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

***Abstract* — The rapid growth of the SIP implementations clearly shows that the classical PSTN network will be exchanged by internet telephony. All Service Providers (SP) are currently deploying SIP infrastructure for offering the next generation networks. The implementations and network concepts used by the SP are different then the original designed in SIP standard. The main SP reasons are protecting their network, high number of customers, service quality quarantine and duties to the executive power. The security aspects in VoIP are generally secondary and planned for the coming years, since at first stage the target is launching the service on time. In this paper we are showing the current provider's SIP implementations and giving the motivation for this structure. Then we are analyzing the possibilities for securing the communication involving the existing standards. There are many security layers and objectives in the SIP networks to be considered. Some of them are practically not possible in the SP network and other are not reasonable. In this paper we giving the understanding, what can be done and how the different security mechanisms are interacting. At the end recommendation for protecting the SIP communication are made.**

***Index Terms*—SIP, Security, RFC 3261, SRTP, MIKEY, IPSec, SSL, SIPS, TLS, SBC, VoIP**

I. INTRODUCTION

The next generation networks are going to exchange the classical PSTN network in the coming years. All telephony Service Providers (SPs) are currently implementing SIP Class 5 in their networks. The first main target is to use one IP backbone for delivering classical telephone services and internet access. In this way the operational costs will be reduced. The second target is to introduce new extended services as for example messaging and video, which will increase the revenue and possibly help to acquire new customers. The primary task is launching the products in time and in this way to over perform the competitors. The security of the communication is at this stage secondary. The security improves the products quality, but unfortunately is not decisive costumer gaining argument. The security will be major issue at following stage, when mobile customers start using intensively VoIP through different access networks and therefore emphasize the privacy.

The major protocol for the next generation services is SIP specified in [SIP]. The protocol, as designed by the IETF, is not considered to be total exchange technology of the classical PSTN. The protocol delivers from user perspective almost the same functionality, but primary designed to deliver new type of services through internet. There is no fully overlapping of ISDN and SIP features. PSTN networks have properties as for example quality of the call, call localization, emergency call, legal interception, high availability. These properties are actually not part of the SIP standard and they must be delivered by other mechanisms. Unfortunately, these are currently not available in internet. The SPs have quality agreement with the customers. In order to achieve this, the SP should control every element of the network. The best effort delivered in internet is not sufficient to guarantee the required end-to-end quality of the service.

The Service Providers have also some regulatory duties as: legal interception and providing call/user information to the executive authorities (police). When the Service Providers implement SIP to deliver classical telephony, they need to fulfill further this requirements and provide PSTN features.

SIP isn't green field service and parallel operation of the legacy ISDN/PSTN together with the new SIP network must be achieved. Consequently, a large number of current customers should be seamless migrated from PSTN to SIP. This is a quite big issue, since the current data is stored in legacy databases, which also need to be migrated without service interruption. The current interconnection points are using SS7[SS7] protocol and these are not going to disappear in the coming decade. Parallel operation and interconnection between the networks must be achieved with all existing features.

Internet not only grows but also evaluates, thus changes its structure. 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) [NAT]. A connection can be established initially only from inside the NAPT device (LAN side). A connection establishment form outside (WAN) will be dropped [NAT]. The SIP protocol assumes and requires bidirectional IP connectivity, which is currently no present because of unidirectional NAPT. Furthermore, in NAPT a keep-a-life mechanism is required to keep established connection open. Otherwise, after some idle timeout the NAPT device removes the connection. To overcome all these problems media and signaling proxies (symmetric SIP and RTP) are used, which are not considered by the original SIP standard.

The arguments in the previous paragraphs lead to different SIP implementation by the telephony SP as the one

recommended in the RFCs. The different SIP structure has big influence on the security features. Most of the literature about the SIP security is not describing the existing SP's SIP network. Therefore, not all in RFC suggested security mechanisms can be implemented by the SP. Some major security questions regarding inter working between the layers are also not deeply resolved.

In the following chapter II we are showing the current SIP implementations at the SP networks. Then we are presenting the security objectives in chapters III and IV. The different mechanisms for securing SIP are described in chapter V. In the last chapter VI recommendations and conclusion are made.

II. SIP NETWORK STRUCTURE

A. *Theoretical SIP Structure*

Let us first briefly overview the SIP structure descried in the RFCs. We are describing only the major security relevant blocks. More details can be found in [SIP].

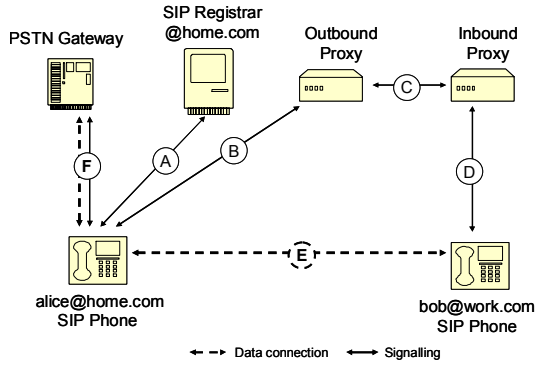

Figure 1 Classical SIP architecture

There are two major procedures in the SIP: registration and call (service) establishment. They are commonly known as *registration* and *invite (message)*. In the *registration,* the client announces its location and status to the registrar, who provides this information to all other sip servers as for example proxies. In this way, incoming requests can be forwarded to the current location of the client. When activated, the client registers at the SIP registrar, step A at **Figure 1**. The registrar address is preconfigured in the client or extracted from the SIP URI. The SIP URI represents the client's address. The registration process requires usually some form of authentication.

The *invite* procedure is used to initiate a call or other type of sip connection. Let us assume a call establishment. The client sends a sip invite message to its outbound proxy, step B at **Figure 1**. The outbound sip proxy is optional element and should be used when the caller has no direct connection to the inbound proxy of the callee. If possible, the user should resolve in DNS the domain from the callee's URI and send the invite message directly to it. When the outbound proxy is involved, it also resolves the domain and forwards the invite, step C at **Figure 1**. The inbound proxy forwards the invite to the callee at his current location, step D. The callee replies directly to the caller or in most of the cases along the return path, step D, C, B at **Figure 1**. After receiving and accepting the call, a data session is established directly between the caller (alice) and the callee (bob), step E at **Figure 1**. The data session is made using RTP protocol [RTP].When the user calls classical PSTN it connects the PSTN Gateway (step F), which established call to PSTN numbers.

B. *SIP implementation at Service Providers*

The spreading of NAPT devices [NAT] in the internet causes a lot of problems for the sip implementations. If caller (alice) and callee (bob) are behind such devices, they can't establish a direct connection. The RTP data stream cannot be directly forwarded between them, as originally designed.

Usually the telephony Service Provider have many million customers of the same administrative domain. The SP require load balancer and protection of their infra-structure by malicious sip packets and DoS attacks, thus firewall structures must be build.

To solve these problems Session Border Controllers (SBC) are involved in SP networks. The SBC is a Back-to-Back user agent. This means, that from the user perspective it represents the SIP registrar, SIP outbound proxy and RTP media proxy. From SIP registrar/proxy perspective the SBC represents the client. The whole SIP and RTP communication is passing thought the SBC device. The SBC have the following major properties:

- Load balancer, which distributes the load between multiple SIP servers.
- Failure detection of SIP servers and failure recovery
- Filtering auf 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.

The main elements in SP network are shown at the following **Figure 2**. By activation the SIP client sends registration request to the SBC I, step A at **Figure 2**. The SBC's FQDN (Fully qualified Domain Name) is usually preconfigured at the client and resolved to ip address in DNS with SRV/NAPT records [SIPL]. From client perspective, the SBC is the SIP registrar. The SBC I forwards the registration request to the physical registrar in step B at **Figure 2**. The SBC keeps track of all active sessions and re-registration can probably be handled only in SBC and in this also unloading of the sip registrar.

By the invite procedure the caller (alice) sends an invite message to the SBC I, step C at **Figure 2**. The SBC is playing the role of an outbound proxy. The SBC I replaces the client ip address and port number with its own ip address and port. Additionally the SBC rewrites the SIP and SDP body. The SBC internally maps the original parameters to new parameters, in order to de-multiplex correctly the return message. The request is forwarded to the SIP proxy, step D at **Figure 2**. The invite is forwarded step E and F, where every node edits the packet attributes. Receiving the invite

the client(bob@home.com) considers that the SBC II is calling him. The RTP Session is build in steps G, H, J. It must be underlined, that the RTP session is not established directly between the clients. This has major influence of the security.

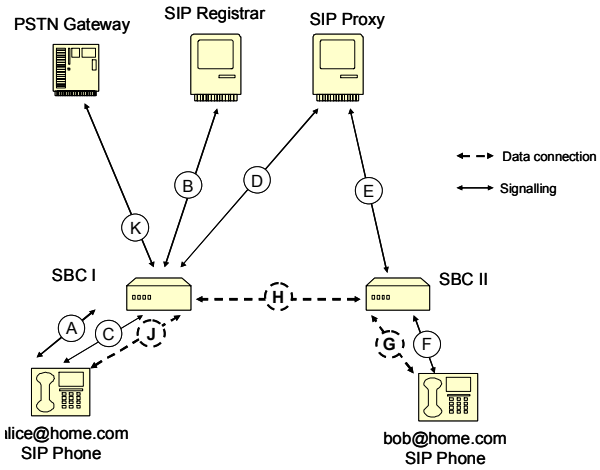

Figure 2 SIP implementation by Service Provider

Another important topology case is the interconnection between Service Providers. The SBC are playing a major role when customers of different SPs have SIP connections to each other. The interconnection term is originating from the PSTN world, where the SP's networks must be connected to enable calls between them. In classical SIP design, there is no need for any interconnection, since the SIP proxies are connected to internet and can directly exchange messages. The interconnection problem does not exist in SIP networks, which was one of the key advantage of SIP. Unfortunately, the Service Providers are currently in the process of implementing closed SIP infrastructures, which are not connected to the internet. In order to deliver end-to-end quality SPs need to control every single element of the network. The SP has a service agreement with the customers, which cannot be achieved with the best effort delivery in internet. The SIP software/hardware shipped by the SP are branded to have connection only to the SBC of the SP, thus free internet calling is not possible. In guarantee for the service quality return is given.

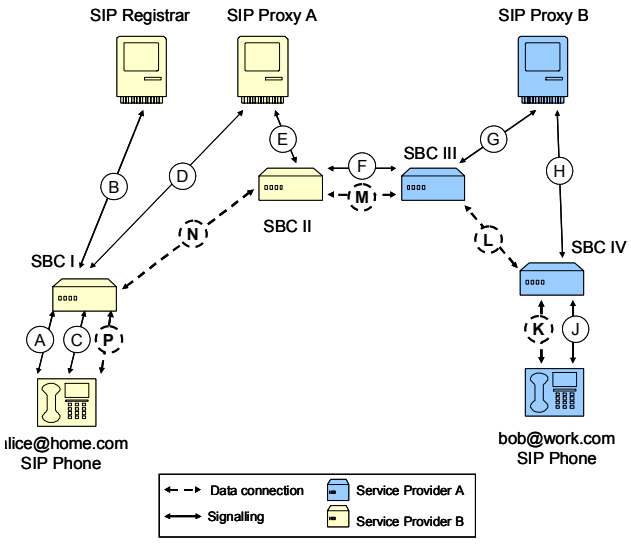

Figure 3 Interconnection between two SPs

The interconnection topology is shown at **Figure 3**. Each SP is installing a SBC for incoming and outgoing traffic as a border node. In this way the topology can be hidden and traffic control are made. The call establishment (invite) from alice to bob are forwarded at steps C, D, E, F, G, H, J at **Figure 3**. The data session (RTP) is made at steps K, L, M, N, P. There are obviously many hops, which definitely bring some delay in packet forwarding. Neither the SIP signaling nor the RTP data stream are established as in the theoretical SIP approach.

III. User Security Requirements and PSTN Network

There are different security targets and objectives in SIP network. At a first step, it is important to define and clear what wants to be secured and against what. The end customers don't have deep security knowledge or any SIP network experience. They cannot made exact requirement, and that's the reason why we are starting from the general requirements from customer perspective and going consequently step by step deeper to the implementation. There are two major customer requirements:

- Authentication: both users desires mutual authentication, thus before accepting incoming call to see who is calling.
- Confidentiality and integrity: third person cannot tap the conversation (no eavesdropping).

These are the common requirements by the customers, which we take as basis and break down to concrete sip requirements.

In PSTN there is no direct technical realization of authentication and confidentiality requirement. The low misuse rate is achieved due: (1) low number of providers, which are strictly observed by the authorities, (2) the telephone companies (now SP) were originally state companies with a high reputation, as for example mail service; (3) restrictive physical access to the network elements and in general to the technology and (4) the users authenticate themselves acoustically by listening to each other. Exactly as in the real world, the voice is the basis for authentication.

IV. Implementation of Security Requirements

The general customer requirements can be break down in multiple sub cases in the real network. Then we can consider which can cover the needs. Some of them cover only partially the requirements.

There are three nodes types form security point of view: client, SBC and SIP server. The SIP server denotes SIP registrar and SIP proxy. The security mechanisms and protocols for SIP registrar and SIP proxy are the same, thus for the security perspective it is the same node type. There are two communication types: SIP signaling and RTP data stream. Both of them must be considered separately, since they can be secured differently. We agree that confidentiality can't be achieved without authentication, thus encryption without authentication does not make sense in the cryptography. Further in text we are considering confidentiality as encryption, authentication and integrity protection. Now we continue with counting all the possible security relations, which have to be evaluated.

There are 3 node types which can communicate unidirectional with each other, thus there are 9 (3x3) types of communication relations, for example: “Client to SBC”, “SBC to client”. They are two different communication sessions: signaling and data. We have 18 (9x2) session types, which can be protected. The protection types could be: authentication or confidentiality (authentication, encryption and integrity). At the end, there are 36 (18x2) possibilities which must be evaluated.

At a next step we reduce these 36 possibilities regarding topological properties and justified needs. The main target is to obtain the reasonable alternatives, which correspond to the customers requirements.

The encryption should be usually bidirectional, thus cases like “Client to SBC” and “SBC to Client” make sense for authentication, but not for encryption. Furthermore, we consider these cases by encryption only as one.

The SBC is a back to back user agent, so from client perspective the SBC is the SIP Server, thus registrar and proxy. From SIP server perspective the SBC represents the end client. The client can not differentiate between SBC and SIP server. The SBC and the SIP server are from the client perspective the same node. Cases like “Client to SIP server” and visa versa are not further considered, since covered by “Client to SBC” and “SBC to client”

The SBC and the SIP server are usually part of the same security domain. In SP network, they are part of the backbone internal structure. Protection between two systems in the same security domain is not very reasonable. The protection “SBC to Server” and “Server to SBC” are not further considered.

Now we have reduced the possible cases to 14, thus seven cases for RTP data and seven for SIP signaling.

For authentication they are:

- “Client to Client” mutual authentication. The caller and callee should authenticate themselves. The user should know, who he is talking with.
- “Client to SBC” the client should authenticate to the SBC (SIP server).
- “SBC to Client” – the client must authenticate the server. The client should know whom he is sending its credential.
- “SBC to SBC”. In the case for interconnection, the SBC of the two SP needs mutual authentication. This is more a requirement of the SP than of the client.

For encryption, authentication and integrity, they are:

- “Client to Client” (end to end) encryption brings confidentiality. The end to end protection is very important to the customers.
- “Client to SBC” is known as first mile protection. It’s important when using untrusted access networks, like hotel or wlan hotspots.
- “SBC to SBC” is relevant by Service Provider interconnection.

V. Covering the requirement for security in SIP

There are numerous security protocols, which can be implemented with SIP and RTP, like TLS, IPSec, MIKEY etc. A layer overview (IOS/OSI) of the protocols is made of Figure 4. We group the major protocols to possible solutions and present them in the following paragraph. For every solution are presented the covered security arias and addition technical issues. The results are summarized at **Table 1**.

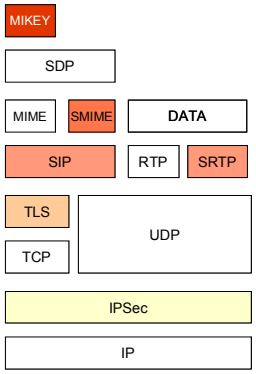

Figure 4 Overview layers

Most of the suggested protocols contain SRTP, therefore one note in advance. The advantage of SRTP is that it can be done end-to-end (client to client). Most of the SBC should not have problems forwarding SRTP packets. There are no additional requirements for proceeding of SRTP.

1) **SIPS with SRTP** [SIPS, SRTP] SIPS use TLS to protect the SIP communication. TLS is defined only over TCP, so is can be used to protect SIP signaling and not the RTP data. In order to protect the RTP session SRTP is involved.

Authentication with SIPS can be unidirectional SBC to client and optimal client to SBC (Server). For authentication x509 certificates are used. Management of many user certificates is a sophisticated problem. It could be more suitable to use TLS only for server to client authentication, without client certificates. For client to server authentication username and password can be used, since this is part of the SIP standard (md5 digest authentication). End-to-end (client to client) authentication and protection cannot be achieved, since there is no direct network layer connection between the clients.

Unfortunately, SIPS can not protect incoming calls in dynamic NAT environments, since TCP session can not be established from outside NAT device. Even using symmetric SIP it is not possible to initiate TCP session form SBC to client, when the client is behind dynamic NAT device. Regarding the wild spread of dynamic NAT we consider SIPS currently can protect only outgoing calls [SSP].

The SRTP protocol does not provide any key generation mechanism - it must be delivered by other protocol. In SIPS/SRTP combination the key can be delivered provided by key attribute in SDP (k-attribute). The lower TLS layer protects the signaling session, and thus the key can be send in clear. The key attribute could be exchanged between the end clients or SBC and client. Corresponding SRTP session is established between the end clients or SBC to client.

The client can control the SIPS protection only to the SBC, so it makes more sense using the key attribute only for SBC to client connections. In this case, the SRTP session is established client to SBC. The SBC must encrypt/decrypt the SRTP to RTP and visa versa.

A workaround for end-to-end SIPS protection suggested in the RFC standards is called “hop by hop”. This means, that only the transport between the nodes is protected and in the nodes the data is in clear. Each server node can read and modify the signaling packet. The trust chain is build hop by hop. The caller trusts its outbound proxy. The outbound proxy trusts the inbound proxy etc. From our point of view this is an improvement for sure, but not as an acceptable end-to-end solution. The client can’t influence the trust decisions in the next hops. In hop-by-hop protection it can happen that some nodes don’t trust each other, but are in a trusted hop-by-hop chain. This happens when there is a difference in the trust status between the nodes. For example the sip client do not trust the inbound proxy of the callee, but trusts its own outbound proxy. If the outbound proxy trusts the inbound proxy the trust chain is established.

The main issue using different layer for protection is that the identifier in application and protection layers must match. From security perspective the application and security layer are not independent. The id used in the TLS must match the id used in the SIP header. Otherwise insider attacks are feasible, if the credentials in the different layers are separately valid, but both are mismatching. For example the name in the driving license and passport must be the same. For the same reason in RFC [SIPL] the way of matching is defined. The domain in the SIP request, NAPT/SVR Record in DNS and subAlternativeName in the certificate must match. In this way, possible replacement attacks can be prevented.

The SPs commonly use one physical proxy for serving multiple domains, thus the certificate of the proxy must contain all domains. There are the following issues: (1) When new customers with own domains buy the SIP service every time new certificate must be generated for the server. (2) by reading the certificates the customers can see who else is using this proxy. For some companies this can be very undesired and even a security problem. To overcome this at least different ip addresses have to be used for each customer serving proxy.

We recapitulate, that SIPS with SRTP is alternative for protecting outgoing calls in the first mile client to SBC. Incoming calls are not protected. When the user trust the hop-by-hop principle the SIPS and SRTP can be established between the end clients. To underline is there is not end-to-end user authentication with SIPS.

2) **IPSec** [IPS] is a ip layer protocol and can be used to protect (encrypt and authenticate) the SIP signaling and the RTP media (**Figure 4**). The advantage for IPSec is that one session can protect the SIP and RTP and any protocol adjustments are required. End-to-end (client to client) protection can not be made, since the SBC and SIP proxy must read and transform the SIP. IPSec encrypts the SIP header, thus the intermediate SBC/Proxy can not even read the header. Additionally the layer credential matching issue as in TLS is also present.

The IPsec is a good alternative for securing the “first mile” – client to SBC. The protocol provides mutual authentication of SBC and client using certificates or shared secret. Additionally it can be combined with password authentication in SIP(client to SIP Server). This is very attractive alternative for provider, which already have an IPSec infrastructure, but only useful if both endpoints knows each other in advance.

3) **SMIME with SRTP** [SMI] SMIME gives the possibility for protecting the SDP and SIP payload. The SMIME allows mutual client to SBC authentication, when using SDP payloads. For this purpose, the SDP payload is signed by the sender’s private key. The receiver verifies cryptographically the signature and matches the id in the sender’s certificate with the SIP header. To protect against session hijacking, the SIP header must also be signed. According to the SIP standard this is done by tunneling the SIP header in the SDP payload. The hole SIP header is added as additional signed SMIME body. The result packet includes the SIP header twice - first over the UDP layer as usual and second tunneled in the SDP. This solves the authentication issue, but also make handling of the packet difficult. If there is a NAT device between the sender and receiver, the outer SIP header will be modified and the inside protected SIP header will stay unchanged. It can become difficult to differentiate between packet manipulation by a “good” intermediate device (NAT) or by an attacker.

The whole SDP payload cannot be client to client (end-to-end) encrypted in SMIME, because the intermediate devices SBC and SIP Server need to edit at least the RTP contact parameter. The main reasonable possibility is to encrypt and sign only the key-attribute in the SDP. The key attribute contains the protection key for the SRTP. In this way the key can be transmitted end-to-end in a secure way and servers can proceed the SIP packet. The disadvantage of SMIME in general is that the public key (or certificate) of the receiver must be known in advance. This could be problematic, because of forking in the SIP implementations. Forking is used when one client (same SIP URI) is registered multiple times with different devices. A call (invite) message is forked and delivered to all registered clients. If there are multiple registered clients with the same SIP URI, then all must have the same private key, since the SMIME can be decrypted only by owner of the private key.

To encrypt additional parts of the SDP body, except the key-attribute, brings not many advantages. We consider the other attributes e.g. codec type etc. as not security relevant.

Let us recapitulate: the use of SMIME make sense for authentication between the clients. Authentication of client to SBC is possible, but not very convenient. It can be used for end-to-end distribution of the SRTP key. When forking is used the same private key must be used in all devices. One of the restriction is, that SDP media before session establishment should not be used. (**Table 1**)

4) **MIKEY with SRTP** [MIK] MIKEY is a key exchange algorithm, which can be used for user authentication and key derivation for SRTP. It does not have any encryption properties. MIKEY messages are embedded in SDP attributes. This is a big advantage, because the key exchange is made without sending additional packets. MIKEY allows

for an end-to-end key exchange without any affection on the SBC or SIP proxy. MIKEY offers the following exchange modes: (1) Shared secret: Both clients authenticate each other using a shared secret. This is not a very scalable alternative and we are not considering it further. (2) Public/Private key encryption: The session key is generated by the initiator and signed by the public key of the receiver. The public key of the initiator and responder (receiver) must be known in advance and forking issue mentioned by SMIME exists also. (3) Diffie-Hellman with signatures: This is probably the most recommendable alternative in MIKEY. It uses the advantages of certificates with the Diffie-Hellman key exchange. The certificates requires PKI infrastructure. The PKI can use certificates issued from existing CA authority as for example Verisign. Self signed certificate can also be deployed for simplified PKI implementation.

MIKEY associated with SRTP is reasonable for end-to-end client authentication and RTP data protection. (**Table 1**). The forking issues must be carefully considered. It cannot be used for client to SBC protection.

5) **SIP.** The SIP standard provides the possibility for digest authentication. The SIP digest authentication is currently the most spread security technique for client to SBC authentication. The protocol achieves client to SBC authentication. Theoretically, username/password authentication can be used also for client-to-client authentication, which we consider as not usable.

It is important to stress that the security policy in most of the cases is source of many vulnerabilities. For example, protection against downgrade attacks must be handled by the local security policy. For this reason the implementation must pay significant attention on security policy.

All possibilities IPsec, SIPS + SRTP, SMIME + SRTP, MIKEY + SRTP are summarized in the following **Table 1**.

VI. Summary and Conclusion

Deploying security in the current Service Provider SIP implementations is a difficult task. There are many possibilities and combinations depending of the targets. The summary and recommendations are:

- Client to SBC confidentiality, called "first mile", is usually required when using high-risk access networks. For example: wireless hot spots or other public used access networks.

  IPSec: If the SP provider already have IPSec infrastructure is can by easily used for protect the first mile. The implementation is straight forward.

  SIPS + SRTP is possibility for protecting only outgoing calls in NAT environments, which the half of the desired protection.

- For "client to client" (end-to-end) authentication, **SMIME** can be a good alternative. It must be considered careful regarding "forking" and "media before SDP answer" issues.

- "Client to client" confidentiality can be achieved using **SMIME + SRTP**. In this case the RTP session is authenticated, integrity protected und encrypted, The SIP signaling is transmitted in clear. Advantage is that SMIME is a popular protocol with already existing libraries. **MIKEY + SRTP** achieves the same type of end-to-end protection. It's advantage is the use of key generation with Diffie-Hellman algorithm.

- **SIPS** alone can be used for signaling protection of the "first mile", thus Client to SBC. The RTP Data is in clear, which doesn't make much sense.

- For client to server authentication the usage of **SIP** digest authentication is in most of the cases sufficient.

In this paper we focus only on the existing RFCs form theoretical perspective. Before any deployment a careful study of the practical implementation must be done.

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

Table 1 Solution overview

References

[SIP] RFC 3261 "SIP: Session Initiation Protocol", June 2002
[SS7] Common Channel Signaling System No. 7, ITU, CCITT
[NAT] RFC 3022 "Traditional NAT", January 2001.
[TLS] RFC 2246, "The TLS Protocol", January 1999.
[IPS] RFC 2401,"Security Architecture for the IP", November 1998.
[SMI] RFC 2311,"S/MIME Version 2 Message Specification", 1998
[MIK] RFC 3830 ,"MIKEY: Multimedia Internet KEYing", August 2004
[SRTP] RFC 3711, "The Secure Real-time Transport Protocol ", 2004
[RTP] RFC 1889, "RTP: A Transport Protocol...", January 1996
[SIPL] RFC 3263, "SIP: Locating SIP Servers", June 2002
[MPX] "SIP, TCP/IP und Telekommunikationsnetze. NGN VoIP"", U.Trick, 2005
[BS64] RFC 3548, "The Base16, Base32, and Base64 Data Encodings", July 2003
[SSP] Jennings, Mahy "Client Initiated Connections in SIP", draft, 2007