Service Provider implementation of SIP regarding security

Vesselin Tzvetkov, Holger Zuleger

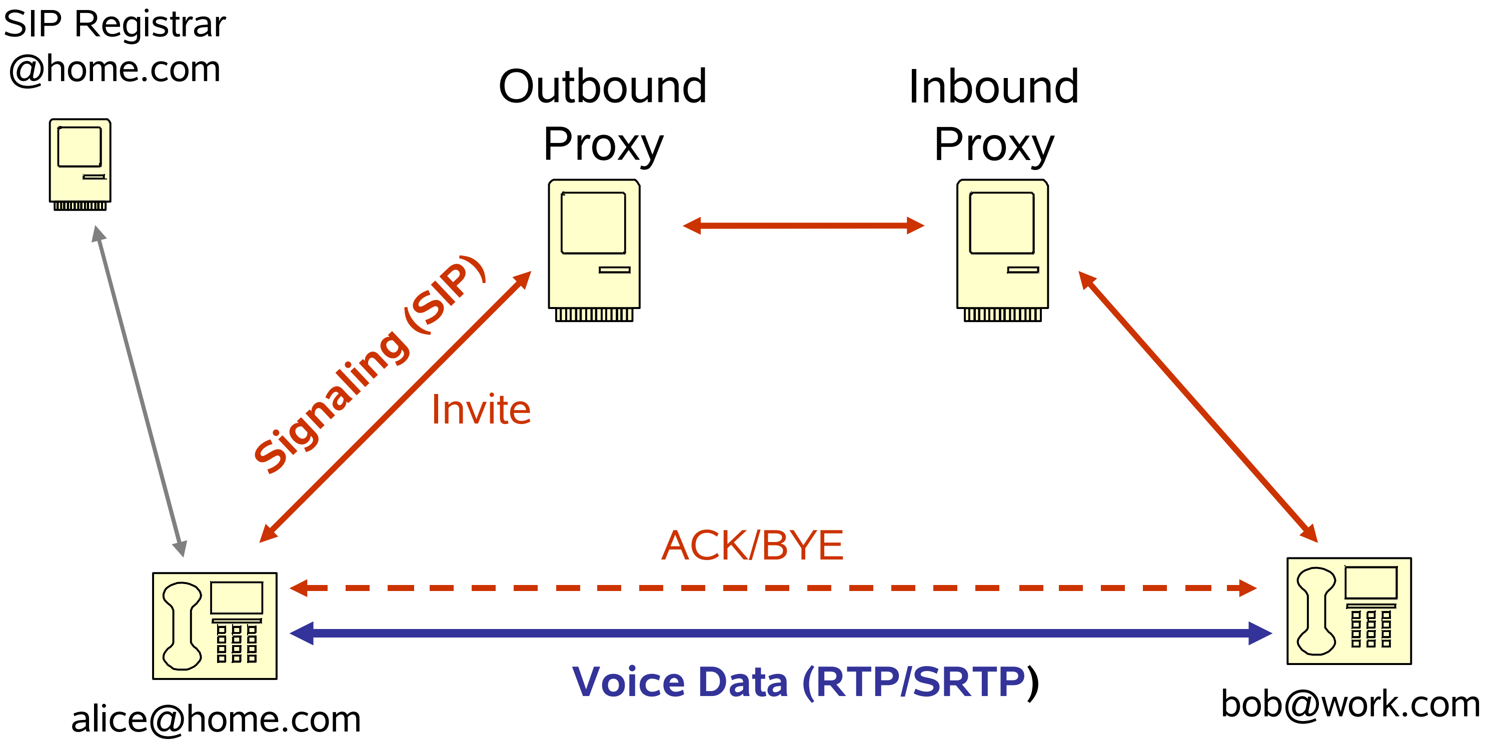
{vesselin.tzvetkov, holger.zuleger}@arcor.net

Arcor AG&Co KG, Alfred-Herrhausen-Allee 1, 65760 Eschborn, Germany

Preface and short digest

- **What is meant by security ?**
  - Protection of the phone call. Just encryption, integrity and confidentiality.
  - No (D)DoS, No Authorization, No infrastructure protection
- **Why the security is an issue ?**
  - The SIP implementations at the Service Providers (SPs) are quite different then the one described in IETF RFCs.
  - The IETF security mechanisms can not be implemented in the SP networks.
- **What is done in this paper ?**
  - Theoretical analysis and implementation recommendation. No practical tests. **No new protocol is designed**.

SIP communication according to the RFCs

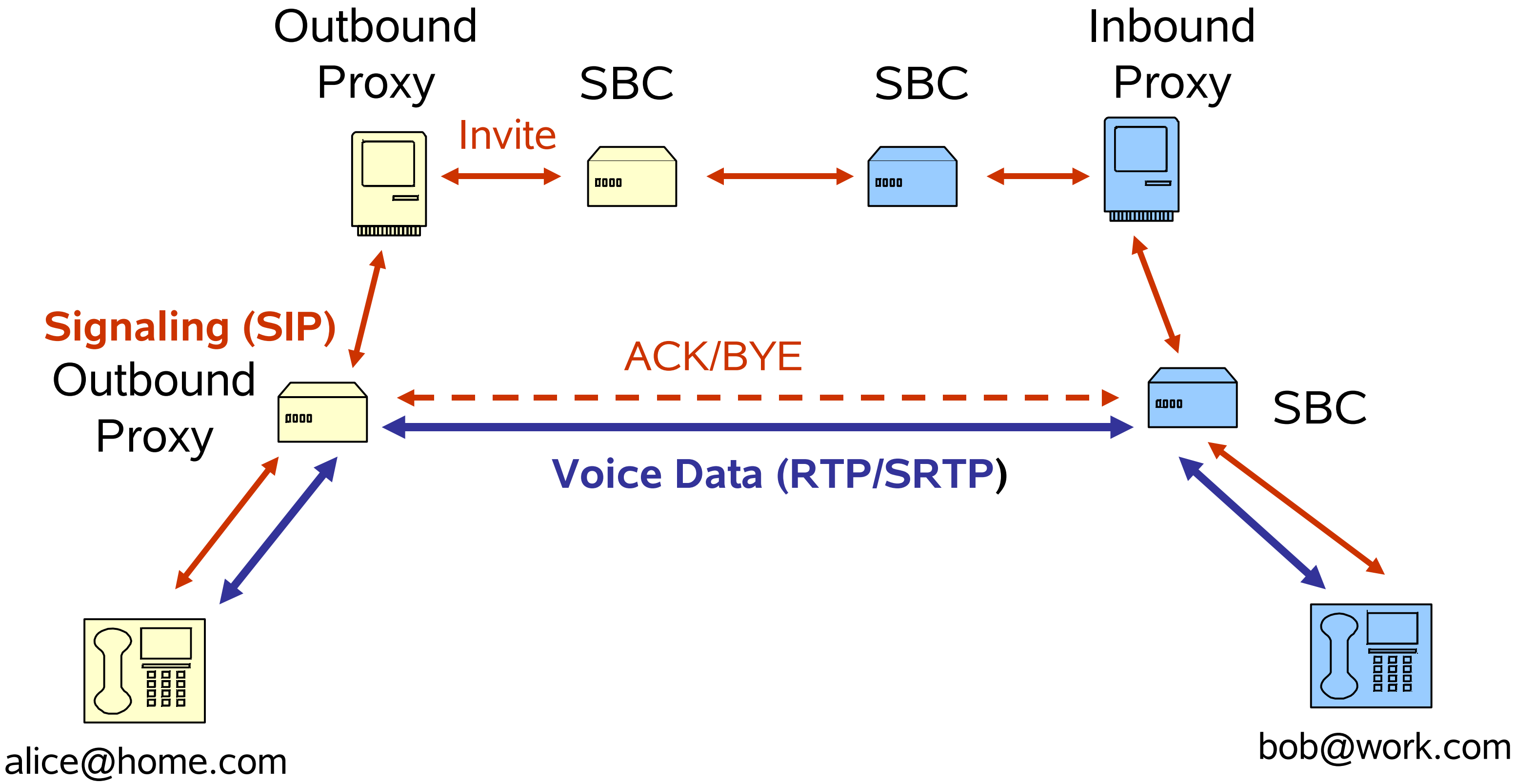


- The RTP(SRTP) stream is send directly between the clients
- The SIP clients are part of the same ip domain, for example public internet
- The outbund proxy is an optional element only for local breakout purposes.

Provider SIP implementations

- **Why the service provider deploy different structure ?**
  - The SP must deliver service quality to the end customers. It must deploy QoS. Currently internet uses best effort service.
  - The Service Providers have regulatory duties as legal interception and providing call/user information (police).
  - SIP isn't a green field service and parallel operation of the legacy ISDN/PSTN together with the new SIP network must be achieved.
  - The wide spread of devices using dynamic Network and Port Translation (NAPT or NAT) interrupts the IP layer connection between the hosts. NAPT is currently implemented in all broadband routers (ADSL).
  - SP have many million customers of the same administrative domain. The SP require load balancer and protection of their infrastructure by malicious sip packets and DoS attacks etc.

Service Provider SIP topology (Peering)



- Session Border Controller are used in the SP networks
- The RTP(SRTP) in NOT send directly between the clients

Session Border Controller

- **Properties of the Session Border Controller**

  - Load balancer, which distributes the load between multiple SIP servers.
  - Failure detection of SIP servers and failure recovery
  - Filtering of malicious packets
  - Hiding the SP network topology
  - Unload the SIP servers. Some SIP request can be answered directly by the SBC, for example re-registration.
  - RTP Media proxy for solving the NAT issues
  - Implements NAT keep-alive mechanisms
  - RTP Transcoding
  - Protection against DoS attacks on SIP registrar
  - Handle private ip address space.

Security protocols

- **What must be secured in the VoIP environment ?**

  - There are 3 node types: Client, SBC, SIP Server
  - There are two types of communication: signalling and voice data
  - The are two directions: incoming and outgoing sessions

There are totally

3(nodes) x 3(nodes) x 2 (connection types) x 2 (directions) =

36 communication relations

Which one must be secured ?

We simplified them to 8 reasonable: “Client to SBC”, “SBC to Client”, “Client to Client”, “SBS to SBS” (inbound and outbound)

Protection

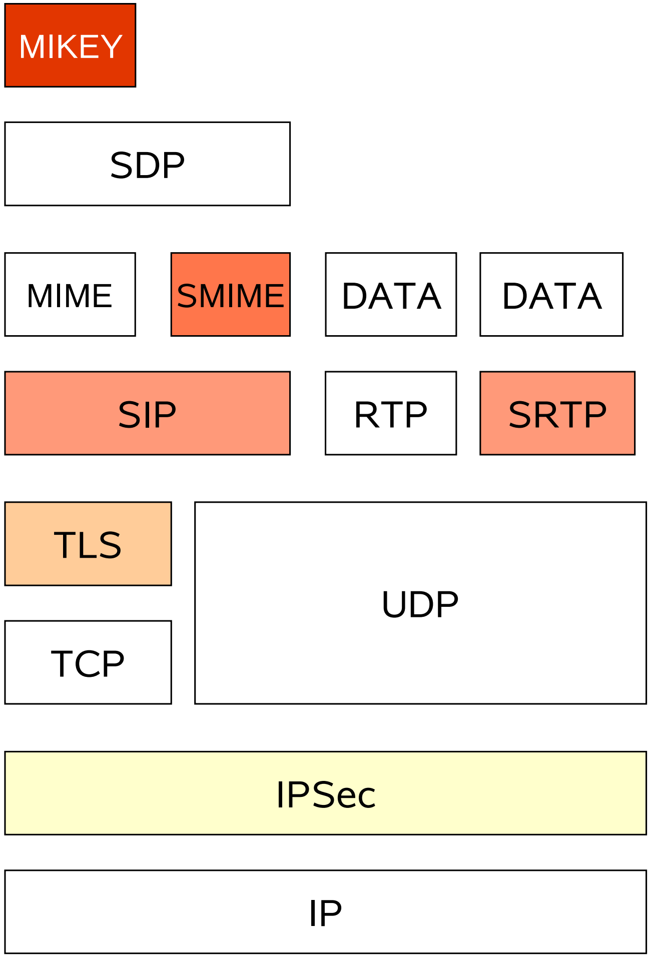
- **What is meant by protecting ?**

  - Authentication
  - Authentication, Encryption and integrity protection

Possibilities with SIP

- **SIP**
- **SIPS**
- **SRTP**
- **IPSec**
- **SIPS + SRTP**
- **SMIME + SRTP**
- **MIKEY + SRTP**
- **Alternative solutions**

ZRTP, MIKEYv2, DTLS-SRTP



General problems with security

Early media

The SP send the ringing signal as RTP stream. Only after the client picks up, there is second RTP stream with the voice.

Shared mail box (answering machine)

The SP offer mail box as service to the customers. If the user doesn't pick up, the call is redirected to the mail box. It is part of the SP equipment and is virtual.

Form client perspective: The user calls "Peter" but somebody else is picking up the phone, for example the virtual mail box.

This is a very complex problem form security perspective, **because the virtual mail box must be authenticated**, that it is authoritative to record the message for "Peter"

General problems with security II

Forking

The SIP client is registered multiple times with the same user (SIP URI). For example with its mobile, soft client and hard phone. The “invite” request is send to all registered clients. The first who picks, gets the call.

Form caller perspective: There a potentially multiple phones, which can take the call. The client can not know in advance who is going to pickup.

Form security perspective these are different nodes. They have the same SIP URI, but support different algorithms and have different credentials. For example the SIP installed on smart phone can not support digital signature for authentication, but the hard phone can do.

General problems with NAT I

NAT (NAPT)

The connection can be established only behind the NAT device. All Broadband users today use NAT in their routers, for example a DSL WLAN router.

How can we then receive a SIP call behind a NAPT ?

Using **symmetric SIP and RTP** allows to receive the session on the same ports, on which is made the outgoing session. The client behind the NAT must keep these port open with sending “nat-keep-alives”. Works only for UDP.

The SIP client must support symmetric SIP/RTP. This do not require any change of the SIP standard only of the implementation structure to send and receive on the same port. The distribution between the RTP and SIP traffic is made in pre-process in the implementation.

General problems with NAPT, II

NAT (NAPT)

Unfortunately, symmetric SIP and RTP is not working in principle for TCP. It is not possible to have multiple sockets bind to the same source and destination port. In TCP there is a sequence number of every packet.

There must be change in the SIP standard in order to work. Currently there are work in progress, but for sure all implementations must be rewritten. See “draft-ietf-sip-outbound-08”, C. Jennings, Ed. At al

Summary

Authentication

		IPSec	SIPS	SIPS + SRTP	SMIME	SMIME + SRTP	MIKEY + SRTP	SIP Digest
Client to SBC	SIP Sign.	✔	🗸	🗸	☑	☑		🗸
	RTP Data	✔		🗸		✔		
SBC to Client	SIP Sign.	✔	🗸	🗸	☑	☑		
	RTP Data	✔		🗸		✔		
Client to Client	SIP Sign.				☑	☑	🗸	🗸
	RTP Data					✔	✔	
SBC to SBC	SIP Sign.	✔	🗸	🗸	☑	☑		
	RTP Data	✔		🗸		✔		

Authentication, encryption and integrity

		IPSec	SIPS	SIPS + SRTP	SMIME	SMIME + SRTP	MIKEY + SRTP	SIP Digest
Client to SBC	SIP Sign.	✔	🗸	🗸	☑	☑		
	RTP Data	✔		🗸		✔		
Client to Client	SIP Sign.				☑	☑	🗸	
	RTP Data					✔	✔	
SBC to SBC	SIP Sign.	✔	🗸	🗸				
	RTP Data	✔		🗸				

✔	SIP/RTP packet (all data)
☑	Parts of SDP body (no SIP header)
✓	Only Client auth. (not SIP/SDP msg)
🗸	Only outgoing comm. when dynm. NAT used

End

Thank you !

SIPS + SRTP

- **SRTP** encryption of the data.

  The protocol do not have any key negotiation mechanism. It must be used in conjunction with other protocol to deliver the key.

- **SIPS** is “SIP over TLS” and protects only the signalling.

  The TLS protocol is used in HTTPS and supports client/server digest authentication. TLS uses TCP as transport. SRTP key can be send protected in the SIPS.

Properties

- Since the TCP layer is interrupted by the SBC there is no Client-to-Client protection possible. Only client to SBC or SBC to Client
- TCP session can not be established outside a NAT router. Only outgoing calls can be protected.
- The client and server must have a certificate
- For early media, the client must totally trust to SBC.
- This is a possible solution of the first mile protection, where no NAT is involved.

SMIME + SRTP

The SDP body is MIME structure. Some attributes can be protected with SMIME

SMIME authentication uses digital signatures, optional also encrypted with private key.

Parts of the attributes are needed by the SBC and SIP Server. We recommend to encrypt and authenticate only the Key-Attribute for protection of the SRTP session.

Properties:

- Enables Client-to-Client authentication, since only part of the parts of the body.
- SBC-to-Client can also be used.
- The SIP URI is not protected, but can be signed and authenticated.
- Forking is a problem. The client credential must be know in advance. If the callee has multiple private keys it is not going to work.
- Early media is also problem, because the caller do not know who is going to pick up: the mail box, media controller giving ring tone or the user.
- Forwarding to PSTN are also a problem

MIKEY + SRTP

MIKEY is a key authentication and negotiation algorithm using SDP attributed. The hole negotiation is done with two exchanged payloads embedded in SDP attributed.

Properties:

- Enables Client-to-Client authentication. It uses only attributes in SDP
- SBC-to-Client can also be used.
- Forking is a problem. The client credential must be know in advance. If the callee has multiple private key it is not going to work.
- Media before call is also problem, because the caller do not know how is going to pick up: the mail box, media controller giving ring tone or the user.
- Forwarding to PSTN is problematic for the same reasons

IPSec

IPSec can be used to protect the SIP and RTP in the same session

There are variety of possibilities for authentication like digital signature, shared secret, passwords

Properties:

- IPSec is a good alternative for protecting the first mile Client-to-SBC. It is not possible to protect Client-to-Client

-There is still unclear how the id in IKE and SIP URI must match

- It is suitable for providers which have already build IPSec infrastructure.

Alternatives

The are currently efforts to develop alternative methods for key negotiation for SRTP :

- **ZRTP** is interesting hybrid approach for key negotiation in RTP. The authentication is done by reading the part of the authentication secret aloud to the communication partner over the voice connection. There is no need of PKI, shared secret etc. (Draft, Phil Zimmermann et. al.)

- **MIKEYv2** enhances v1 to used for broadcast, group keys, smart cards, TLS, optimisation by reeking. (Draft, L. Dondeti)

- **DTLS-SRTP** is a draft provides guidelines on how to use DTLS to establish SRTP and to transport media. DTLS is version of TLS to work with UDP packets. (Draft, J. Fischl et. al.)

All of them are draft documents