Telecommun Syst (2007) 36: 153–159
DOI 10.1007/s11235-008-9065-5

A lightweight protection mechanism against signaling attacks in a SIP-based VoIP environment

Dimitris Geneiatakis · Costas Lambrinoudakis

Published online: 7 February 2008

Abstract The advent of Voice over IP (VoIP) has offered numerous advantages but, at the same time, it has introduced security threats not previously encountered in networks with a closed architecture like the Public Switch Telephone Networks (PSTN). One of these threats is that of signaling attacks. This paper examines the signaling attacks in VoIP environments based on the Session Initiation Protocol (SIP), focusing on the design of a robust lightweight protection mechanism against them. The proposed scheme introduces a new SIP header, namely the *Integrity-Auth* header, which is utilized for protecting the SIP-based VoIP services from signaling attacks while ensuring authenticity and integrity.

Keywords Session Initiation Protocol (SIP) · Signaling attacks · Voice over IP (VoIP) · Security

1 Introduction

Public Switch Telephone Networks (PSTN) are closed networks mainly supporting voice services, exhibiting a high availability, reliability and security level. However, PSTN capabilities are rather limited as far as the provision of more advanced, low cost, services, like audio conferences, personalized call transfers, instant messaging etc. On the other hand, the advent of Internet Telephony, in the form of Voice over IP (VoIP) services, gives the opportunity to telephony providers to offer such services. It is evident, however, that in order to ensure their success, VoIP providers must achieve a reliability, availability and security level at least comparable to that offered by PSTN. PSTN due to its closed architecture exhibits an extremely low attack frequency [1]. For instance, one of the most common attacks in PSTN is the "call eavesdropping" which despite its simplistic nature, it is rather difficult to realize since it requires access to the physical medium.

On the other hand, VoIP utilizes open networks like Internet. As a result the services offered are vulnerable to a plethora of attacks and undoubtedly such open environments must be considered as hostile by any critical real-time application like VoIP. It is therefore clear that the deployment of VoIP services raises security challenges that have not been previously encountered in PSTN.

In addition, the utilization of open networks makes VoIP services vulnerable not only to well known Internet attacks like Distributed Denial of Services (DDoS) [2] but also to more sophisticated attacks that try to exploit vulnerabilities of the signaling protocol, like Session Initiation Protocol (SIP) [3], H.323 [4], MGCP [5] etc., or of the transport protocol, like Real-Time Transport Protocol (RTP) [6]. Attacks of this type have been already presented in [7, 8], focusing on SIP vulnerabilities, as SIP seems to overwhelm the other signaling protocols considering that it has been adopted by various standardization organizations as the protocol for establishing multimedia sessions in both wireline and wireless world in the Next Generation Networks (NGN) era. For instance, a malicious user may generate a SIP signaling message for illegally terminating an established connection or canceling a session in progress. Similar attacks are also applicable to the other signaling protocols. It should be also emphasized that the interconnection between

D. Geneiatakis (✉) · C. Lambrinoudakis
Laboratory of Information and Communication Systems Security, Department of Information and Communication Systems Engineering, University of the Aegean, Karlovassi, 83200 Samos, Greece
e-mail: dgen@aegean.gr

C. Lambrinoudakis
e-mail: clam@aegean.gr

VoIP and PSTN constitutes PSTN also vulnerable to VoIP threats. The protection of VoIP services is thus a critical issue.

This paper presents the signaling attacks that can occur in the SIP realm, trying to cause Denial of Service (DoS), and proposes a lightweight protection mechanism against this type of attacks. It is the authors' belief that the combination of the proposed mechanism with the existing SIP's security mechanisms, as described in RFC 3261 [3], will improve security of SIP based VoIP services, making extremely difficult for an attacker to launch this type of attack. To the best of our knowledge the published research work addressing this problem is very limited [9] and [10]. The paper is structured as follows. Section 2 provides background information concerning SIP functionality, while Sect. 3 highlights the signaling flaws of a SIP-based service that can be exploited by a malicious user, focusing on the BYE attack. Sections 4 and 5 describe and analyze the proposed protection mechanism correspondingly, whereas Sect. 6 presents the related work. Finally Sect. 7 concludes the paper.

2 Sip protocol overview

SIP is an application-layer signaling protocol for creating, modifying, and terminating multimedia sessions among one or more participants [3]. The structure of a SIP message is similar to a HTTP message, and it can be either a request or an acknowledgement to a corresponding request, consisting of the header fields and optionally of a message body. The overall structure of a typical SIP message is illustrated in Fig. 1.

The main signaling "services" of the SIP protocol are (a) the establishment, (b) the cancellation and (c) the termination of a multimedia or voice session among two or more participants. The corresponding SIP messages are: INVITE, CANCEL, and BYE. Consider the case where a User A (caller) wishes to establish a multimedia connection with User B (callee). The caller generates an INVITE message and sends it to the corresponding proxy, which in turn forwards it to the callee. Assuming that the calee is available the session is established. When either of the participants wishes to terminate the session he must issue a BYE message. The establishment-termination process is depicted in Fig. 2.

3 Sip's signaling attacks: the BYE example

The easy access to the communication channel is considered as one of the most severe threats emerged in VoIP. The fact that eavesdropping is the first step of almost every attack, combined with the text-nature of SIP messages (Fig. 1), makes SIP-based services extremely attractive to many attacks.

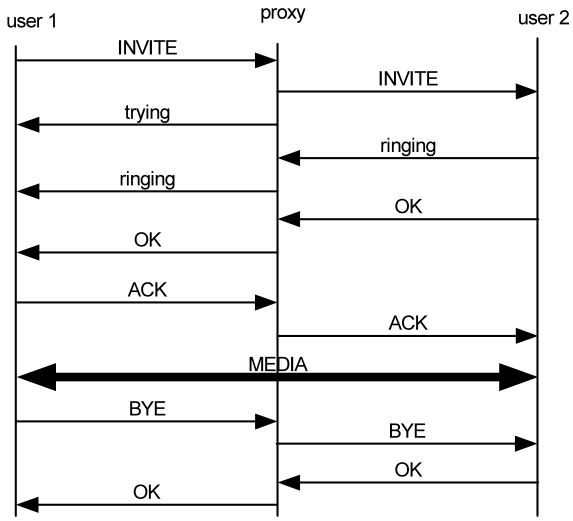

Fig. 2 SIP establishment and termination procedure

Fig. 1 A typical INVITE message

```
INVITE sip:dgen@aegean.gr  SIP/2.0                                  ] FIRST LINE
To: Geneiataki Dimitri <dgen@aegean.gr>                             ]
From: Karopoulos Georgios <sip:gkar@aegean.gr>;tag=76341            ]
CSeq: 2 INVITE                                                      ]
Authorization: Digest username="gkar", realm="195.251.164.23",      ] HEADERS
algorithm="md5", uri="SIP:195.251.164.23",                          ]
nonce="41352a56632c7b3d382b39e0179ca5f98b9fa03b",                    ]
response="a6466dce70e7b098d127880584cd57"                           ]
Contact:  <SIP:195.251.166.73:9384>;>                               ]
CallId : 12345667@195.251.166.73                                    ]
Content-Type: application/sdp                                       ]

v=0                                                                 ]
o=Tesla 2890844526 IN IP4 lab.high-voltage.org                      ] MESSAGE
c=IN IP4 100.101.102.103                                            ] BODY
t=0 0                                                               ]
m=audio 49170 RTP/AVP 0                                             ]
a=rtpmap:0 PCMU/8000                                                ]
```

For instance consider a case where an attacker captures (by utilizing, for instance, ethereal [11]) the SIP traffic for a specific session. Possible consequences of such an eavesdropping action could be: (a) disclosure of confidential information (e.g. identities of communicating parties) (b) malicious use of session specific information aiming to cause DoS. For instance an attacker may create a spoofed BYE or CANCEL message, using the appropriate session parameters, in order to terminate, cancel or illegally modify a session. These kinds of attacks are known as signaling attacks [8].

As an example we will describe in more detail the BYE attack. For an attacker to launch a BYE attack it is necessary to "discover" the correct session-dialog parameters. These parameters are included in the signaling messages exchanged prior to the establishment of the connection. Specifically the required parameters are: callid, the tag in the FROM header and the tag in the TO header (see Fig. 1). It must be stressed that the tag in the TO header is included in the OK message and thus the attacker must also capture the corresponding OK message in order to acquire all the information necessary for launching the attack. Nevertheless, in some cases the BYE message is employed for terminating (canceling) a non-completed session, without requiring an OK messages; such a case is described in RFC 3261 [3]. Consequently an attacker can also launch a BYE attack without the final OK message, but this depends on the SIP User Agent implementation.

Having "discovered" the parameters, the attacker can generate the spoofed BYE message for terminating/canceling the corresponding session. The attack sequence is depicted in Fig. 3. The user who receives the "spoofed" BYE message cannot recognize that it has not been sent by the other (legal) participant. Similar steps are adopted for the CANCEL, RE-INVITE, UPDATE and REFER attacks [8].

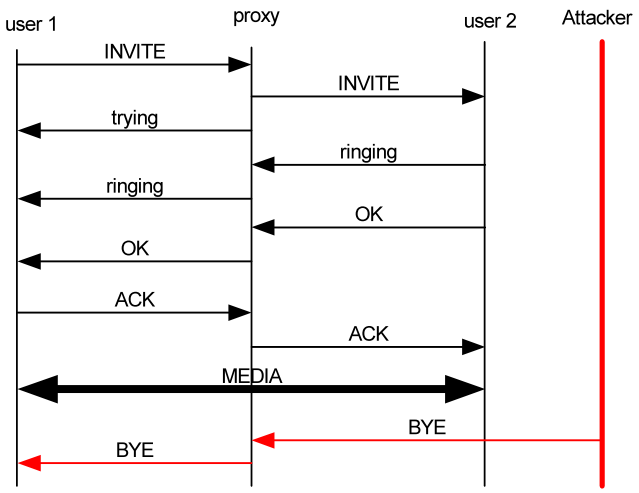

Fig. 3 Illegal call termination

One could claim that the security mechanisms suggested by RFC 3261 [3] could be employed for protecting SIP-based services against this type of attacks. However, this is not precisely the case, since there are several limitations [12, 13, 23] associated with these security mechanisms when applied to a SIP environment.

For instance, the utilization of the Transport Secure Layer (TLS) [14] mainly offers hop-by-hop security (in general TLS can be employed to secure communication among different SIP domains), since a potential attacker can obtain the required information in the intermediaries systems, or at the final hop, as only few SIP User Agents (UA) currently implement TLS [24–26]. On top of that, SIP invokes, as a default protocol, the User Datagram Protocol (UDP) and is thus unable to utilize TLS in all cases.

Another limitation concerns the Secure MIME (S/MIME) [15]; since a SIP proxy requires access to specific headers for processing an incoming message it is evident that it cannot offer protection against passive attacks like eavesdropping. Furthermore, S/MIME requires a PKI infrastructure, while until now there is only one SIP client implementing S/MIME [24].

Finally, SIP provides a stateless, challenge-based mechanism for message authentication that is based on HTTP authentication [16], in which utilizes headers like Proxy-Authenticate, Proxy-Authorization, WWW-Authenticate and, Authorization to request authentication or to send the computed credentials. However, the HTTP digest does not provide (a) message integrity, (b) any protection against signaling attacks and (c) also constitutes SIP messages vulnerable to man-in-the-middle attacks (someone can "use" the appropriate credentials for modifying the message in such a way that a new request takes the place of the initial one). Moreover there are methods specified in the RFC 3261 [3], like CANCEL and ACK, which raise additional authentication requirements. The HTTP digest cannot fulfill such requirements. A detailed analysis of the limitations of SIP's security mechanisms can be found in [12, 13, 23].

4 The proposed protection mechanism

As highlighted by the following RFC 3261 [3] statement: "*Protective measure above and beyond those provided by Digest need to be taken to prevent active attackers from modifying SIP request and responses*", a security mechanism, complementary to the existing ones, which will provide protection against signaling attacks, is necessary.

4.1 The proposed scheme

In addition to the existing limitations of the SIP security mechanisms (as briefly described in Sect. 3), someone wishing to launch a signaling attack takes advantage of the fact

that the authenticity and integrity of the SIP messages (like CANCEL, BYE, INVITE etc.) is not ensured/protected.

The proposed scheme provides integrity and authenticity security services without requiring any modification neither in the core architecture of the User Agent, nor in the existing pre-shared trust between the user and the proxy of the provider.

The only precondition of the proposal scheme is the introduction of a new header, named *Integrity-Auth* header. Even though one could argue that the introduction of such a header is impractical, this is not the case. On the contrary there are many cases [10, 27–30] where new headers have been employed for improving either SIP's functionality or its security. On top of that RFC 3261 allows new header field parameters and new parameter values to be defined. Consequently, the proposed mechanism can be employed in real environments without imposing any need for modifications in the SIP core.

Figure 4 illustrates the grammar of this new header (Integrity-Auth) that conforms to the SIP syntax as described in RFC 3161 [3].

The Integrity-Auth header must be used in all SIP messages, either requests or responses. The credential value will be computed through a slight variation of the Keyed–Hashing for Message Authentication (HMAC) [21] function, as illustrated in Fig. 5. Specifically, the Integrity-Auth value will be the hash value of the following two terms: (a) the SIP message concatenated with a random number, and (b) the hashvalue of the user's password after being xored with the random number. Consequently, the employment of this header provides message integrity and authenticity simultaneously. Furthermore, the utilization of the random number offers protection against replay attacks. A detailed security analysis of the proposed scheme is provided in Sect. 5.

As far as the computational processing is concerned, the overhead introduced by the Integrity-Auth header is minimal since the processing cost of the hash function is extremely low [14]. Negligible is also the corresponding message overhead, as the length of the Integrity-Auth value is not longer than 128 or 160 bits, depending on the algorithm employed (SHA-1 or MD5). It should be also noticed that, as mentioned in the RFC 2104 [21], HMAC is independent from the specific implementation of the underlying hash function, and thus the proposed scheme could engage any secure hash function.

Integrity-Auth = "lntegrity-Auth" HCOLON integrity-auth-value
integrity-auth-value = credentials-value;algorithm;nonce
algorithm-"algorithm" EQUAL alg-value
alg-value = "MD5|SHA1"
credentials-value = quoted-string

Fig. 4 Integrity-Auth header grammar

4.2 Applying the proposed scheme: the case of a BYE attack

In the case of a BYE attack, the attacker creates a spoofed BYE message in order to terminate a specific session (see Sect. 3). Such an attack is avoided if the User Agent employs the proposed security scheme. Specifically the legitimate user who needs to terminate a session generates a BYE message that includes the Integrity-Auth header. In accordance to Fig. 5, the value of this header in the SIP BYE message will be:

$$Integrity\_Auth = Hash(SIP\_BYE\_MESSAGE{:}Random, Hash(PWDuser \oplus Random))$$

Therefore the User Agent will send to the proxy the BYE message including the corresponding Integrity-Auth header. Upon receipt, the proxy retrieves from the appropriate database the user's password and then computes and validates the final value of the Integrity-Auth header through the following formula:

$$Hash(SIP\_BYE\_MESSAGE{:}Random, Hash(PWDuser \oplus Random))$$

If the value received matches the one that was locally computed, the verification is successful and the proxy forwards the BYE message to the other call participant after removing the initial Integrity-Auth header and inserting a new one. The only difference of the Integrity-Auth header inserted by the proxy is that this time the password of the other participant is utilized for computing the corresponding header value, as shown below:

$$Hash(SIP\_BYE\_MESSAGE{:}Random2, Hash(PWDuserother \oplus Random2))$$

When the other call participant (in our example User 2) receives the message, checks its validity through a similar procedure with that described for the proxy. If the validation procedure terminates successfully, User 2 generates the appropriate response including in a similar way the Integrity-Auth header, protecting it from unauthorized modification. The aforementioned procedure is illustrated in Fig. 6.

$$Integrity\_Auth = Hash(SIP\_MESSAGE{:}Random, Hash(PWDuser \oplus Random))$$

Fig. 5 Integrity-Auth header formula

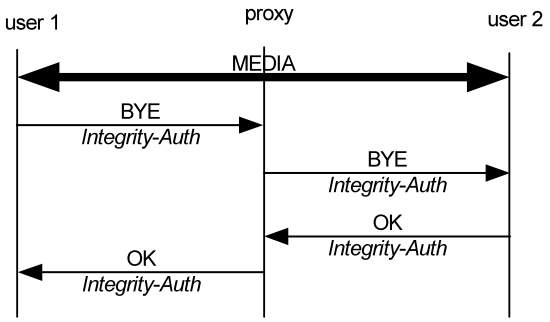

Fig. 6 Flow of a BYE request utilizing the proposed scheme

The same mechanism can be also applied for protecting session participants against other signaling attacks [8] like *CANCEL, REFER, RE-INVITE* and *UPDATE* attacks.

5 Security analysis of the proposed scheme

As demonstrated in the previous sections the proposed scheme can provide protection against any signaling attack. Its pros and cons are presented through the following scenarios. In all cases it is assumed that the proposed scheme is utilized.

Let's assume that a malicious user decides to bypass the proposed scheme and launch a signaling attack. The only way to do that is to try to impersonate either a legitimate user or a proxy. For instance, in the first case the malicious user generates a spoofed BYE message (see Sect. 3) and forwards it to the corresponding proxy. The proxy receives the spoofed message and then attempts to verify the validity of the Integrity-Auth header. Considering that the malicious user does not know the password of the legitimate user, and thus the received Integrity-Auth value cannot match the value calculated by the proxy, the verification will fail and the proxy will reject the message. Even in the case where the attacker is a "legitimate" internal user who utilizes his own legal password in the spoofed message for computing the Integrity-Auth value, the proxy will again reject the message since the attacker's password does not match that of the legal user that the proxy will employ during the recalculation of the Integrity-Auth header. In the case where the malicious user attempts to impersonate the proxy, both users will be able to detect that the proxy is a malicious one. This is due to the fact that the proxy does not know the valid users' passwords and thus cannot generate the correct values for the Integrity-Auth header. Moreover, there is no way that the malicious user can launch a replay attack as in the value of the Integrity-Auth header a random number is also involved (see Fig. 5).

One might argue that a potential attack against the proposed scheme is the brute force attack. Specifically, an attacker could capture the exchanged Integrity-Auth header value, the random number and the SIP_MESSAGE correspondingly, and then launch the brute force attack presented in Fig. 7.

For each candidate password *PWDi* do:
brute_force_value = *Hash*(*SIP_MESSAGE*:*Random*, *Hash*(*PWDi* $\oplus$ *Random*))
If(brute_force_value == captured_value)
then password = *PWDi*

Fig. 7 A brute force attack example

Table 1 Security services supported by SIP's security mechanisms

	HTTP digest	SSL	Proposed scheme
Integrity	No	Yes	Yes
Authenticity	Yes	Yes	Yes
Confidentiality	No	Yes	No
Non-repudiation	No	No	No
Mutual authentication	No	Yes	Yes

Table 2 Protection services supported by SIP's security mechanisms

	HTTP digest	SSL	Proposed scheme
Replay attacks	Yes	Yes	Yes
Signaling attacks	No	No	Yes
Man in the middle	No	No	Yes
Internals attacks	Partial	Partial	Yes
External	Yes	Yes	Yes

Nevertheless such an attack is practically feasible only with passwords belonging to a cryptographically small space [22]. Consequently, the limitation of the proposed scheme lies in the use of a pre-shared secret, implying that if this password gets compromised the security of the entire system breaks down. On the other hand, the use of the pre-shared key is not compulsory, since there are alternative solutions that could be adopted, like the use of a session key established during the initiation of the call as described in [17], or during the registration phase.

Furthermore, one could claim that a functionality similar to the one of the proposed scheme could be achieved by utilizing the HTTP digest. This is not true, since the HTTP digest for every authenticated message requires three additional messages and it cannot be applied in cases like the CANCEL signaling attack. In addition it is vulnerable to man-in-the-middle attacks. Tables 1 and 2, summarize the main features of the proposed scheme and compares them with the respective features of SIP's security mechanisms as described in RFC 3261 [3].

6 Related work

VoIP IDS/IPS systems are still in their very early stages and thus there is only limited research work published [9, 10, 18–20] addressing solutions for the protection of VoIP infrastructures from related attacks [7, 8]. Specifically, [18] describes an architecture that can effectively protect against attacks like irresolvable DNS attacks, malformed messages and single SIP flooding attacks. In [19] a similar architecture to [18] is also presented. The main difference lies at the introduction of SIP stateful analysis checks. An alternative solution for SIP stateful analysis is presented in [20]. None of the above-mentioned systems provides any protection against signaling attacks. To the best of our knowledge the only published work dealing with signaling attacks are [9, 10]. Particularly, SCIDIVE [9] can defend only against the BYE attack. The SCIDIVE solution cannot be compared to the proposed scheme, as it is based on the cross protocol intrusion detection architecture. It assumes that an attack is taking place if RTP messages follow a BYE message. It is therefore feasible for the attacker to generate spoofed RTP messages, after the legitimate user generates the BYE message, triggering a false alarm. Furthermore, an attacker, in order to ensure that a BYE attack will not be detected, may first cause a DoS to one of the callers and then send the BYE message to the other. Such cases cannot be detected by the SCIDIVE architecture. In addition such a scheme does not offer any protection against man-in-the middle attacks.

The solution described in [10] focuses on protecting the session's responses. This solution is mainly effective in cases of signaling attacks, in which a rogue SIP proxy (man in the middle) generates a "spoofed" response to redirect the session to an unauthorized user; however it cannot be utilized to provide a complete protection against signaling attacks like CANCEL, BYE etc. Particularly it provides protection for all messages generated by the calee. For instance, consider the case in which User 1 establishes a connection with User 2 (see Fig. 3). All messages (responses and requests) generated by User 2 and sent to User 1 can be authenticated by User 1. As a result, if an attacker tries to spoof User 2 and launch a BYE attack, he will fail. However, if the attacker sends a BYE, CANCEL etc, message to User 2, the attack will be successful since User 2 cannot validate the identity of User 1.

Tables 3 and 4 summarise the main features of all the solutions that have been proposed for the protection of SIP based services against signaling attacks.

Table 3 Security services supported by different solutions

	SCIDIVE	[10]	Proposed scheme
Integrity	No	Partial	Yes
Authenticity	No	Partial	Yes
Confidentiality	No	Yes	No
Non-repudiation	No	No	No
Mutual authentication	No	No	Yes

Table 4 Protection services supported by different solutions

	SCIDIVE	[10]	Proposed scheme
Replay attacks	No	Yes	Yes
Signaling attacks	Only BYE	Partial	Complete
Man in the middle	No	Yes	Yes
Internals attacks	Partial	Partial	Yes
External	Partial	Partial	Yes

7 Conclusion

VoIP systems gradually become more and more popular as their user base increases fast and the associated services gain in acceptance. In this context, SIP seems to overwhelm other standards mainly due to the fact that it has been adopted by various standardization organizations (e.g. IETF, ETSI, 3GPP) as the protocol for both wireline and wireless world in the Next Generation Networks era. Meanwhile, various kinds of attacks against those sensitive real-time systems are reported, stemming mainly from VoIP open nature inherited by the Internet. It is beyond doubt that malicious users will try to expose and finally exploit any vulnerability in SIP systems as well as in any VoIP subsystem, aiming to decrease the availability and trustworthiness of the entire voice network. Although the reported VoIP attacks are only a few, not including any signaling attacks, it is believed that in the near future such phenomena will become more and more frequent in real VoIP systems. Therefore the protection against this type of attacks is considered to be a crucial issue.

The paper has presented a computational inexpensive security scheme that can be employed in SIP environments to provide not only protection against signaling attacks but also ensuring authenticity and integrity. A new SIP header, named Integrity-Auth, has been introduced. It is the authors' belief that the combination of the proposed mechanism with the existing SIP security mechanisms, as described in RFC 3261 [3], will increase the robustness of VoIP services, making extremely difficult for an attacker to launch a signaling attack.

Acknowledgement We would like to thank the anonymous reviewers for their valuable comments.

References

1. Sicker, D. C., & Lookabaugh, T. (2004). *VoIP security*: *not an afterthought. QUEUE*. New York: Assoc. Comput. Mach.
2. Gibson: Distributed reflection denial of service. On-line tutorial, http://grc.com/dos/drdos.htm.
3. Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Spark, R., Handley, M., & Schooler, E. (2002). *Session initiation protocol*. RFC 3261, June 2002.
4. Hersent, O., Petit, J., & Gurle, D. (2005). *IP telephony*: *deploying voice-over-IP protocols*. New York: Wiley.
5. Andreasen, F., & Foster, B. (2003). *Media Gateway Control Protocol* (*MGCP*) *Version 1.0*. RFC 3435, January 2003.
6. Schulzrinne, H., Casner, S., Frederick, R., & Jacobson, V. (2003). *RTP*: *A transport protocol for real-time applications*. RFC 3550, July 2003.
7. VOIPSA (2005). *VoIP security and privacy threat taxonomy*. http://www.voipsa.org/Activities/taxonomy.php, October 2005.
8. Geneiatakis, D., Dagiuklas, T., Kambourakis, G., Lambrinoudakis, C., Gritzalis, S., Ehlert, K. S., & Sisalem, D. (2006). Survey of security vulnerabilities in session initiation protocol. *IEEE Communications Surveys and Tutorials*, *8*(3), 68–81.
9. Wu, Y.-S., Bagchi, S., Garg, S., & Singh, N. (2004). SCIDIVE: a stateful and cross protocol intrusion detection architecture for voice-over-IP environments. In *Proceedings of international conference on dependable systems and networks* (Vol. 28, pp. 433–442). June 1–July 2004.
10. Cao, F., & Jennings, C. (2006). Providing response identity and authentication in IP telephony. In *Proceedings of the first international conference on availability, reliability and security* (Vol. 20–22, p. 8). April 2006.
11. Ethereal Sniffer, www.ethereal.com.
12. Salsano, S., Veltri, L., & Papalilo, D. (2002). SIP Security Issues: The SIP authentication procedure and its processing load. *IEEE Network*, *16*(6), 38–44.
13. Geneiatakis, D., Dagiuklas, T., Kambourakis, G., Lambrinoudakis, C., & Gritzalis, S. (2005). Session initiation protocol security mechanisms: a state-of-the-art review. *INC'05 International Network Conference*, July 2005 (pp. 147–156).
14. Rescorla, E. (2000). *SSL and TLS—designing and building secure systems* (1st ed.). Reading: Addison-Wesley.
15. Ramsdell, B. (2004). *Secure/Multipurpose Internet Mail Extensions* (*S/MIME*) *Version 3.1 message specification*. IETF RFC 3851, July 2004.
16. Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., & Stewart, L. (1999). *"HTTP authentication*: *basic and digest access authentication" IETF*. RFC 2617, June 1999.
17. Yang, C.-C., Wang, R.-C., & Liu, W.-T. (2005). Secure authentication scheme for session initiation protocol. *Computers and Security*, *24*(5), 381–386.
18. Dagiuklas, T., Geneiatakis, D., Kambourakis, G., Sisalem, D., Ehlert, S., Fiedler, J., Markl, J., Rokos, M., Botron, O., Rodriguez, J., & Liu, J. (2005). *"General reliability and security framework for VoIP" infrastructures*. http://www.snocer.org, August 2005.
19. Niccolini, S., Garroppo, R. G., Giordano, S., Risi, G., & Ventura, S. (2006). SIP intrusion detection and prevention: recommendations and prototype implementation. In *Proceedings of 1st IEEE workshop on VoIP management and security* (Vol. 3, pp. 47–52). April 2006.
20. Chen, E. Y. (2006). Detecting DoS attacks on SIP systems. In *Proceedings of 1st IEEE workshop on VoIP management and security* (Vol. 3, pp. 53–58). April 2006.
21. Krawczyk, H., Bellare, M., & Canetti, R. (1997). *HMAC*: *Keyed-Hashing for message authentication*. RFC 2104, February 1997.
22. Jablon, D. P. (1997). Strong password-only authenticated key exchange. *ACM SIGCOMM*, *Computer Communication Review*, p. 526.
23. Gupta, P., & Shmatikov, V. *Security analysis of voice-over-IP protocols*. Available on http://citeseer.ist.psu.edu/761544.html.
24. The LynxPhone, http://www.bitlynx.com/lynxphone.php.
25. Minisip, http://www.minisip.org.
26. Snom 300, http://www.snom.com.
27. Schulzrinne, H., Oran, D., & Camarillo, G. (2002). *The reason header field for the session initiation protocol*. RFC 3326, Internet Engineering Task Force.
28. Niccolini, S., Tartarelli, S., Stiemerling, M., & Srivastava, S. *SIP extensions for SPIT identification*. Work in progress available on http://tools.ietf.org/html/draft-niccolini-sipping-feedback-spit-03.
29. Willis, D., & Hoeneisen, B. (2002). *Session Initiation Protocol* (*SIP*) *extension header field for registering non-adjacent contacts*. RFC 3327.
30. Garcia-Martin, M., Henrikson, E., & Mills, D. *Private header* (*P-Header*) *extensions to the Session Initiation Protocol* (*SIP*) *for the 3rd-Generation Partnership Project* (3GPP). RFC 3455.

Dimitris Geneiatakis was born in Athens, Greece, in 1981. He received the five-year Diploma in information and communication systems in 2003, and the M.Sc. in security of information and communication systems in 2005, both from the department of Information and Communications Systems Engineering of the University of Aegean, Greece. His current research interests are in the areas of security mechanisms in Internet telephony, Smart Cards and Network Security. He is an author of several refereed papers in international scientific journals and conference proceedings. Mr. Dimitris Geneiatakis is a member of the Technical Chamber of Greece.

Costas Lambrinoudakis was born in Greece in 1963. He holds a B.Sc. (Electrical and Electronic Engineering) degree from the University of Salford (UK), an M.Sc. (Control Systems) and a Ph.D. (Computer Science) degree form the University of London (UK). Currently he is an Assistant Professor at the Department of Information and Communication Systems of the University of the Aegean. His current research interests include: Information Systems Security, Smart Cards and Computer Architectures. He is an author of several refereed papers in international scientific journals and conference proceedings. He has participated in many national and EU funded R&D Projects. He has served on program and organizing committees of national and international conferences on Informatics and he is a reviewer for several scientific journals.