A Technology Independent Security Gateway for Real-Time Multimedia Communication

Fudong Li[1], Nathan Clarke[1,2], and Steven Furnell[1,2]

[1] Centre for Security, Communications and Network Research (CSCAN), School of Computing & Mathematics, Plymouth University, Plymouth, PL4 8AA, United Kingdom
info@cscan.org
[2] School of Computer and Information Science, Edith Cowan University, Perth, Western Australia

Abstract. With currently more than 178 million users worldwide, the demand on real-time multimedia communication services (e.g. VoIP, video conference) grows steadily. However, whilst the protocols utilised in such communications are standardised, internal aspects are not. For example, if calling parties utilise incompatible media codecs or security mechanisms, a real-time multimedia communication cannot be established. The latter would result in either a failure to establish a connection or a plaintext connection that leaves the communication open to attacks. This paper proposes a novel technology independent security gateway for real-time multimedia communications which offers ciphering assistance for these terminals when they have incompatible security mechanisms and/or media codecs, allowing them to communicate in a seamless and secure manner despite their incompatibilities. The proposed security gateway operates across standard IP protocols and provides a flexible, scalable and robust system that is capable of managing the ciphering requirements of a modern communications system.

Keywords: IMS, security gateway, SIP, cross-ciphering.

1 Introduction

With the foundation laid by the IP Multimedia Subsystem (IMS), Internet users can establish real-time multimedia calls not only within the Internet Protocol (IP) world but also interconnect with terminals from other types of communication networks, such as the traditional telephony network and Terrestrial Trunked Radio (TETRA) networks. For instance, users can utilise their IMS terminals to participate a business video conference, make a Voice over IP (VoIP) call to a normal telephone and even communicate to a police officer's TETRA terminal in a life threaten situation [1]. In comparison with other communication networks, the IMS architecture provides a cheap, flexible and convenient communication channel to many Internet users. Indeed, with currently more than 178 million subscribers worldwide, the demand on real-time multimedia communication services grows steadily on a yearly basis [2].

J. Lopez, X. Huang, and R. Sandhu (Eds.): NSS 2013, LNCS 7873, pp. 14–25, 2013.
© Springer-Verlag Berlin Heidelberg 2013

In order to facilitate the high demand for real-time multimedia communication services, various types of terminals have been developed by different providers around the world [3]. Within the IMS architecture, it is universal that these terminals rely upon the Session Initiation Protocol (SIP) for call setup and control in the signalling plane and the Real-time Transport Protocol (RTP) or Secure RTP (SRTP) for media transmission in the media plane [4-6]. However, they can utilise various types of codecs to encode and decode the media and different security mechanisms to secure the media transmission. As a result, in addition to the existing mismatch issues among terminals from different communication networks (e.g. between IMS and TETRA), this may also create incompatibility issues (e.g. early call termination during the setup phase in the signalling plane) between various IMS terminals.

Regarding the challenge posed by incompatible codecs, many media gateways have been devised in the media plane for the purpose of transcoding (i.e. converts media data from the format of one codec into another's), enabling two terminals to establish a communication despite utilising different codecs and/or from different network domains [7]. For instance, Asterisk which is one of the most popular open source media gateways supports more than 10 popular codecs enabling various transcoding options, such as facilitating an IMS terminal which utilises G.711 codec to communicate a normal mobile phone terminal which employs Adaptive Multi-Rate Narrowband (AMR-NB) codec [8]. Another example, by utilising its own media gateway, Skype, one of the most well-known proprietary VoIP applications, can establish communication with landline telephones despite utilising different codecs.

When users utilise different media security mechanisms within terminals to communicate with one another, a call cannot be established in normal circumstances unless in plain text (i.e. RTP format). However, it is well documented that unprotected real-time media traffic is open to eavesdropping and man-in-the-middle attacks [9]. By utilising these tricks, attackers can collect user's sensitive information (e.g. bank account details) and then abused them. As a result, a security gateway, which can provide ciphering support (i.e. transforms encrypted data from one format to another), is required to ensure the communication can be established and protected between security mechanisms and/or media codecs incompatible terminals. In comparison with the maturity of the media gateway, little work has been carried out on investigating the need of a security gateway. Therefore, this paper proposes a novel technology independent security gateway for real-time multimedia services that can provide ciphering support for terminals with incompatible security controls allowing them to communicate in a safe and secure fashion.

This paper begins by presenting the popularity and importance of the real-time multimedia services. The paper then proceeds to describe existing gateways that support real-time multimedia services. In section 3, a novel technology independent security gateway for real-time multimedia communication is proposed and details of its components, capabilities, working modes and challenges are thoroughly described and discussed. The paper finishes by highlighting the future development of the security gateway.

2 Existing Gateways for Real-Time Multimedia Services

In order to allow real-time multimedia services to run smoothly between incompatible terminals and/or different types of communication networks, a gateway which provides media and/or security support is required (as illustrated in Figure 1). During a call setup phase, control elements (e.g. Serving Call Session Control Function (S-CSCF)) of a communication network (e.g. IMS) examine the capability of the caller and callee's terminals and decide whether the assistance of the gateway is required; if it is required, the element of the signalling plane will notify the Resource Function Controller of the gateway and exchange configuration parameters with it for setting up both the incoming and outgoing legs. Once the call setup phase is completed, the Resource Function Processor of the gateway will provide the media and/or ciphering support in a transparently manner allowing two terminals to communicate despite their incompatibility.

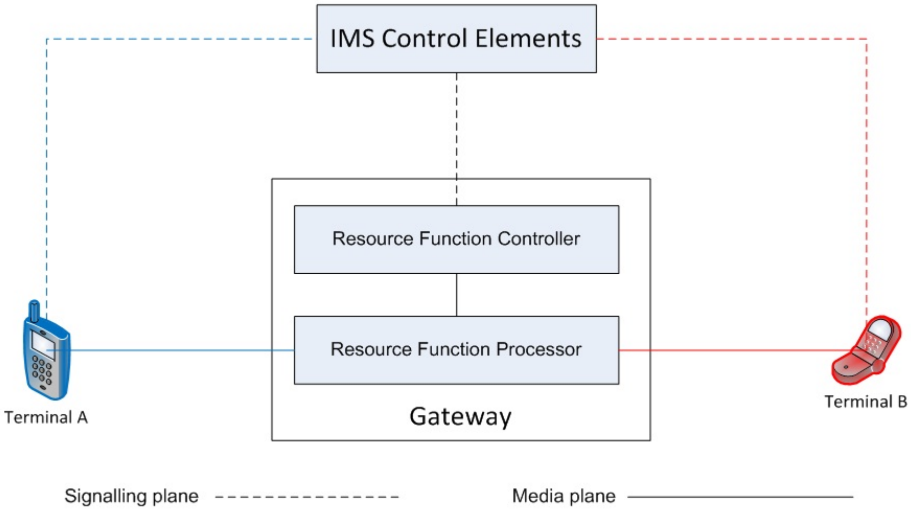

Fig. 1. A generic gateway for real-time multimedia services

Based upon the functionality, a gateway can be either categorised as a media gateway or a security gateway.

A media gateway is dedicated to provide media support when terminals have incompatible codecs. It is further divided into a Media Resource Function Controller (MRFC) and a Media Resource Function Processor (MRFP) [10]. The MRFC is a signalling node that is in charge of interpreting information coming from the signalling plane and also controlling the MRFP; the MRFP is a media plane node that is utilised to transparently perform media transcoding process if required. Ideally, the media gateway should be equipped with as many codecs as possible, to support a wide range of transcoding tasks.

The idea of the media gateway was first proposed in 1999 by [11], describing a VoIP call being established between terminals from Asynchronous Transfer Mode (ATM), IP and Integrated Services Digital Network (ISDN) networks despite the incompatibility of the terminals. Since then much research in the field of media gateways have been carried out to provide interoperability between incompatible terminals from the same or different networks, including: [12-16]. In addition to the work performed by the research community, telecommunication bodies and manufacturers have also contributed significantly towards the maturity of the media gateway. For instance, 3rd Generation Partnership Project (3GPP) has published a series of technical reports (e.g. 3GPP TS 29.232 (from release 4 to 12) on regulating the functionalities of the media gateway [17]. Also, Cisco, one of the world leading networking equipment manufacturers, has a wide range of gateways, which can support multimedia communication [18]. Nevertheless, it is not authors' intention to discussion the capability and performance of these existing media gateways, but to highlight the amount of work have been given in the area of media gateway.

A security gateway is designed for providing ciphering support when terminals have different security mechanisms and/or incompatible codecs. Similar to the media gateway, it should also have two components: Security Resource Function Controller (SRFC) and Security Resource Function Processor (SRFP). The SRFC is a signalling node that communicates with other controlling functions in the signalling plane and also controls the SRFP. In order to provide ciphering assistance, the security gateway should also support as many security mechanisms as possible.

With the purpose of providing security for the real-time multimedia traffic, several media gateways are equipped with security mechanisms to support SRTP traffics. [19] describes a security gateway that provides secured communications for terminals that do not support any security controls within its local network. As a result, the call is transported in plain text between the security gateway and the security incompatible terminal, allowing anyone on the same local network to listen to the conversation via a network monitoring tool (e.g. Wireshark). Asterisk, one of the most popular open source media gateways, offers terminals with same security compatibilities to establish secured communication [20]; nonetheless, it cannot provide any cross-ciphering support for terminals with incompatible security mechanisms. Skype, one of the most popular proprietary VoIP applications, utilises AES encryption to secure end-to-end Skype-to-Skype calls [21]; however, it does not support interoperability with any other proprietary or open source VoIP applications. In addition, as these existing gateways are designed predominately for the purpose of transcoding, it would be difficult for them to provide sufficient security support to these high demands real-time multimedia services. Therefore, a dedicated security gateway that can provide ciphering support allowing interoperability between incompatible terminals is required for real-time multimedia services.

In the next section, a novel security gateway that can provide interoperability support for incompatible terminals will be proposed and fully described, along with its internal components and functionalities.

3 A Technology Independent Security Gateway for Real-Time multimedia communication

With the purpose of enabling a wide range of incompatible terminals to securely communicate with each other at a high level of performance, a novel technology independent security gateway (TI-SGW) for real-time multimedia service is proposed. In order to provide the ciphering support in a secure and timely fashion, a number of internal modules of the TI-SGW architecture have been devised and are illustrated in Figure 2.

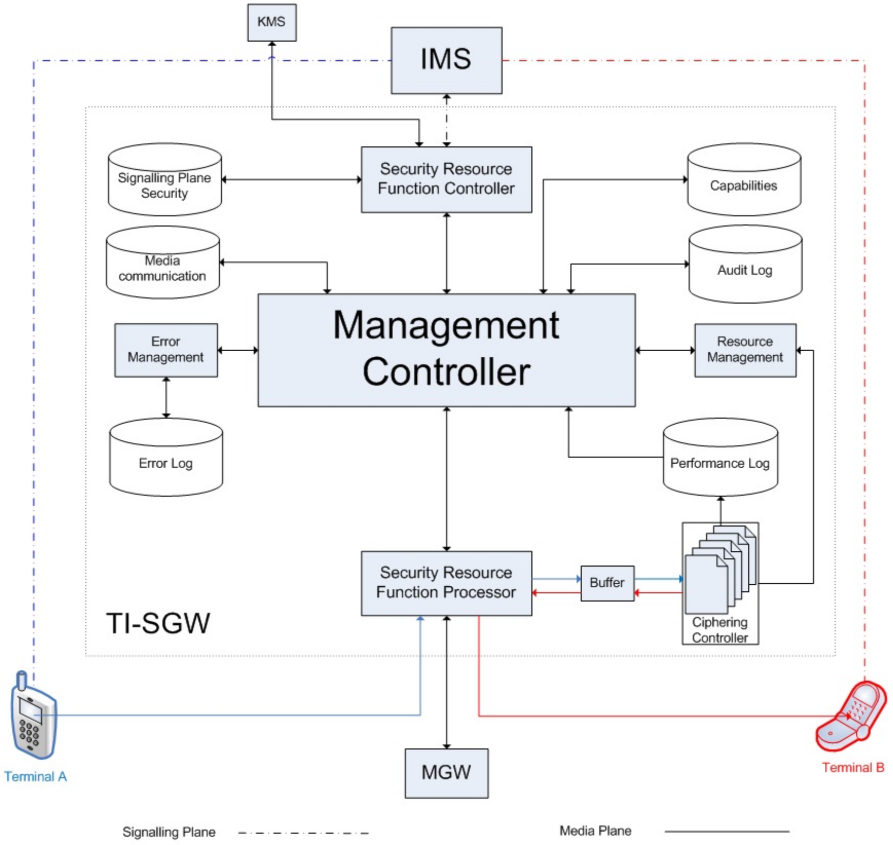

Fig. 2. TI-SGW Architecture

The architecture is largely divided into three areas: the signalling, media and management segments. For the signalling plane, its principal responsibility is to securely establish signalling communication with the IMS controlling system. From the IMS controlling system, the TI-SGW can obtain all the parameters required to set up a seamless media plane ciphering process for both calling parties upon request.

The media plane is responsible for identifying incoming media flows, applying appropriate ciphering on the media and forwarding it to the appointed receivers in a secure and timely manner. The Management segment of the TI-SGW controls both the media and signal plane interfaces and also provides resource management, error control, performance monitoring and accountability functionalities.

3.1 Components of the TI-SGW Architecture

The following sections describe each of the architectural components in more detail, providing an overview of its role and the relationship between components.

Security Resource Function Controller (SRFC) is mainly responsible for establishing mutual authentication with the IMS signalling plane and determining the parameters for setting up media plane security when any ciphering assistance is required. Two functions have been designed to achieve these responsibilities:

- Authentication function (TI-SGW-AF)
- Media plane security setup function (TI-SGW-MPS)

The TI-SGW-AF is employed to facilitate all signalling plane security setup procedures between the TI-SGW and the IMS signalling plane, including mutual authentication, key establishment and security association setup [22]. In addition, the TI-SGW-AF is utilised to perform the mutual authentication process between the TI-SGW and a Key Management Server (KMS). This permits the TI-SGW to securely request and retrieve keys and tickets from the KMS when a KMS is utilised as the key management solution. All details to assist the setup of authentication processes are stored in the Signalling Plane Security database.

The TI-SGW-MPS is responsible for configuring the security associations for the setup of media transmissions between the TI-SGW and a real-time multimedia terminal. When ciphering assistance is requested, the TI-SGW-MPS selects an appropriate set of crypto suite and key management solutions from a capability list to set up both the incoming and outgoing calling legs. Also, all the information which is related to the configuration, such as caller and callee's contact details (e.g. IP addresses), their crypto suites and key management solutions, will be securely stored in the Media Communication database as a reference for the later ciphering process in the media plane.

Security Resource Function Processor (SRFP) is the interface of the TI-SGW to any media transmissions. Upon receiving the media traffic, the SRFP inspects it based upon the information stored in the Media Communication database for obtaining details (e.g. cipher keys) which will be utilised for requesting computing resources (e.g. storage and processing power) to establish the ciphering process. Once the ciphering process is completed, the SRFP will send the processed media to the appointed receiver. Details of the whole process will then be stored in the Audit Log for the purpose of accounting.

Resource Management is employed to manage the allocation of computer processing resource for the ciphering process. It constantly monitors the resource, and reserves and distributes it based upon each ciphering request. At the same time, it also gathers all necessary security parameters (e.g. crypto suites) from each request and passes it onto the ciphering process. This will enable the ciphering process to be taken smoothly and also enable the TI-SGW to scale up accordingly with large volumes of media connections.

Ciphering Controller serves the TI-SGW by providing the actual ciphering and deciphering process. Upon receiving the media data, it decrypts the media on the incoming leg by utilising crypto suites and cipher keys that are used by the caller; and then encrypts the plain text media by employing crypto suites and ciphering key which are utilised by the callee. As the TI-SGW is designed to serve multiple incoming communications, the ciphering function operates in a multitasking manner. All details of ciphering process (e.g. cipher suites and time of ciphering process) will be stored in the Performance Log storage for the purpose of valuation of the ciphering process. For media connections that also require a change in codec, the deciphered text is sent to a media gateway (MGW) for transcoding prior to the re-ciphering process.

Error Management provides oversight and control of internal errors that can arise from any unexpected events that may be experienced. Controls will ensure errors within any of the architectural components are identified and reported. All details of the error event will be stored in the Error Log for the purpose of accountability.

Management Controller is the primary controller of the TI-SGW that regulates the system and liaises between components. Apart from overseeing the entire ciphering process, it is also responsible for managing the ciphering capability of the TI-SGW and the feedback of the ciphering process; both tasks are carried out by the Capability List function and the Performance Enquiries function respectively.

- **Capability List function:** By default, the TI-SGW is equipped with various crypto suites and key exchange solutions that are utilised to assist the ciphering process. During the setup process of these security mechanisms, details of them are extracted by the Capability list function and then stored in the Capabilities storage. This is utilised to assist the negotiation of the media plane security during the call setup process.
- **Performance Enquiries function:** is utilised to present answers to any enquires regarding the performance of the ciphering process which is stored in the Performance Log storage, such as which crypto suite was utilised, how long a typical ciphering process takes, what the memory and processing consumptions are for a particular ciphering task. The primary propose of this function is to ensure the ciphering process is undertaken in a timely manner and in accordance with Quality of Experience (QoE) expectations. The resulting audit is useful in identifying particular issues with crypto suites and performance. For instance, security policies could be amended based upon particular performance characteristics of certain crypto suites.

3.2 Ciphering Capability of the TI-SGW

As mentioned in the previous section, the main task of the TI-SGW is to provide ciphering assistance. In order to offer the assistance whenever it is requested, the TI-SGW needs to support as many real-time multimedia security mechanisms as possible. It is well established that these security mechanisms utilise the SRTP as the fundamental protocol for securing the real-time multimedia traffic and the SRTP employs a number of crypto suites and key exchange solutions to achieve that. Therefore, all the crypto suites and key exchange solutions which the TI-SGW should support are described in the following section.

Crypto Suites of the TI-SGW. A crypto suite is a combination of encryption and message authentication code (MAC) algorithms that provide confidentiality, integrity and authentication for data. The default encryption method for the SRTP is Advanced Encryption Standard (AES) which can operate in two modes: Segmented Integer Counter Mode AES (AES_CM) and AES in f8-mode [6]; while the default message authentication and integrity method for the SRTP is HMAC-SHA1 [6]. By utilising the combination of encryption methods, message authentication and integrity solutions, in addition to various key lengths, a number of crypto suites (as demonstrated in Table 1) can be obtained [23-24]. Furthermore, it is envisaged that the TI-SGW should also provide support for future releases of crypto suites for the SRTP, enabling future compatibility and longevity of the system.

Table 1. A list of crypto suites of the SRTP

Crypto suites
AES_CM_128_HMAC_SHA1_80
AES_CM_128_HMAC_SHA1_32
AES_F8_128_HMAC_SHA1_80
AES_192_CM_HMAC_SHA1_80
AES_192_CM_HMAC_SHA1_32
AES_256_CM_HMAC_SHA1_80
AES_256_CM_HMAC_SHA1_32

Key Exchange Solutions of the TI-SGW. A number of key exchange protocols have been proposed to manage the key exchange between terminals to enable the establishment of the SRTP communication [25]. The decision as to whether the assistance of the TI-SGW should be required is decided by the IMS signalling plane. Any potential key exchange protocols of the TI-SGW must be indicated and initialized in the IMS signalling plane, otherwise the call which is meant to be supported by the TI-SGW cannot be established. Therefore, key management solutions that utilize the media plane for advertising their usage will not be supported by the TI-SGW. Based upon these premises, the IT-SGW will support the following key exchange protocols: Session Description Protocol (SDP) Security Descriptions for Media Streams (SDES) [23], MIKEY pre-shared key (MIKEY-TICKET) [26], MIKEY-public key encryption (MIKEY-IBAKE) [27], IMS Authentication and Key Agreement (AKA) [25], Otway-Rees based key management solution [25] and ZRTP [28]. In addition, the

TI-SGW should be easily adaptable with any future key exchange solutions that also utilize the IMS signalling plane for initialization of the key management.

3.3 Operational Modes of the TI-SGW

When two terminals share common codecs and security mechanisms, the media flow can be directly established between them. While two terminals do not have common security mechanisms and/or codecs, the TI-SGW and/or MGW will be required in the media flow to provide ciphering and/or transcoding support respectively allowing interoperability between the two incompatible terminals. The usage of the MGW is required only when two calling parties do not share common codecs. In comparison, the need of the TI-SGW will be compulsory in the following three scenarios:

1. Two terminals do not share same security mechanisms but same codec.
2. Two terminals do not share same security mechanisms or same codec.
3. Two terminals do share same security mechanisms but not same codec.

Each of these scenarios defines one working mode of the TI-SGW. As a result, the TI-SGW has three working modes accordingly to the above scenarios:

- Cross-ciphering mode **without** the presence of the MGW.
- Cross-ciphering mode **with** the presence of the MGW.
- Mono-ciphering mode **with** the presence of the MGW.

3.4 Challenges of the TI-SGW

The proposed the TI-SGW can provide ciphering support for the real-time multimedia services whenever it is required. Hence, this solution can ensure that the real-time multimedia services are protected during a session despite terminals may have incompatible security mechanisms and/or codecs. Nonetheless, there are a number of challenges that the TI-SGW has both internally and externally.

For the internal challenges, they are related to the TI-SGW itself, including the security mechanism, multitasking and performance:

- Security mechanisms: the TI-SGW needs to be regularly updated with any newly released security mechanisms to ensure that the gateway can provide maximum ciphering support for the real-time multimedia services.
- Multitasking: the TI-SGW is required to simultaneously handle multiple ciphering jobs if required. These jobs can be concurrently carried out in various working modes of the TI-SGW. In addition, should operational requirements exceed a singular TI-SGW, a load-balancing approach with multiple TI-SGWs can be implemented.
- Performance: as the real-time multimedia services require a high level of demand on performance. The TI-SGW has to be able to complete the ciphering job in a timely manner to minimise the impact that is introduced by the encryption and decryption process.

For the external challenges, they are the surrounding environments and factors which affect the TI-SGW, including:

- Upgrading of the IMS control element: the IMS control element (e.g. SCSCF) is required to be equipped with an intelligent function which can intercept and analyse the SDP message, detect the need of the TI-SGW and configure it for the ciphering support.
- Regulations: efforts of standardisation bodies and industrial forums are also required for setting up new standards and regulations to govern the development of the TI-SGW and avoid any incompatibilities between any future security gateways.

All of the aforementioned challenges are critical for the development of the TI-SGW as any of them can affect the role that the TI-SGW is designed to complete, enabling a secured communication channel between media security mechanisms and codecs incompatible terminals to be established.

4 Conclusions and Future Work

The paper has identified the need for a technology independent security gateway that is capable of meeting the needs of incompatible security requirements in an efficient and effective manner. The proposed TI-SGW has been devised to incorporate a series of management control functions that permit various performance and accountability functions in addition to providing wide-spread security compatibility.

In the next phase of the research, a prototype of the designed security gateway that can provide ciphering assistance for incompatible terminals of real-time multimedia services will be developed. This will be incorporated within a complete inter-domain IMS/TETRA-based system that will permit an operational evaluation of the system. With respect to performance, a series of experiments will be devised to study the ciphering, multitasking and performance capabilities of the security gateway.

Acknowledgements. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement 284863 (FP7 SEC GERYON).

References

1. Aiache, H., Knopp, R., Koufos, K., Salovuori, H., Simon, P.: Increasing Public Safety Communications Interoperability: The CHORIST Broadband and Wideband Rapidly Deployable Systems. In: IEEE International Conference on Communications Workshops, ICC Workshops 2009, June 14-18, pp. 1–6 (2009), doi:10.1109/ICCW.2009.5208003
2. Infonetics Research: VoIP services market growing strong as businesses seek flexibility, easier management (2012), http://www.infonetics.com/pr/2012/VoIP-UC-Services-Market-Forecast-and-SIP-Trunking-Survey-Highlights.asp

3. Myvoiprovider: Top 100 VoIP Provider World Ranking (2012), http://www.myvoipprovider.com/en/Top_100_VoIP_Providers
4. Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., Schooler, E.: SIP: Session Initiation Protocol. RFC3261, IETF (2002), http://www.ietf.org/rfc/rfc3261.txt
5. Schulzrinne, H., Casner, S., Frederick, R., Jacobson, V.: RTP: A Transport Protocol for Real-Time Applications. RFC3550, IETF (2003), http://www.ietf.org/rfc/rfc3550.txt
6. Baugher, M., McGrew, D., Naslund, M., Carrara, E., Norrman, K.: The Secure Real-time Transport Protocol (SRTP). RFC 3711, IETF (2004), http://www.ietf.org/rfc/rfc3711.txt
7. Voip-Info: VoIP Gateways (2012), http://www.voip-info.org/wiki/view/VoIP+Gateways
8. Asterisk: Codec Modules (2012), https://wiki.asterisk.org/wiki/display/AST/Codec+Modules
9. Keromytis, A.D.: A Comprehensive Survey of Voice over IP Security Research. IEEE Communications Surveys & Tutorials 14(2), 514–537 (2012), doi:10.1109/SURV.2011.031611.00112
10. 3GPP TS 24.147: Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3, release 11 (2012), http://www.3gpp.org/ftp/Specs/html-info/24147.htm
11. Grilo, A.M., Carvalho, P.M., Medeiros, L.M., Nunes, M.S.: VTOA/VoIP/ISDN telephony gateway. In: 1999 2nd International Conference on ATM, ICATM 1999, pp. 230–235 (1999), doi:10.1109/ICATM.1999.786807
12. Conte, A., Anquetil, L.P., Levy, T.: Experiencing Megaco protocol for controlling non-decomposable VoIP gateways. In: Proceedings of the IEEE International Conference on Networks (ICON 2000), pp. 105–111 (2000), doi:10.1109/ICON.2000.875776
13. Castello, F.C., Balbinot, R., Silveira, J.G., Santos, P.M.: A robust architecture for IP telephony systems interconnection. In: 2003 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, PACRIM, August 28-30, vol. 2, pp. 593–596 (2003), doi:10.1109/PACRIM.2003.1235851
14. Yoo, H.K., Kang, B.R.: A media stream processing of VoIP media gateway. In: The 9th Asia-Pacific Conference on Communications, APCC 2003, September 21-24, vol. 1, pp. 91–94 (2003), doi:10.1109/APCC.2003.1274318
15. Guo, Y., Liang, M., Guo, Y., Zhang, L.: A design scheme of PSTN media gateway. In: Proceedings of the 2004 7th International Conference on Signal Processing, ICSP 2004, August 31-September 4, vol. 3, pp. 2651–2654 (2004), doi:10.1109/ICOSP.2004.1442327
16. Kang, T., Bae, H., Kim, D., Kim, D.: SIP/SDP signaling of media gateway with transcoding function in converged network. In: The 6th International Conference on Advanced Communication Technology, vol. 2, pp. 842–845 (2004), doi:10.1109/ICACT.2004.1292988
17. 3GPP TS 29.232: Media Gateway Controller (MGC) - Media Gateway (MGW) interface; Stage 3 (2012), http://www.3gpp.org/ftp/Specs/html-info/29232.htm
18. Cisco: Voice and Unified Communications (2012), http://www.cisco.com/en/US/products/sw/voicesw/products.html
19. Li, J.S., Tzeng, J.J., Kuo, C.M.: Building Security Gateway. In: International Conference on Information Networking, ICOIN 2009, January 21-24, pp. 1–3 (2009)
20. Asterisk: Secured calling tutorial (2011), https://wiki.asterisk.org/wiki/display/AST/Secure+Calling+Tutorial

21. Skype: Privacy and Security (2012), https://support.skype.com/en/faq/FA31/does-skype-use-encryption
22. 3GPP TS 33.203: 3G security; Access security for IP-based services (2012), http://www.3gpp.org/ftp/Specs/html-info/33203.htm
23. Andreasen, F., Baugher, M., Wing, D.: Session Description Protocol (SDP) Security Descriptions for Media Streams, RFC 4568, IETF (2006), http://www.ietf.org/rfc/rfc4568.txt
24. McGrew, D.: The Use of AES-192 and AES-256 in Secure RTP, RFC 6188, IETF (2011), http://www.ietf.org/rfc/rfc6188.txt
25. 3GPP TR 33.828: IP Multimedia Subsystem (IMS) media plane security (2012), http://www.3gpp.org/ftp/Specs/html-info/33828.htm
26. Mattsson, J., Tian, T.: MIKEY-TICKET: Ticket-Based Modes of Key Distribution in Multimedia Internet KEYing (MIKEY), RFC6043, IETF (2011), http://www.ietf.org/rfc/rfc6043.txt
27. Cakulev, V., Sundaram, G.: MIKEY-IBAKE: Identity-Based Authenticated Key Exchange (IBAKE) Mode of Key Distribution in Multimedia Internet KEYing (MIKEY), RFC 6267, IETF (2011), http://www.ietf.org/rfc/rfc6267.txt
28. Zimmermann, P., Johnston, A. (ed.), Callas, J.: ZRTP: Media Path Key Agreement for Unicast Secure RTP, RFC 6189, IETF (2011), http://www.ietf.org/rfc/rfc6189.txt