>BUSINESS MADE **SIMPLE**

Enabling Secure Realtime Media with SIP

Robert Dolphin
Senior Architect, Enterprise Networks

NORTEL

Agenda

> **SIP call setup**

> Signaling Encryption

> SRTP and Key Negotiation

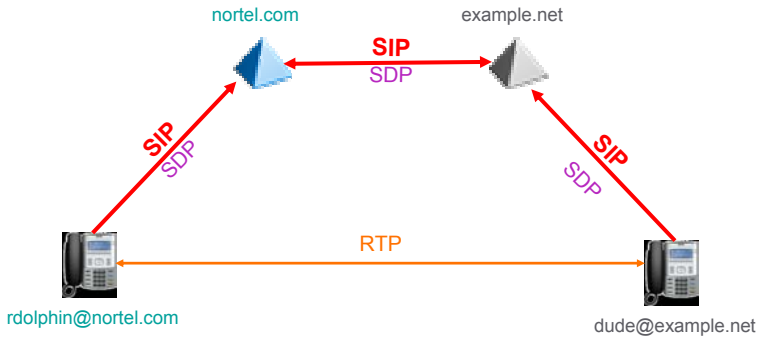
> Specific Solutions

> Conclusion

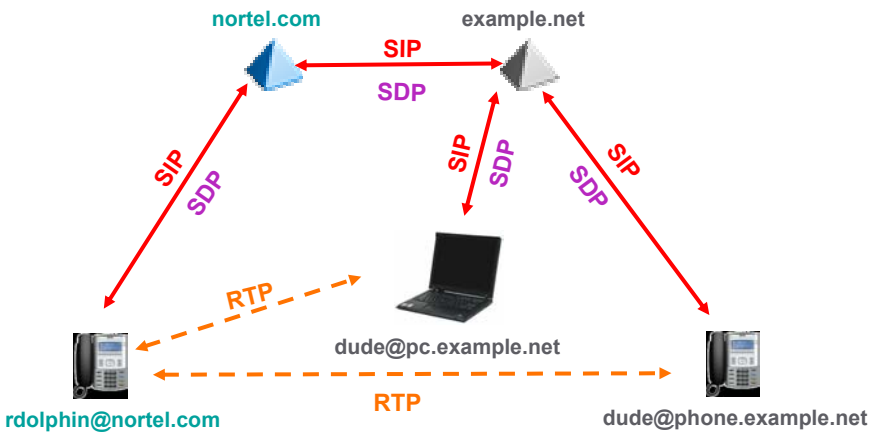
SIP Call Setup

> Signaling typically routed via SIP proxies

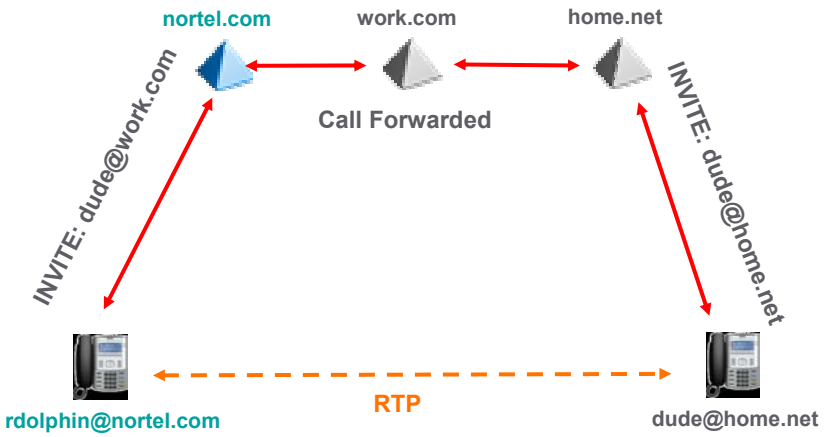
> Media path established point to point using RTP



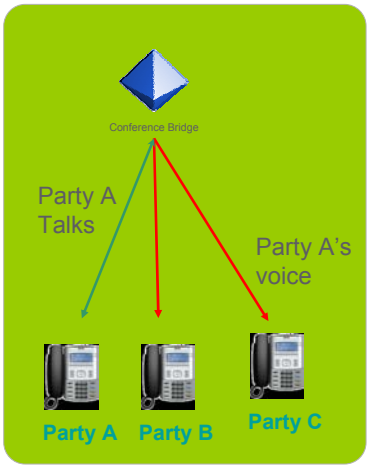
Call Forking



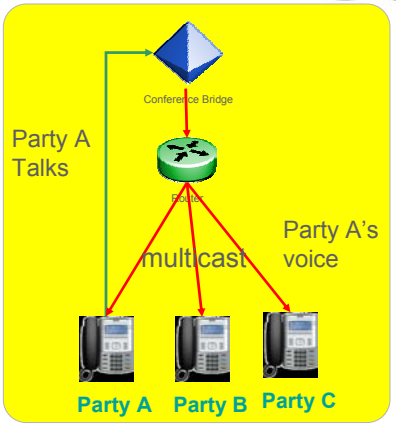
Retargeting



Conferencing



Different media stream to each participant



Same media stream to each participant

Shared key conferencing

Not really seen in SIP based systems

Agenda

> SIP call setup

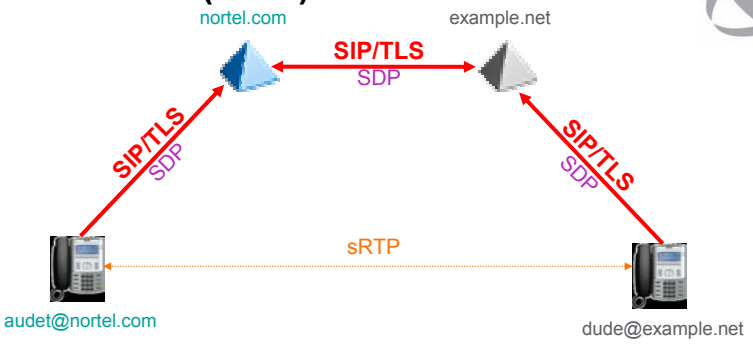
> Signaling Encryption

> SRTP and Key Negotiation

> Specific Solutions

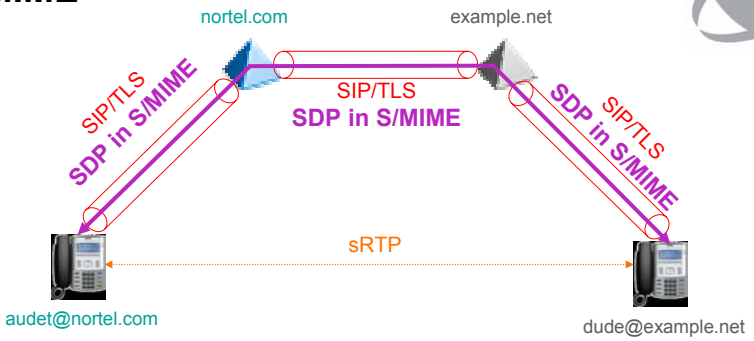
> Conclusion

SIP over TLS (SIPS)



> Whole SIP signaling channel
> UA → Proxy: Client/Server
> Proxy ↔ Proxy: Mutual Authentication
> Hop-by-hop
> Mandatory in SIP (RFC 3261)
> Being implemented in Nortel products

S/MIME



> S/MIME for encrypting Bodies inside SIP, end-to-end
> Breaks Application Level Gateways that rely on inspecting SDP
> Certificate management (sip-certs draft)
> Many skeptics

Agenda

> SIP call setup

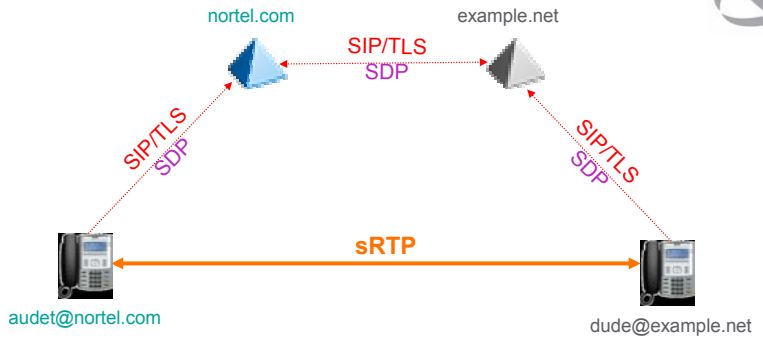
> Signaling Encryption

> SRTP and Key Negotiation

> Specific Solutions

> Conclusion

Media (sRTP)



> RFC 3711

> sRTP is a profile of RTP

> Very efficient

> Requires key negotiation

Key negotiation

> This is the complicated part

> Each side needs to know what session key to use

> Three approaches exist

- Handshake in signaling channel (standardised)
- Handshake in media channel (draft only)
- Combination of the above (draft only)

> One SIP/SDP Offer/Answer exchange is preferred

Agenda

> **SIP call setup**

> **Signaling Encryption**

> **SRTP and Key Negotiation**

> **Specific Solutions**

> **Conclusion**

SDESCRIPTIONS

>Key in SDP Offer/Answer

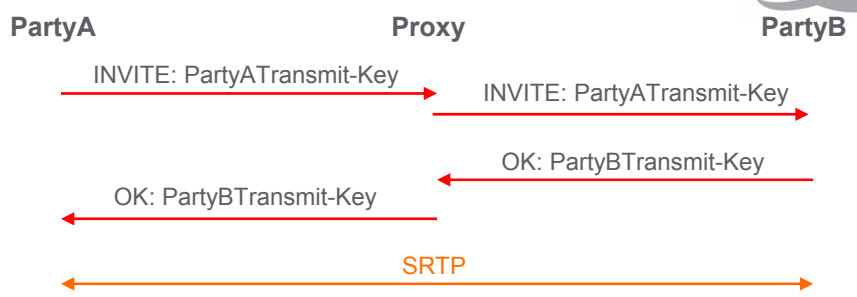
>No “negotiation” is involved: Very simple

>Rejecting the key implies rejecting the session

>Keys are not encrypted

>SDESC in SDP over TLS is currently the most practical solution

SDESCRIPTIONS



Requires signalling confidentiality	Yes (SIP/TLS or S/MIME)
Forking	Yes (insecure)
Media before SDP answer	No
Shared-key conferencing	Yes
Requires PKI	No
Rekeying	Yes (New Offer)
Downgrade attack protection	No

MIKEY/KMGMT

>MIKEY is a Real key management protocol

>KMGMT is the SDP extension to carry MIKEY

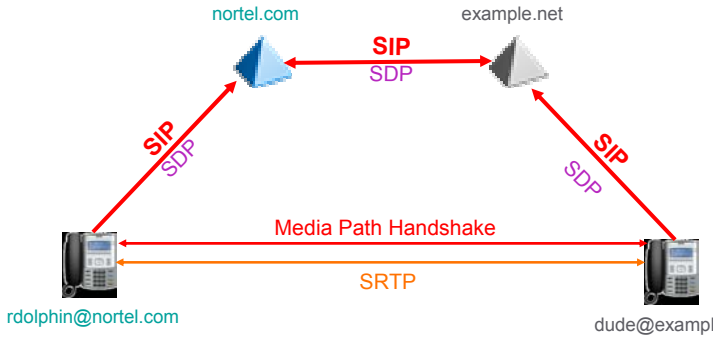
>May use Multiple Offer/Answer exchanges

>Master key is encrypted in SDP

>Quite complicated

>Many modes of MIKEY

EKT, ZRTP, DTLS



EKT uses a combination handshake in SDP and RTCP

ZRTP and DTLS use media path handshakes

NONE OF THESE APPROACHES ARE STANDARDISED

How do different modes score?

	Signaling Conf Required	Forking	Media before Answer	Shared-key conf.	PKI Needed ?	Rekey	Bid-down protection
MIKEY-PSK	No	No	Yes	Yes	No	Yes	Yes
MIKEY-RSA	No	No	Yes	Yes	Yes	Yes	Yes
MIKEY-DH	No	No	No	No	Yes	Yes	Yes
MIKEY-DHHMAC	No	No	No	No	No	Yes	Yes
MIKEY-RSA-R	No	Yes	No	Yes	Yes	Yes	Yes
SDES	Yes	Yes	No	Yes	No	Yes	No
SDES-EM	Yes	Yes	Yes	Yes	No	Yes	No
EKT	Yes	Yes	Yes	Yes	No	Yes	Depends
SDP-DH	No	No	No	No	No	No	No
ZRTP	No	Yes	Yes	No	No	Yes	Yes
DTLS	No	Yes	Yes	No	No	Yes	Yes

Source: Dan Wing IETF

Agenda

> SIP call setup

> Signaling Encryption

> SRTP and Key Negotiation

> Specific Solutions

> Conclusion

Conclusion

> What's important?
- Media before SDP answer ("clipping")
- Secure Forking
- Shared-Key Conferencing
- Ubiquitous interoperable security

> Architecture Choice
- Key Exchange in Signaling
- Key Exchange in Media
- PKI

> What can we do today?

More Information

> http://www.ietf.org/rfc.html

> http://www.ietf.org/ietf/1id-abstracts.txt

> draft-wing-rtpsec-keying-eval-01.txt