A Survey of Requirements and Standardization Efforts for IP-Telephony-Security

Christoph Rensing[1], Utz Roedig[1], Ralf Ackermann[1], Ralf Steinmetz[1,2]

[1] Darmstadt University of Technology, Merckstr. 25, D-64283 Darmstadt, Germany
[2] GMD IPSI, Dolivostr. 15, 64293 Darmstadt, Germany
{Christoph.Rensing, Utz.Roedig, Ralf.Ackermann, Ralf.Steinmetz}
@KOM.tu-darmstadt.de

Abstract. Security as a dimension of trustworthiness in IP-Telephony systems and protocols is a main condition for the commercial success of IP-Telephony. In this work, we present a survey of security requirements and show how various standardization efforts address these requirements. We describe the basic tasks and elements of IP-Telephony systems and compare them to Telephony via PSTNs to derive some possible attacks for example. We classify the security preconditions to achieve trustworthiness of users and providers in this systems. We list weighty criteria for further evaluation of security mechanisms which can fulfil these requirements. After this, we describe the integration of security mechanisms in current IP-Telephony protocols and figure out work areas which have to be solved in future.

1 Introduction

Trustworthiness of service users and service providers in applications and systems is a necessary condition for commercial success of IP-Telephony also called "Voice over IP" and for the total replacement of Public Switched Telephone Networks (PSTN) by IP-Networks for Voice Communication, as it is predicted sometimes.

Trustworthiness in Information Technology Systems generally has different dimensions: correctness, availability and security. In this paper we are focusing on security, which is concerned about ensuring that a system resists potential attacks that can compromise the secrecy, integrity, or availability of data and services. To achieve security in IP-Networks is more sophisticated than in PSTNs. The risk to be attacked using IP-Telephony Infrastructure is higher than using PSTNs for a telephone call due of the differences of the networks and system architecture: IP-Networks are not centrally managed or controlled. In IP-Telephony voice transmission and signaling is done over the same IP-Networks. Active elements of an IP-Network, like routers or network-servers, are, by design, accessible from the network they control. Endpoints of IP-Networks, personal computers and servers, can be used to attack the network.

Single aspects of IP-Telephony security only are content of related work and IP-Telephony standards most times. The goal of this paper is, to give a complete survey of the risks of IP-Telephony, the resulting requirements and how they are addressed and possibly solved in the existing standards. In addition, we list some criteria which should be noted choosing security mechanisms.

2 IP-Telephony basic Tasks and their Security Requirements

PSTNs and IP Networks exist separately from each other for long days. In the last years voice and data networks are converging more and more. Three different kinds of convergence can be distinguished:

- Telecommunication Providers use IP-Access to configure and manage the PSTN components like exchanges or databases storing the operational Information for e.g. billing or charging.
- The service user request is triggered via an IP-Network, but the service is provided by the PSTN as transport infrastructure. The PINT-Working Group of the IETF [1] is concerned with this scenario.
- Voice transfer and signaling is done via one IP-Network. This is called *IP-Telephony* or "Voice over IP".

2.1 IP-Telephony basic Tasks

IP-Telephony should rather be a reengineering of existing PSTN services in the Internet but to implement new value added services. This is getting more and more important because the cost reduction argument for investigating in IP-Telephony will not be a strong argument in future [2]. Nevertheless, IP-Telephony systems and protocols have to carry out three basic tasks like in the old PSTNs. These basic tasks are the same in every scenario and have to be done for providing every service:

- *Signaling* addresses the set up and tear down of calls, including the setup and maintaining of databases and processors used for call routing and number translation.
- *Transmission* is the carrying of the audio and / or video data.
- *Operation* implies the provision, configuration and maintenance of all services which are used by providers and different users, like location services or charging- and billing services.

We distinguish these basic tasks in order to reduce the complexity of defining the security requirements and the mechanisms possibly used to fulfil these requirements.

2.2 IP-Telephony Infrastructure and Protocols

The current IP-Telephony Infrastructure is based on a decentral organized and managed architecture. Inside this, some islands e.g. in company networks are administered in a centralistic structure. The main signaling and operational functions are distributed over intelligent end systems and network servers in IP-Telephony architectures. In PSTNs, they are located in central nodes controlled by the providers in contrast. The end systems are either especially for IP-Telephony build computers, IP-Phones, or normal computers with software implemented phones like MS-Netmeeting. On the other side, there are network servers used for maintaining the signaling information and for operational functions. A common characteristic of these network servers is the decentral set-up and maintenance.

Currently, two major different protocol families for IP-Telephony exist. The ITU approach is described in the ITU H.323 umbrella standard [3]. H.323 is supported by the most existing systems and applications. In contrast, the IETF approach is based on the Session Initiation Protocol [4] for signaling. It is not in the focus of this paper to explain the different protocols and system architecture. They are described in detail in [5,6]. The appearing of network servers like named above is common in both architectures. In H.323 they are called Gatekeeper or Gateways. Proxy Server, Redirect Server, Registrars and Gateways are satisfying almost the same tasks in the IETF architecture.

2.3 Characteristics of IP-Telephony

The risk to be attacked using IP-Telephony Infrastructure is higher than using PSTNs for a telephone call due to the differences of underlying networks and system architecture:

- For IP-Telephony signaling, the same IP-Network as for audio transmission is used. This increases the options for fraud, because a user can maybe forge signaling informations like IP-addresses or user-IDs.
- IP-Telephony network elements are configured via the IP-Network in contrast to the PSTN, where the network servers are managed centrally. So, in IP-Telephony, these elements are accessible for users (and attackers) and have to be secured.
- In IP-Telephony, more functions are located in the decentral end-systems and network servers. This results in a higher effort to administrate these systems in a secure way and to achieve a high security level, than in an environment, where function is provided more centralized.
- In IP-Networks, mechanisms, to access data on different nodes of the network and to use them remote by the users (and possibly attackers) of the network, are available in general. Vulnerabilities of IP-Networks and end-systems (operating systems) are documented and people are more skilled with this. This increases the risk of an attack.
- Tapping in PSTNs is difficult, since the attacker needs a physical access to the wire the audio is transmitted. In an IP-Network the attacker only needs physical access to the network anywhere, when he gets logical access to a router or network server on the route from endpoint to endpoint.
- Most of the end systems in IP-Telephony are computers, which use and provide general network services in addition to telephony specific services. These computers and services can be attacked and can be used to compromise the entire telephone system.

In this work we only look at IP-Telephony related risks in depth and not at the risks of general network services or risk resulting by integration of new IP-Telephony services in existing IP-Networks.

2.4 Attacks on the basic Services

We show in the following some different workable attacks on the three basic tasks defined above, to clarify the listed risks.

Eavesdropping with a packet sniffer is the simplest *attack on the transmission service* in a non switched network. The attacker can listen the conversation. This attack can be done by everyone who has access to a general network node on the way from end system to end system. These can also be IP-Telephony related network servers like proxies or gateways, whose providers maybe can not be trusted.

Attacks on the signaling service can be used to fraud attacks. The caller ID or called ID can be changed and the attacker can use services he is not authorized to or without payment, when the service is with costs, for example. The signaling servers like gatekeepers or proxies and redirect servers can be attacked also. An invader can change the entries in the database for instance, so that all calls are rejected or forwarded to his own voice mail box. This can be done by direct access on the systems, which is not part of this work, or by sending a forged request to the signaling server. Traffic analysis is an other kind of attacks. It can be realized by eavesdropping the signaling informations. Especially service providers may not ignore this problems due of legal regulations.

Attacks on the operational services can result in wrong accounting, no provisioning of services an so on. They can be done on the one hand by direct attacks on the systems, these services are located on, or, on the other hand, by forged configuration or management commands in the same way.

Additionally, *general network attacks*, which are not especially IP-Telephony related, can be used. Such attacks are name server attacks or denial of service attacks for example.

2.5 Required Security Services

Five different security services are distinguished in principle. We are using the X.800 security services defined in [7] for future use. These are authentication, access control, confidentiality, integrity and non-repudiation. They are necessary for the IP-Telephony tasks transmission, signaling, operation and other not especially IP-Telephony related services in principle. We illustrate how these essential services are used for IP-Telephony, to figure out which services are essential.

Communication security is the part of security, this work is related with. It includes all security mechanisms which have to be integrated in the IP-Telephony specific protocol stack for signaling and transmission. Encryption of voice data respectively RTP-Streams and some signaling information is necessary for confidentiality. Encryption of voice data protects against some attacks on the transmission service. Authorization of service users, especially callers, has also to be part of signaling. It protects for misusing services. Authentication is a elementary requirement. Different kinds of authentication (end-system to end-system, end-system to network-system, network-system to network-system and hop by hop authentication) are needed. Hop by hop authentication is necessary, because a call can be forwarded via different domains with not trusted proxies or gatekeepers. End-system to network-system authentication is used, when an end-system registers at a network-system. Caller ID, Called ID and "who we thought we are calling"-ID are the informations that have to be authenticated at least. Authentication protects from many attacks on signaling and operational services.

It is not possible to describe all security requirements in detail in this work. In addition to the above categories, the following table shows an executive summary of the requirements, whereby the essential requirements are marked in grey.

Table 1: Security requirements for basic IP-Telephony tasks

	Signaling	**Transmission**	**Operation**
Authentication/ Integrity	end to end hop by hop end to network		end to end (a network servers in this context is a end system)
Non-Repudiation	especially for services which are liable for costs	not for simple calls, for special services e.g. voice information on call	outside IP-Telephony related services e.g. Billing
Confidentiality	for anonymity reasons for protection from traffic analysis	end to end (end to gateway)	for data protection reasons
Access Control	for particular service requests	not IP-Telephony specific but for used services e.g. QoS admission	for every management request
Key Management	end to end hop by hop	end to end (end to gateway)	outside IP-Telephony specific protocols

Key management is not a fundamental security requirement, but it is necessary for many cryptographic security mechanisms, used to ensure the other requirements. So, it is part of the table, though it is not clear, whether it is part of the IP-Telephony specific signaling itself or part of an external key exchange protocol.

Other security aspects has to be observed by manufactures and system administrators, using IP-Telephony solutions in addition to the communication security. We mention it in this work, because it is also essential form a security view.

Systems security covers well known requirements. Many manufacturers are developing new end systems like IP-Phones and network servers like Gatekeepers and Gateways. They can be combined with existing PBXs mostly. They are integrated in the corporate IP-Network on the other hand, since they are specialized computers in a distributed heterogeneous environment. The same security requirements have to be achieved for these systems like for existing computer systems and applications. Our observations from a big field trial [8] are, that many systems unfortunately do not meet the requirements. We will present our results after the vendors had time to fix the problems in detail.

The support of additional telephony services in an IP-Network should not result in new security risks for the environment, the IP-Telephony systems are integrated in. This can not be guaranteed in any case, because many existing security mechanisms are not designed for supporting IP-Telephony communication. The access from and to a corporate IP network is controlled via a firewall for example. Firewalls do often network address translation in addition. Both, existing firewall mechanisms like packet filters or proxies and network address translation, represent a problem for IP-Telephony protocols vice versa. This problem is described in [9] in detail. To enable IP-Telephony over existing firewalls, the security level has to be reduced in many cases. Therefore, new approaches for firewall architectures, as described in [10], or the support of firewalls by the IP-Telephony protocols, are necessary. The IETF SIP Working Group has addressed this problem as open task. First starting points are described in [11,12].

Laws and regulations have to be observed at the end. This leads to new requirements which are sometimes contradictionary to users requirements. For example lawful interception is a must in many cases.

2.6 Evaluation Criteria for Security Mechanisms

Many cryptographic mechanisms do exist. They are solving most requirements in principle, but not every solution can be used in every scenario. At this point, we list different criteria to evaluate the different mechanisms:

- Quality of service is a major concern for realtime IP-Telephony services. It must match or exceed that of PSTNs [13]. Different measures should be considered.
  The call setup delay is one significant aspect. The integration of cryptographic mechanisms can result in a bigger delay, especially if public-key mechanisms are used. The work overhead per sending and receiving packet for encryption and decryption is an other criteria. Asymmetric encryption of the coded audio data can not be done in realtime by simple end-systems. The bandwidth overhead, incurred by inflating the data packets via cryptographic transformations, should also be considered from the communication network point of view.
- Scalability is the second major concern. For commercial use, the implemented mechanisms have to work in large environments and not only in a testbed. Scalability can be observed on the different levels. The verification of a certificate or the number of different domains are examples.
- A precondition for choosing mechanisms is the general availability and operationality of the infrastructure, used by the cryptographic mechanisms inside the IP-Telephony protocols. Per-user public keys and the integration of Certification Authorities in the architecture are necessary for using public key mechanisms for example. An other example is the broad implementation of IPSec if it should be used.
- Reliability of security mechanisms is a further criteria. No single point of failure may exist.

- The grade of security the mechanisms provide is an other criteria. A reasonable grade has to be choosen. But, it is difficult to quantify the degree of security. For algorithms for example it depends on how hard they are to break [14].

The evaluation of security mechanisms is a difficult tasks, because all aspects do not have to be considered isolated. It is only necessary to address this task for the purpose of this paper.

3 Security Mechanisms in IP-Telephony Standards

Security mechanisms have to be part of the IP-Telephony standards due to meet the mentioned requirements and to achieve compatibility and operability between different IP-Telephony systems. We will describe where security is part of the standards and show where the requirements are realized in the following section. Our focus is on the main security requirements marked in Table 1.

3.1 Transmission Services

Confidentiality of the media streams is the primary requirement for transmission services. RTP [15] and RTCP are the underlying protocols used for transmission services in both IETF and ITU architecture. To realize confidentiality, the data streams have to be encrypted. This can be done after coding and segmenting the data by the sender. The encrypted segments can be sent as RTP data units and decrypted by the receiver. The RTP-Headers are not encrypted. The use of symmetric encryption is necessary, due to the bad performance of asymmetric encryption. The ITU suggests the encryption of the media streams in this way in H.235 [16]. The encryption capabilities of the systems can be negotiated during signaling. DES, Triple DES and RC2 are intended as encryption algorithms. SIP covers only the signaling, but the encryption of the media streams is possible in the same way. RTCP security is not done so far.

The use of symmetric encryption results in the necessity, to exchange session keys between the partners. The key management is not part of the transmission service (RTP) itself. It is part of the H.245 signaling in the ITU world and not defined in SIP. So the key management has to be part of the SIP message body.

3.2 Signaling Services

Authentication, confidentiality and in addition key management are the two major security requirements for signaling. The realisation of this security services differs in the two approaches.

ITU H.235. Recommendation H.235 retains the security aspects within the H.323 protocol family. Authentication and call authorization is necessaryly done during call establishment and sometimes before the call is accepted. TLS [17] or IPSec [18] on transport or network layer are the only possibilities to realize this. Authentication of users is supported during call control. It is done either during the initial call connection in the process of securing the signaling-channel (H.245) by support of challenge response mechanisms or by exchanging certificates on the H.245 channel. H.245 [19] supports the negotiation of the necessary parameters. Hop by hop authentication is provided by using this mechanisms only. End to end authentication is not provided.

In H.235 two security profiles are defined. The simple security profile and the signature profile. Both profiles do not cover the confidentiality of the signaling information, except using TLS or IPSec. The key management is part of the profiles. The exchange of certificates and a Diffie Hellmann key exchange are supported. But the key management only covers the exchange of certificates, not the criteria by which they are mutually verified and accepted.

SIP. Security support is inside the SIP protocol. There is a hard discussion about which problems should be solved in the Working Group actually. From this, we can only describe the existing RFC.

SIP requests may be authenticated using the Authorization header field to include a digital signature of certain header fields, the request method and version number and the payload. For authentication PGP or HTTP authentication are intended. Not all header fields can be authenticated, because they have to be changed possibly by proxies. So, end to end authentication is not achieved completely. On the other hand, hop-by-hop authentication can be provided. It is not specified which mechanism should be used on the underlying layers. IPSec and TLS are discussed.

SIP supports three complementary forms of encryption to protect confidentiality. End-to-end encryption of the SIP message body and certain sensitive header fields; hop-by-hop encryption to prevent eavesdropping that tracks who is calling whom; hop-by-hop encryption of Via fields to hide the route a request has taken. Not all header fields can be encrypted because they are used for call routing. Additionally SIP requests and responses may also be protected by security mechanisms at the transport or network layer, maybe IPSec or TLS. The specification of using a particular mechanism is not part of SIP signaling. It has to be specified outside of the signaling.

3.3 Operational Services

Many different protocols have to be surveyed for securing operational services. The security requirements are strongly related to systems security most times, if the services are maintained and configured by closed groups, e.g. by the providers of the services. This is in contrast to the management of signaling information. In this case, well known mechanisms for authentication and authorization can be used. Due to this characteristic, we will not focus the operational aspects so far.

3.4 Summary

The major security requirements are covered in the standardization efforts, as shown in Table 2. Many additional requirements, like non repudiation, are not performed. Eventually, this prevents the evaluation of new commercial services. An other disadvantage is the use of mechanisms which are not spreaded, like IPSec or the use of public key certificates. We do not believe, that every user of an IP-Phone holds a public key certificate. Also, some other criteria we defined, are not accomplished. The verification of certificates during call establishment grows up the setup delay. Also, such mechanisms maybe do not scale in large environments. The evaluation of the mechanisms in detail by using the criteria listed above, is for future work.

Table 2: Security support in the IP-Telephony protocols

	Signaling	**Signaling**	**Transmission**	**Transmission**
	ITU (H.323)	IETF (SIP)	ITU (H.235)	IETF (SIP)
Authentication/ Integrity	hop by hop	end to end apart from some header fields; hop by hop by TLS or IPSec	not supported	not supported
Non-Repudiation	part of signature security profile	not supported	not supported	not supported
Confidentiality	only by TLS or IPSec	end to end apart from some header fields; hop by hop by TLS or IPSec	end to end RTP encryption	end to end RTP encryption
Access Control	not supported	by authentication of SIP requests	not supported	not supported
Key Management	different mechanisms	not defined	part of H.245 signaling	part of SIP message body

4 Conclusion and future work

IP-Telephony Security was given less or no attention in recent years. Nowadays, when IP-Telephony becomes a commercial available service and many vendors implement systems, it is necessary to support security mechanisms by the protocols and to build secure systems and applications. This demand is recognized by the standardization bodies during the last months. ETSI-TIPHON has founded a new working group “TIPHON Security” at End of 1999 [20]. The IETF-SIP Working Group has consensus to make security a WG effort. An informal design team has the goal, to clarify the SIP specification with respect to security and to describe practices and mechanisms for interaction with other security systems. The discussion started at the 47th IETF meeting in March 2000 [21].

Much work has to be done, we think. Especially, many security mechanisms, which are discussed in the different groups, like IPSec, are not in widespread use. Additionally, it is insufficient to define the standards, they have to be implemented. No commercial implementation, supporting confidentiality of transmission, exists to our knowledge. It is useful to point out the security aspects. Therefore, we give a review of the different requirements, evaluation criteria and standardization efforts in this paper. Our main focus of future work will be on integration of authentication mechanisms in signaling protocols, systems vulnerability and firewall mechanisms for multimedia communication in general.

References

1 H. Lu, M. Krishnaswamy, L. Conroy, S. Bellovin, F. Burg, A., DeSimone, K. Tewani, P. Davidson, H. Schulzrinne, K. Vishwanathan: “Toward the PSTN/Internet Inter-Networking--Pre-PINT Implementations” RFC 2458, November 1998

2 C. A. Polyzois, K. H. Purdy, P. Yang, D. Shrader, H. Sinnreich, F. Ménard and H. Schulzrinne: "From POTS to PANS -- A Commentary on the Evolution to Internet Telephony," IEEE Network, vol. 13, no. 3, pp. 58--64, May/June 1999.

3 ITU-T Recommendation H.323 V.2 ”Packet-Based Multimedia Communication Systems”, Februar 1998.

4 M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg: “SIP: Session Initiation Protocol” RFC 2543, März 1999.

5 I. Dalgic, H. Fang: “Comparsion of H.323 and SIP for IP Telephony Signaling” In Proceedings of Photonics East, Boston, Massachusetts, September 20-22, 1999.

6 B. Douskalis: “IP Telephony - The Integration of Robust VoIP Services” Prentice Hall, 2000.

7 ITU: “X.800, Security Architecture for Open Systems Interconnection for CCITT Applications” 1991.

8 KOM, TU Darmstadt; http://www.kom.e-technik.tu-darmstadt.de/~rac/personal/IPTEL_FRONTPAGE/iptel_field_trial.html

9 Utz Roedig, Ralf Ackermann, Ralf Steinmetz: “Evaluating and Improving Firewalls for IP-Telephony Environments” In Proceedings of the 1st IP-Telephony Workshop (IPTel2000), ISSN 1435-2702, GMD-Forschungszentrum Informationstechnik GmbH, April 2000

10 U. Roedig, R. Ackermann, C. Rensing and R. Steinmetz: “DDFA Concept” Technical Report KOM-TR-1999-04, KOM, December 1999

11 B. Biggs: “A SIP Application Level Gateway for Network Address Translation” Internet Draft, draft-biggs-sip-nat-00.txt.

12 J. Rosenberg, D. Drew, H. Schulzrinne: “Getting SIP through Firewalls and NATs”, Internet Draft, draft-rosenberg-sip-firewalls-00.txt.

13 T. Eyers and H. Schulzrinne, "Predicting Internet Telephony Call Setup Delay," in Proceedings of the 1st IP-Telephony Workshop (IPTel 2000), ISSN 1435-2702, GMD-Forschungszentrum Informationstechnik GmbH, April 2000

14 B.Schneier: “Applied Cryptography” John Wiley & Sons, New York, 2. Auflage, 1996.

15 H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson: “RTP: A Transport Protocol for Real-Time Applications” RFC 1889, IETF, Jan. 1996

16 ITU-T Recommendation H.235 ”Security and Encryption for H. Series (H.323 and other H.245 based) Multimedia Terminals”, Februar 1998
17 T. Dierks and C. Allen: “The TLS Protocol Version 1.0”, RFC 2246, Januar 1999.
18 R. Thayer, N. Doraswamy und R. Glenn: “IP Security Document Roadmap” RFC 2411, November 1998.
19 ITU-T Recommendation H.245, Version 3 “Control Protocol for Multimedia Communication” September 1997
20 ETSI TIPHON: “15 meeting report (Leipzig October 4 – 8, 1999)”, http://docbox.etsi.org/tech-org/tiphon/Document/tiphon/03-permanent/(99)23.doc
21 http://www.softarmor.com/sipwg/teams/sipsec/index.html