A Mechanism for Ensuring the Validity and Accuracy of the Billing Services in IP Telephony

Dimitris Geneiatakis, Georgios Kambourakis and Costas Lambrinoudakis

Laboratory of Information and Communication Systems Security
Department of Information and Communication Systems Engineering
University of the Aegean, Karlovassi, GR-83200 Samos, Greece
{dgen, gkamb, clam}@aegean.gr

Abstract. The current penetration, but also the huge potential, of Voice over IP (VoIP) telephony services in the market, boosts the competition among telecommunication service providers who promote new services through many different types of offers. However, this transition from the closed Public Switched Telephone Network (PSTN) architecture to the internet based VoIP services, has resulted in the introduction of several threats both intrinsic i.e. VoIP specific, and Internet oriented. In the framework of this paper, we are considering threats that may affect the accuracy and validity of the records of the billing system that the service provider is using for charging the users. We are proposing a simple, practical and effective mechanism for protecting telecommunication service providers and end users from malicious activities originated from the end users and telecommunication service providers respectively. In both cases the malicious activity concerns fraud through the billing system. The proposed mechanism focuses on VoIP services that are based on the Session Initiation Protocol (SIP). However, it can be easily amended to cover other VoIP signaling protocols, as it takes advantage of the underlying AAA network infrastructure to deliver robust time stamping services to SIP network entities.

Keywords: Session Initiation Protocol (SIP), Billing, Voice Over IP (VoIP)

1. Introduction

The advent of Voice over IP (VoIP) Telephony[1] services offers to Telecommunication Service Providers (TSPs) new opportunities for providing advanced services, like conference rooms, click to dial, and multimedia delivery. In PSTN such services could not be realized at a large scale and at a relatively low cost. Furthermore, the potential of such services is highlighted by the estimation that up to the year 2012, VoIP users would reach the number of twelve million. Note, that currently the number VoIP users is not

[1] Hereafter the terms Voice over IP and IP Telephony services are considered equivalent

more that one million [1]. However, in order for TSPs to support such services, they should, among other things, provide accurate accounting services and particularly billing. This will boost the trustworthiness and popularity of VoIP services to potential consumers and will greatly increase IP telephony market share.

Several researchers [2]-[4] have already identified various types of attacks that could be launched against VoIP services. Such attacks can severely affect not only the end-users but also the VoIP providers and the underlying infrastructure. Putting aside Quality of Service (QoS) issues, when end-users acquire VoIP services they are mostly worried about the accuracy and validity of their billing accounts. For example, the service provider could act maliciously and modify in an illegal way the Call Detail Records (CDRs) in order to overcharge the billing account of a given end-user. In the same way, an end-user could repudiate the calls included in his billing account in order to avoid the charges. It should be stressed that in such cases neither the end-user nor the TSP can prove the validity of the CDRs due to the lack of the appropriate non-repudiation mechanisms in IP Telephony services.

This paper proposes a simple, practical and effective mechanism for protecting, both end-users and TSPs, from billing frauds. While our mechanism focuses on VoIP services that are based on Session Initiation Protocol (SIP) [5], it can be easily amended to cover other VoIP signaling protocols as well. This is because our scheme takes advantage of the underlying AAA network infrastructure to deliver robust time stamping services to SIP network entities.

The rest of the paper is organized as follows. Section 2 provides background information regarding billing services in VoIP. Section 3 presents various security incidents that affect the validity and accuracy of the billing service, while Section 4 introduces and thoroughly analyzes the proposed scheme. Finally, Section 5 concludes the paper giving directions for future work.

2. Billing Services in IP Telephony

VoIP attracts gradually more and more subscribers [1] and as already mentioned it is anticipated to gain a significant market share in the next few years. This growth is actually driven by two key factors: the low cost of VoIP service acquisition and the similar levels of QoS when compared to those of PSTN. TSPs do promote VoIP services through various offers, like free usage time, lower costs for prepaid cards and many more. In fact, all these offers are based on different billing methods that the TSPs must support. According to

[6],[7] the billing methods that are available for services provided through the Internet architecture can be classified into the following categories:

- *Fixed Charge*: The subscriber pays a fixed subscription fee for a specific period of time (e.g. monthly) irrespectively of the service usage.
- *Usage Charge*: The subscriber pays a fee based on service usage (e.g. the volume of the data being transferred). For Internet oriented services two basic usage models are employed: (a) Service Time usage and (b) Transferred Media. Note that the latter model is not suitable for voice services.
- *Service Quality Charge*: According to this model whenever the subscriber access the service, he pays a fee based on the provided QoS offered by the TSP as the case may be.

Nowadays most TSPs employ mixed billing schemes, combining *Fixed* and *Usage* charging schemes, which rely either on prepaid or post billing services. However, in every case the employed billing scheme does not influence the general accounting method in use. To be more precise, by the term *accounting method* we refer to the process of collecting information about chargeable events, which will be later used as input to the billing service. Consequently, the billing process for IP telephony requires, among others, accurate tracing of "start" and "end" events for all the services acquired by a given subscriber in order to charge him appropriately. These events are known as *Call Detail Records* (CDRs). An example of such an event logging process sequence in a SIP based VoIP service, is presented in Table 1. Normally, CDRs are captured either by the Authentication, Authorization and Accounting (AAA) Server in charge, or the corresponding SIP proxy, depending on the service configuration parameters.

Table 1. An Example of Call Detail Records

Call-Id	Caller	Callee	Type Msg	Time-Date
123@sip.gr	dgen@sip.gr	gkar@sip.gr	INVITE	1/1/2008:11:00:00
123@sip.gr	dgen@sip.gr	gkar@sip.gr	200 OK	1/1/2008:11:00:01
123@sip.gr	dgen@sip.gr	gkar@sip.gr	BYE	1/1/2008:11:05:04

Let us consider a User A (caller) who wishes to establish a voice connection with a User B (callee), through some specific SIP based VoIP service. First of all, the caller generates a SIP INVITE message and sends it to the corresponding SIP proxy, which in turn forwards it to the callee. It is assumed that the caller must have been previously authenticated by the local AAA server which is responsible to authorize him (or not) to access the voice service. Other interactions are also possible in this stage, i.e. if the user is roaming to a foreign domain the local AAA server may contact the AAA server of the caller's home domain in order to obtain the proper authentication and/or authorization credentials. However, for the sake of simplicity of the

example, we assume that the caller uses a postpaid service. Provided that the callee is available, the session will be successfully established after the caller sends, through the SIP proxy, the final ACK message to the callee. Whenever any of the participants wishes to terminate the session, he issues a BYE message. Upon that, the SIP proxy is responsible to send to the AAA server (immediately or at a latter time) the corresponding CDRs that will be used as input to the billing service. The aforementioned procedure is depicted in Figure 1.

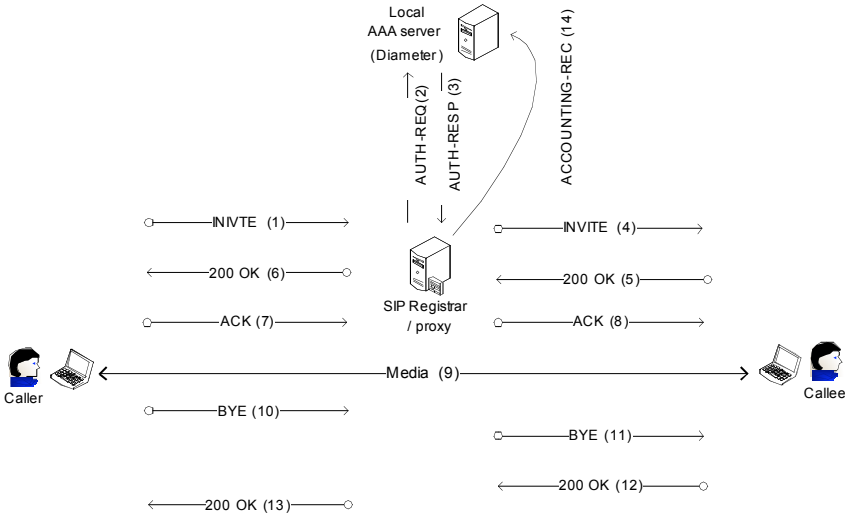

Fig. 1 Call Establishment procedure in SIP based IP Telephony Services

3. Billing Attacks against IP Telephony

Fraud attempts could be launched against any telecommunication system by employing several different methods and techniques. According to [8] there are 200 types of known telecommunication frauds. However, the closed architecture of PSTN offers very few opportunities to malicious users for frauds through the manipulation of signaling data. A well known fraud incident in PSTN took place in early 1960's, when common associated signaling was used by TSPs [9]. This attack unfolds as follows: the aggressor sends a termination tone to the call center without hanging on his device. Although the call was terminated successfully, resources related with the previous connection remain allocated since the call center is waiting for the on hook condition. At the same time the malicious user could dial a new telephone number along with a start tone and establish a new connection without charging his account. Currently, the introduction of Common Channel

Signaling (CCS), in conjunction with PSTN's closed architecture, makes such type of attacks impossible.

On the contrary, the advent of VoIP which relies on the Internet, introduces several threats both intrinsic i.e. VoIP specific, and Internet oriented. For example, a malevolent user may try to evade charging, or even worse, charge another innocent legitimate user with calls that he has never performed. This is due to the fact that there are several methods that a malicious user could exploit in order to manipulate VoIP signaling data as demonstrated in [3]. Considering the call establishment procedure of Figure 1, a malicious caller instead of sending an ACK message after receiving the "200 OK" response from the callee, manipulates his telephone to suppress it. As a result, the SIP proxy assumes that the call has not been established, but the caller is actually able to communicate with the callee. In another scenario depicted in Figure 2, a malicious user may act as a *Man In The Middle* (MITM) in order to modify an INVITE message. That is, the INVITE's message *Contact* header is set to the malicious user IP address and the *To* header to that of the person that the malicious user wishes to communicate with. The spoofed INVITE is then forwarded towards the corresponding proxy. The proxy sends the request towards the callee who, after accepting the call, generates a "200 OK" response message which is finally passed to the malicious user. Upon receiving it, the attacker replaces it with a "Busy" message and forwards it to the legitimate user who acknowledges the spoofed Busy response and terminates the session. Under this context, the conversation between the malicious user and the callee has been successfully established, while the malicious user wangled to debit a legitimate user's account for a call that did not actually made.

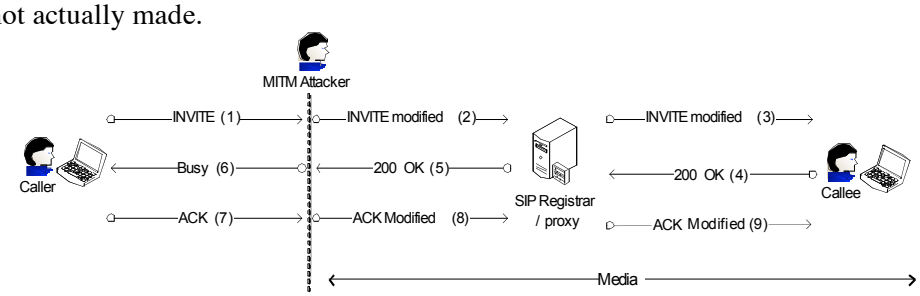

Fig. 2 An Example of Man-In-The-Middle Attack during Call Establishment

Similar techniques are used in billing attacks known as *"Fake busy"*, *"Bye Delay"* and *"ByeDrop"*, which are discussed in detail in [10]. The difference between the aforementioned scenario and the *"Fake Busy"* one is the existence of another malicious user acting on behalf of the callee. This second aggressor intercepts the SIP messages and generates a "200 OK" response in order to make his IP address available to his collaborator in the attack which

is placed on the side of the caller. After that, a media session between the two attackers can be successfully established. In this case the (legitimate) callee is unaware of the incoming invitation. As far as the rest of the attack scenarios, i.e. *Bye Delay* and *Bye-Drop*, the MITM attacker captures the SIP BYE message that the legitimate user (caller or callee) sends to the Proxy and sends back to the (legitimate) user a spoofed "200 OK" response message. This fact gives the impression to the service provider that the session is still active, whereas the legitimate user thinks that the session has been successfully terminated. It should be stated that in all the above security incidents the malicious user attempts to debit the legitimate user for calls that he never made.

4. The Proposed Mechanism

Billing accuracy severely affects end-users' trust to VoIP services. Thus, service providers should employ robust solutions and countermeasures against threats similar to those described in Section 3. Normally, TSPs start charging a caller as soon as the 200 OK response message has been received by the corresponding SIP proxy. This is crucial in order to thwart clever attackers from establishing free calls. Even this countermeasure, however, is not an accurate indication that the session between the two ends has been established successfully. For example, referring to Figure 1, the caller's network may become inoperable before the caller sends the final ACK (message #7). Even though this will interrupt the session in an abnormal way, the TSP will wrongly charge the caller for some service time. It is therefore clear that the employment of mechanisms for protecting both end-users and TSPs against billing frauds is necessary.

4.1 Architecture and General Description

The objective is to introduce a lightweight, practical and effective solution for preserving non-repudiation and non-usurpation in SIP. Thus, the choice was not to use mechanisms that mandate Public Key Infrastructure (PKI), like [12]. For the same reason we have set aside recent solutions [13] that are more generic and require third network entities or additional components. The proposed scheme is fully compatible with the underlying network infrastructure and the protocols employed. Moreover, it can support roaming users and heterogeneous network realms towards 4G. Figure 3 depicts the general architecture and the message flow of the proposed scheme. A detailed description of each step follows.

1. At first, the SIP user authenticates himself to the network using a standard AAA protocol. Here, we select Diameter [14], but RADIUS [16] is also an option without any loss of generality. Note, that up to this point, the user authentication is performed by utilizing any sort of credentials that the user has, via standard EAP methods, like EAP-TLS [17], EAP-AKA [18], etc.
2. Secondly, the user needs to register with the SIP registrar server in order to be able to receive and make calls. Here, a standard SIP authentication method, like the digest one [19] may be used.
3. After that, when the user initiates a SIP call, the User Agent (UA) sends a standard Diameter accounting request to the local AAA server. It is worth noting that the Accounting-Record-Type Attribute Value Pair (AVP), i.e. AVP Code 480, which contains the type of accounting record being sent, must set to EVENT_RECORD. This value indicates that a one-time event has occurred [14].
4. The AAA server sends a triplet of {Origin host || Session_ID || Timestamp} information to the local SIP proxy. It also keeps a signed, with his private key, copy of the triplet to a log file that could be used in case of dispute. The origin host field contains the IP address of the user's device. The IP address of the local SIP proxy may be pre-configured to the AAA server. If not, there are at least two more ways to find it. Normally, the location information can be discovered dynamically, based on Dynamic Host Control Protocol (DHCP). The DHCP server shall inform the AAA with the domain name of the local SIP proxy and the address of a Domain Name Server (DNS) that is capable to resolve the Fully Qualified Name (FQDN) of the SIP proxy by using DHCP. A second option is to include the IP address of the local SIP proxy to the Diameter accounting request (see step 3).
5. The proxy acknowledges the message, otherwise the AAA server may retransmit it after a given time interval, following SIP's retransmission time settings for a Non-INVITE request [5]. It also stores the received triplet to the corresponding queue. As discussed in the next subsection, for some predetermined time interval the AAA server will ignore any similar requests that originate from the same UA and have the same session_ID.
6. The AAA server responds back to the originating UA with a Diameter accounting response, which contains an Event-Timestamp AVP. As described in [14] a Timestamp AVP, records the time that the reported event occurred. The SIP INVITE procedure begins at this point and assuming that the callee accepts the call, a 200 OK message is returned to the caller.
7. At this point, the UA is ready to start the call by sending a SIP ACK message to the local SIP proxy. Before doing so, the UA concatenates the received timestamp with the SIP ACK message. Upon reception, the SIP

proxy will check its queue for a match, i.e. a same {Origin host || Session_ID || Timestamp}. It is noted that the corresponding queue has a limited length. That is, a triplet should remain in the queue until the session exceeds as it is specified in the SIP's Finite State Machine (FSM) [5]. If the matching procedure returns true, the proxy forwards the INVITE message to the caller, probably via other proxies, and logs the event along with the corresponding ACK message. The log files may be collected in batches at a later time by the underlying accounting service.

The same procedure should be followed before the call is terminated, that is, before the corresponding SIP BYE message, to timestamp the event of call termination. Eventually, the start and stop instances of user charging are designated by the two timestamps acquired by the AAA server.

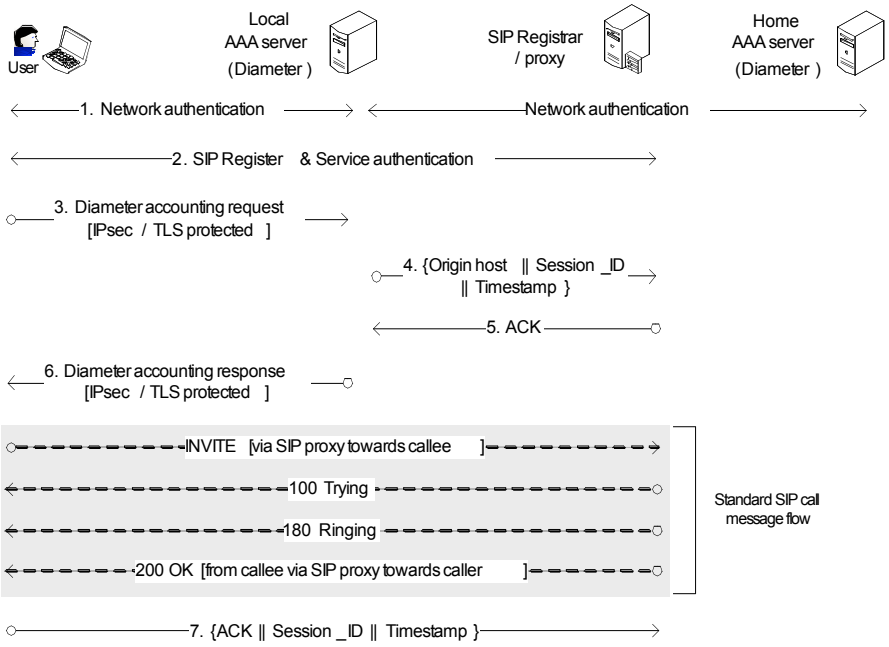

Fig. 3 Generic architecture and scheme's message flow

4.2 Security Analysis

In terms of security there are several aspects of the proposed scheme that must be carefully examined. The network authentication and the SIP register / authentication phases depend on the authentication methods and security policies employed. However, this is outside the scope of this paper. In fact, our security analysis concentrates on steps 3 to 7. As highlighted in [14] the

Diameter protocol must not be used without any security mechanism (TLS or IPsec). Therefore, the communication links between any Diameter nodes (Client, Agent or Server) are considered secure. Furthermore, when end-to-end security is required the End-to-End security extension, known as CMS Security Application [15], may be utilized. As a result, messages 3 & 6 in Figure 3 are considered to be secure when in transit. Nevertheless, an attacker may exploit the Diameter accounting request message to trigger a Denial of Service (DoS) attack against the local AAA server. Such a scenario will possibly enable the attacker to flood the AAA server with Diameter accounting request messages. However, this attack cannot be mounted since, as already mentioned, the AAA server will drop all subsequent requests (arriving after the first one) that originate from the same UA and have the same Session_ID, for a predetermined time interval (see step 5 in the previous subsection). Under these circumstances, the attacker will need a large number of zombies to launch such an attack, having each zombie sending a request every 30 seconds, a scenario that is considered highly improbable. IP spoofing by a limited number of machines is also out of question since all modern routers will easily detect such an attack. Moreover, giving the fact that the {Origin host || Session_ID || Timestamp} queue holds only a limited number of records, overflow style DoS attacks are not feasible.

Another scenario could be the eavesdropper to acquire a Diameter accounting response in order to use it for his own benefit or to just cause commotion to the accounting system. This is however infeasible since the communication between the UA and the AAA server is encrypted and also because the SIP server will match each INVITE SIP message with its own records. Furthermore, in order to protect the integrity and authenticity of SIP ACK and BYE messages, against MITM attacks, a mechanism like the *Interity-Auth* header proposed in [20] should be adopted.

4.3 Resolution of Disputes

Let us now consider a case where a legitimate user repudiates a specific call (or part of it) that has been included in his billing account. If that happens, the TSP will requests from the AAA server the log file of the signed timestamps that correspond to the sessions-calls made. Furthermore, the TSP locates in the SIP proxy logs, the SIP ACK and the corresponding SIP BYE message, designating the start and end of the specific call. With the AAA signed triplet {Origin host || Session_ID || Timestamp} and the user's SIP ACK and BYE messages, the TSP is able to prove that a call was indeed generated by the claimant. The TSP is also able to prove the exact duration of the call. Note that due to the employment of the *Integrity-Auth* scheme [20], only properly authenticated entities can establish or terminate calls by generating the

corresponding SIP messages. This ensures that no legitimate user is able to put calls on behalf of another. The claimant may also contend that the TSP generated these messages by his own, relied on the fact that the *Integrity-Auth* scheme is based on a pre-shared password. However, this is not feasible since the AAA (which has the role of a trusted third party) issues timestamps only for requests received by end-users. So, even in cases where the TSP tries to illegally modify a timestamp, he will not be able to match it later with the original AAA's signed timestamp. This means that the user would be able to prove that the corresponding accounting data were illegaly modified.

5. Conclusions and Future work

Billing mechanisms are of major importance for real-time services, like VoIP. This work elaborates on the accounting process, proposing a novel and robust billing system. The requirements of the proposed mechanism are defined and all the accounting scenarios that the system should cope with are examined. The proposed mechanism is generic and capitalizes on the existing AAA infrastructure, thus providing secure means to transfer and store sensitive billing data. More importantly, it can be easily incorporated into the TSP's existing mechanisms regardless of the underlying network technology. At the same time its generic nature allows for interoperability between different network operators and service providers. The next steps of this work include the implementation and evaluation of a prototype system.

References

[1] VoIP IP Telephony blog, available at: http://snapvoip.blogspot.com/2007/03/virtual-voip-carriers-vvcs-will-grow-to.html

[2] VOIPSA, "VoIP Security and Privacy Threat Taxonomy", http://www.voipsa.org/Activities/taxonomy.php, Oct. 2005.

[3] Geneiatakis, D., Dagiuklas, T., Kambourakis, G., Lambrinoudakis, C., Gritzalis, S., Ehlert, K.S., Sisalem, D., "Survey of security vulnerabilities in session initiation protocol," Communications Surveys & Tutorials, IEEE, vol.8, no.3, pp.68-81, 3rd. Qtr. 2006.

[4] Sisalem, D., Kuthan, J., Ehlert, S., "Denial of service attacks targeting a SIP VoIP infrastructure: attack scenarios and prevention mechanisms," Network, IEEE, vol.20, no.5, pp. 26-31, Sept.-Oct. 2006.

[5] Rosenberg, J., Schulzrinne H., Camarillo, G.; Johnston, A.; Peterson, J.; Spark, R.; Handley, M., Schooler E., "Session Initiation Protocol", RFC 3261, June 2002.

[6] Hyun Wook, Jaecheon Han, Miyoung Huh, Sunok Park, ShinGak Kang, "Study, on robust billing mechanism for SIP-based internet telephony services", in ICACT 2004, vol.2, no., pp. 756-759, 2004.

[7] Ibrahim, H.A., Nossier, B.M., Darwish, M.G., "Billing system for Internet service provider (ISP)", MELECON 2002, Vol., no., pp. 260-268a, 2002.

[8] Peter Thermos, Ari Takanen,Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures, Addison-Wesley Professional, Aug. 2007.
[9] John G. van Bosse, Fabrizio U. Devetak, Signaling in Telecommunication Networks, 2nd Edition, Wiley InterScience, Dec. 2006.
[10] Ruishan, Xinyuan Wang, Xiaohui Yang, Xuxian Jiang, "Billing Attacks on SIP-Based VoIP Systems" in proc. of first USENIX workshop on offensive technologies, Aug. 2007
[11] Rigney, C., "RADIUS Accounting", RFC 2139, April 1997.
[12] Adams, C., Cain, P., Pinkas, D., Zuccherato, R., "Entrust Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)", RFC 3161, Aug. 2001.
[13] Hakala, H., Mattila, L., Koskinen, J-P., Stura, M., Loughney, J., "Diameter Credit-Control Application", RFC 4006, Aug. 2005.
[14] Calhoun, P., Loughney, J., Guttman, B., Zorn, G., Arkko, J., "Diameter Base Protocol", IETF RFC 3588, Sept. 2003.
[15] P. Calhoun, W. Bulley, S. Farrell, "Diameter CMS Security Application", July 2001.
[16] Rigney, C. et al., "Remote Authentication Dial In User Service", RFC 2865, June 2000.
[17] B. Aboba, B., Simon, D., "PPP EAP-TLS Authentication Protocol", RFC 2716, Oct. 1999.
[18] Arkko, J., Haverinen, H., "EAP-AKA Authentication", RFC 4187, Jan. 2006.
[19] Franks, J. et al., "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.
[20] Geneiatakis, D., Lambrinoudakis, C., "A Lightweight Protection Mechanism against signaling Attacks in a SIP-Based VoIP environment", Telecommunication Systems, 2008, Springer.