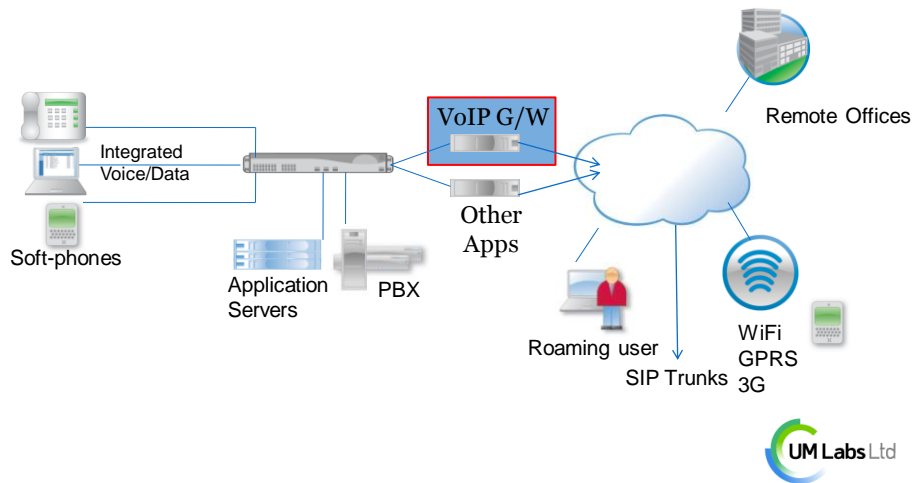


Media and Signalling Encryption Options

- **SDES/SRTP**
 - Built in as standard
 - Secures calls to remote users and “private trunks”
 - Supported by hardware phones (e.g. snom) and softphones (e.g. Counterpath)
- **ZRTP**
 - Designed by Phil Zimmermann
 - Secures calls to remote users
 - Key exchange over media stream
 - Supported for softphones and on a wide range of cell phones



Deploying VoIP Security



Conclusions

- VoIP's popularity is growing
 - Greater flexibility
 - New services
 - Reduced costs
- Voice communication is part of *critical infrastructure*
- Too many organisations ignore or are unaware of the security issues
- No one would run an email or web service without adequate security controls, many VoIP systems lack these



About UM Labs

- **Products**
 - EC4200 and RC2100 SIP Security Controllers
 - SIP Security Gateways ranging from small office to large enterprise
- **Consultancy and Training**
 - VoIP and UM Security Audits
 - Security Workshops
- **Contact**
 - Phone: +44 20 3021 3200
 - VoIP: sip:info@um-labs.com
 - Email: info@um-labs.com
 - Web: www.um-labs.com

