NGN Architectures, VoIP Security and Protocols

UKNOF 5 25/10/06

Neil J. McRae – Director of Network Architecture
Nico Fischbach – Head of Network Security

COLT Telecom Group
Agenda

What is VoIP?
VoIP Architectures
VoIP Protocols & Security Concerns
Questions
COLT and VoIP

COLT Telecom
> Voice, Data and Managed Services, Tier 1 ISP in EU
> 14 countries, 60 cities, 50k business customers
> 20 000 km of fibre across Europe + DSL

VoIP “experience”
> 3 major vendor directions
  – One “we're coming from the TDM world”
  – One “we're coming from the IP world”
  – One “we're a VoIP company”

> Internet and MPLS VPN-based VoIP services
> Own network (fiber + DSL) and wDSL
> Going MSPP + VoIP NGN + IMS – TDM scaling issues
What is VoIP? The Customer Viewpoint

Computer with softclient (SIP or Skype)

Hardphone (analog or SIP or Skype)

Internet
Hosted IP PBX

POTS

VoIP/ToIP

PBX could be IP-enabled with IP phones on LAN

UKNOF 5 : NGN VoIP : Neil J. McRae
PBX Trunking over IP

TDM PSTN

Voice Switch

PRI (ISDN over E1)

PBX

VoIP/ToIP

Softswitch

MGCP

H.323(/MGCP)/RTP

No NAT

T.38 (FAX)

64kUR (PBX Mgmt)

POTS

VoIP/ToIP

MGW

RTP

FW

H.323(/MGCP)

DTMF

POTS

VoIP/ToIP

PBX

CPE

T.38 (FAX)

UKNOF 5 : NGN VoIP : Neil J. McRae
Softswitch: it combines the Call Control, the Signalling Gateway and the Media Gateway Control function. Together with the Media Gateway function it provides signalling and media inter-working with the legacy TDM voice network. The intelligence of the system (call control functionality) as well as the customer database resides within the softswitch function.

Session Border Control: it provides secure access control to the customer appliances and mediates between the COLT IMS and any 3rd party IP network.

Management and Provisioning: it is an integrated OSS platform that allows end to end provisioning and management across the technology components.
**Interworking with TDM Voice Network:** it provides signalling and media inter-working with the TDM voice network.

**Core SIP Call Control:** it is a set of SIP enabled devices that control the flow of SIP messages between the customer appliances (IP phones, soft phones, wireless handhelds) and the rest of the IMS components.

**Customer Profile Database:** it contains the user identity and the user service profile, providing session authentication and access to service applications.

**Session Border Control:** it provides secure access control to the customer appliances and mediates between the IMS and any 3rd party IP network.

**Application Layer:** it provides the service logic, with a set of Application Servers dedicated to specific services (e.g., an IP Centrex AS for telephony services, a Mobility AS for FMC integration, a Messaging AS for unified messaging and presence services).

**IMS Management and Provisioning:** it is an integrated OSS platform that allows end-to-end provisioning and management across the IMS technology components.
Softswitch Architecture – Logical Level

1. Direct VoIP Traffic
2. Indirect VoIP Traffic
3. Indirect TDM Traffic

- Media
- Signalling
- AA

3rd party TDM/SS7 Networks

3rd party IP Networks

COLT NGN Transport Network

UA

RTP

H.323 / SIP

MGW

H.323 / SIP

RTP Proxy

ALG

Session Border Control

Softswitch

Call Control

MGCF

Subscriber DB

Voice Apps

Application Layer

Legacy Apps

NGIN

User Agent

ALG Application Layer Gateway

MGW Media Gateway

MGCF Media Gateway Ctrl Function

SGW Signalling Gateway

NGIN Next Gen IN

ISUP

TDM

H.323 / SIP

UA

RTP

H.323 / SIP

RTP

H.323 / SIP
 IMS Architecture – Logical Level

1. Direct VoIP Traffic
2. Indirect VoIP Traffic
3. Indirect TDM Traffic

- Media
- Signalling
- AA

SMG Architecture with TDM Voice Network

SIP

AS

Diameter

Session Border Control

CSCF

Core SIP Call Control

HSS

Customer Profile Database

NGIN

Application Layer

3rd party TDM/SS7 Networks

3rd party IP Networks

NGN Transport Network

UA

SIP

RTP

Media Gateway

Media Gateway Ctrl Function

Signalling Gateway

Application Server

Next Gen IN

User Agent

I-C/BGF

Access-BGF

Call/Session Ctrl Function

Home Subscriber Server

MGW

MGCF

SGW

AS

NGIN

UA

I-BGF

A-BGF

CSCF

HSS

ISUP

PCM

SIP

RTP

Interworking with TDM Voice Network

SGW

MGCF

MGW

RTP Proxy

SIP ALG

Direct VoIP Traffic

Indirect VoIP Traffic

Indirect TDM Traffic

UKNOF 5 : NGN VoIP : Neil J. McRae
VoIP Core Network Architecture with Security

- Billing
- DB
- WEB
- FW
- IP PBX
- SBC
- Softswitch
- MGW
- PBX
- CPE
- IP / MPLS
- TDM / PSTN
- Internet
- Carrier

VoIP Core

OSS/BSS

H.323/RTP
H.323/MGCP/RTP
SIP/RTP

UKNOF 5 : NGN VoIP : Neil J. McRae
VoIP Protocols

H.323
- ITU, ASN.1, CPE/Phone<->Gatekeeper
- H.225/RAS (1719/UDP) for registration
- H.225/Q.931 (1720/TCP) for call setup
- H.245 (>1024/TCP – or over call setup channel) for call management

MGCP (Media Gateway Control Protocol)
- IETF, Softswitch (CallAgent)<->MGW
- CallAgents->MGW (2427/UDP)
- MGW->CallAgents (2727/UDP)
- Used to control MGWs
- AoC (Advice Of Charge) towards CPE - **
VoIP Protocols

SIP

- IETF, HTTP-like
- Session based – Does anyone here not know what SIP is? :D

RTP

- Media stream (one or one per direction)
- CODECs (G.711{a,u}, G.726, G.729(a))
- RTCP: control protocol for RTP
- SRTP: Secure RTP (w/ MiKEY)
- Often 16000+/UDP or default NAT range, but can be any UDP>1024
- Can be UA<->UA aka “Free Intersite” or UA<->MGW<->UA
The majority of current COLT VoIP products is based on H.323. This is mainly owing to missing functionality on SIP. Questionable interoperability and scalability concerns still exist though (10s of billions of minutes). SIP is not expected to completely replace H.323 in the mid/long term. Protocols are somewhat complementary—no religion here though!

More detail on the differences:

- and more insight on understanding of our direction at:

  http://www.packetizer.com/voip/h323_vs_sip/

This is expected to change over time.
What is the role of an SBC?

- Security
- Hosted NAT traversal (correct signalling / IP header)
- Signalling conversion
- Media Conversion
- Stateful RTP pin-holing based on signalling

Can be located at different interfaces: Customer/Provider, inside customer LAN, Provider/Provider (VoIP peering)

What can be done on a FW with ALGs?

What can be done on the end-system?

Is there a need for a VoIP NIDS (especially with SIP-TLS)?
VoIP Hardware

Mix of software and hardware (mostly DSPs)

- Softswitch: usually only signalling
- MGW (Media Gateway): RTP<->TDM, SS7oIP<->SS7
- IP-PBX: Softswitch+MGW

Operating systems

- Real-time OSes (QNX/Neutrino, VxWorks, RTLinux)
- Windows
- Linux, Solaris

Poor OS hardening

Patch management:

- OSes not up-to-date
- Not “allowed” to patch them
Security Challenges

VoIP protocols

> No, VoIP isn't just SIP
> SIP is a driver for IMS services and cheap CPEs
> H.323 and MGCP (still) rock the carrier world

Security issues

> VoIP dialects
> Only a couple of OEM VoIP stacks (think x-vendor vulnerabilities)
> FWs / SBCs: do they solve issues or introduce complexity?
> Are we creating backdoors into customer networks?
> CPS and QoS
One more backdoor?

- "Executive floor" WLAN AP
  - ap
  - s
  - r
  - External laptop
  - r
  - External laptop
  - r
  - r
  - CPE
- "IT floor" Internet access
  - fw
  - cpe
  - External laptop
  - r
  - r
- Corporate Internet access
  - fw
  - cpe
  - r
  - r
  - CPE
- Remote office/Partners IP VPN
  - r
  - s
  - r
  - s
- Remote maintenance
- Vendor
- Office
- Partner

VoIP
- IP PBX
- Shared TFTPd
- UKNOF 5: NGN VoIP: Neil J. McRae
VoIP Dialects

No way to firewall / ACL (especially if non-stateful) based on protocol inspection

Vendors who never heard of timeouts and don't send keep-alives

Result:

> Clueful:
  – Permit UDP <port range> <identified systems>

> Half clueful:
  – Permit UDP <port>1024> any

> Clueless:
  – Permit UDP any any

End-result:

> 0wn3d via exposed UDP services on COTS systems

> Who needs RPC services (>1024/UDP) ?
Lawful Intercept

> Re-use existing solutions: TDM break-out
> Install a sniffer (signalling & media stream)
> Re-route calls (but hide it in the signalling)
> Eavesdropping not a real threat (own network)
> Enterprise network: Needs to be a part of a global security strategy – How many have this?
  - Clear text e-mail
  - Clear text protocols (HTTP, Telnet, etc)
  - VoIP
  - Etc
> VoIP over WLAN easy.
IP Phones Reliability

> Quite easy to crash (weak TCP/IP stacks and buggy software implementation)

> Mostly an insider threat – How clueful is your cleaner?
  - DHCP server
  - TFTP server (phone configuration)
  - Credentials (login + PIN) – Fraud issues.

VoIP doesn't mean that you need to move to IP Phones

> PBX with E1 (PRI/BRI) to router and then VoIP

> PBX with IP interface towards the outside world (but do you really want to put your PBX on the Internet) ?

> Means that you have to maintain two separate networks, but “solves” the QoS issues on a LAN

> What about soft clients ?! – All the usual Unix/Windows issues.
Denial of Service

Generic DDoS

> Not a real issue, you can't talk to our VoIP Core
  - ACLs are complex to maintain use edge-only BGP blackholing
> We are used to deal with large DDoS attacks :)
  - http://www.securite.org/presentations/ddos/

DoS that are more of an issue

> Generated by customers: not too difficult to trace (IT Clue)
> Protocol layer DoS : H.323 / MGCP / SIP signalling
  - Replace CPE / use soft-client
  - Inject crap in the in-band signalling (MGCP commands, weird H.323 TPKTs, etc)
  - Get the state machine of the inspection engine either confused or in a block-state, if lucky for the “server” addresses and not the clients – Vendors not really thinking about this.
Security Challenges

Online services

> Call Management (operator console)
> IN routing (Fraud potential)
> Reporting / CDRs

Security issues

> Multi-tenant capabilities
> Have the vendors ever heard of web application security?
> Who needs security or lawful intercept if a kid can route your voice traffic via SQL injection

WebApp FWs are really required…
Security Challenges

TDM / VoIP: two worlds, two realms, becoming one?

- Security by “obscurity” / complexity vs the IP world
- Fraud detection

Security issues

- New attack surface for legacy TDM/PSTN networks
- No security features in old Class4/Class5 equipment
- No forensics capabilities, no mapping to physical line

- Spoofing and forging

VoIP is damn complex

Only way to debug most of the issues: VoiceEng + IP/DataEng + SecurityEng on a bridge/online chat

Requirement: be able to sniff all traffic

Tool: Ethereal/Wireshark

Attacker: Just use any of the protocol decoder flaw in the sniffer

Make sure your sniffers are on R/O SPAN ports, in a DMZ which only allows in-bound VNC/SSH

Do not underestimate the effort on a multi Country setup – What is EU?!

If the guy is really good and can upload a rootkit over RTP: get his CV and offer him a job – you need this guy – serious skills shortage
VoIP Carrier Interconnect

Aka “VoIP peering” / Carrier interconnect

Already in place (TDM connectivity for VoIP carriers/Skype{In, Out})

Connectivity: over the Internet, IX (public/private), MPLS VPN or VPLS (Ethernet)

No end-to-end MPLS VPN, break the VPN and use an IP-IP interface

Hide your infrastructure (topology hiding), use {white, black}listing and make sure only the other carrier can talk to you

Signalling/Media conversion (SBC)

Remember – this isn’t web traffic – its termination money in both directions!
Do we want to introduce it?
Vendor X: “We are compliant”. Sure.
Vendor Y: “It's on our roadmap”. Q1Y31337?
Vendor Z: “Why do you need this?”. Hmmm...

IPsec from CPE to VoIP core
> Doable (recent HW with CPU or crypto card)
> What about CPE<->CPE RTP?
> Still within RTT / echo-cancellation window
May actually do mobile device<-> IPsec -> VoIP core
> Bad guys can only attack the VPN concentrators
> No impact on directly connected customers

Still reliability issues in vendor implementations

UKNOF 5 : NGN VoIP : Neil J. McRae
IMS = IP Multimedia Subsystem

Remember when the mobile operators built their WAP and 3G networks?
> Mostly “open” (aka terminal is trusted)
> Even connected with their “internal”/IT network

IMS services with MVNOs, 3G/4G: overly complex architecture with tons of interfaces

Large attack surface: registration/tracking servers, application servers, etc

Firewalling: complex if not impossible

Next thing to try: Attack Fixed<->Mobile handover (GSM<->WiFi)
Questions?