Analysis of Token and Ticket Based Mechanisms for Current VoIP Security Issues and Enhancement Proposal

Patrick Battistello[1,2] and Cyril Delétré[1]

[1] Orange Labs, 2 av. Pierre Marzin, 22307 Lannion Cedex, France
[2] Telecom Bretagne, 2 rue de la Châtaigneraie, 35576 Cesson Sévigné, France
{patrick.battistello,cyril.deletre}@orange-ftgroup.com

Abstract. These last few years, the security of VoIP architectures has become a sensitive issue with many vulnerability announcements. This article first aims to distinguish the threats and the applicable protection mechanisms depending on the underlying VoIP architecture. We then investigate the properties of a specific class of existing call establishment mechanisms based on tokens or tickets. In the last section, an enhancement to these mechanisms is proposed which lifts some of the previously seen limitations, especially the DoS risks, the token storage constraint or the transport impact of large tickets.

Keywords: VoIP, security, SPIT, DoS, authentication, token, ticket.

1 Introduction

VoIP is a fast-growing application, with the first deployments starting around ten years ago, first in local networks then in wide or operator networks, for both residential and professional customers. This technology claims on one hand the integration of voice and data applications within a single network architecture, and on the other hand the support of advanced services (notification, presence, WebPhone, ClickToPhone) as well as the support of media flows other than voice in peer to peer or group communications.

In parallel to these advantages, the introduction of VoIP has also brought new issues, amongst which the QoS guarantee and the security of communications [1] that require specific solutions to reach the same quality as PSTN.

This article first aims to provide a state of the art of the major threats, and the associated protection mechanisms, distinguishing the different VoIP architectures. This is treated in section 2, starting from the historical intra-domain (or single domain) context and then moving to the more tricky inter-domain (or cross-domain interconnection) one. Then, section 3 focuses on a class of call establishment signalling mechanisms based on tokens or tickets, analysing pros and cons. In section 4, we introduce the framework of a call establishment mechanism operating in the signalling plane which lifts some of the previously seen limitations, especially the DoS risks, the token storage constraint and the transport impact of large tickets. Finally, section 5 provides the conclusions.

B. De Decker and I. Schaumüller-Bichl (Eds.): CMS 2010, LNCS 6109, pp. 154–165, 2010.

2 Current Stakes in VoIP Security

This section analyzes the major VoIP risks according to the possible architectures, because as explained in [2] there is no single VoIP model. We will begin with the intra-domain context which constitutes the historical VoIP deployments. Then we will analyze the inter-domain context which is the intra-domain natural extension, but presents increased security risks. A wealth of literature about security and threats in VoIP being available ([1], [3], [4], [5], [6]), this section will rather treat threats per architecture types than be exhaustive; distinguishing threats specific to VoIP from those which are not. For each category of architectures, we enumerate the major protection mechanisms with their pros and cons.

Beforehand we remind the reader that VoIP networks are based on several protocols. On the signalisation side, the IETF SIP protocol has progressively become the fundamental brick in association with the IETF SDP protocol for negotiating the multimedia session characteristics[1]. The media flows are conveyed via the IETF RTP protocol associated with the RTCP control protocol.

2.1 Intra-domain Context

We gather in this chapter the set of architectures characterized by the fact that VoIP communications remain confined in a same network or administrative domain, even if in each of these architectures signalisation and media gateways may be added to interconnect with the PSTN. An essential characteristic of the intra-domain context is that the operator, or administrator, is able to authenticate each entity[2] and localize it for call routing.

2.1.1 Main Architectures in the Intra-domain Context

The *VoIP initial architecture*, according to ITU-T H.323 and IETF SIP standards is made up of VoIP endpoints connected to registrar servers for endpoint registering and localization and to proxy servers for call routing between endpoints. This is a centralized architecture which can also support non-VoIP endpoints through phone adaptor or circuit to VoIP gateway.

The *extended architecture* is an extension of the initial architecture in which a same VoIP domain is distributed over several sites, or VoIP sub-networks, interconnected between themselves. The interconnection is performed either at the IP level or at the VoIP level (IP Centrex solution).

In parallel to incumbent operators, new players from the computer world have proposed alternative architectures like the *VoIP P2P architecture* where registrar and proxy functions are distributed over a set of nodes (instead of being centralized by an operator). The P2PSIP proposal [7] reuses DHT (Distributed Hash Table) concepts to route calls between the VoIP nodes of the P2P network, in association with "classical" VoIP protocols (SIP, SDP, and RTP).

Another alternative is the *VoIP web-based architecture*. It aims to simplify the access to VoIP by bringing the VoIP endpoint directly in the client's web browser; this

[1] Among the various SIP messages, the INVITE request initiates the call establishment process.
[2] Based on a unique identifier attached to each VoIP endpoint inside the domain.

new type of endpoint is called a WebPhone. This model mostly reuses websites principles and is often associated with "social networking" application. In this centralized model, the VoIP operator authenticates each WebPhone and routes calls between them using classical web-based protocols, as for example *FlashPlayer* and TLS for security aspects.

2.1.2 Threats and Protection Mechanisms in the Intra-domain Context

Several threats have been identified in previous architectures: signalling or media flows tapping, DoS, identity hijacking or endpoint compromission. Nevertheless, these threats are not linked to VoIP protocols themselves but rather to the vulnerability of the underlying layers and they are common to many applications. Therefore they are solved with "classical" protection mechanisms: system and application hardening, access filtering, flows priorization and transport over secure links. However, security protocols like TLS may raise performance issues for the servers [8] when facing a large number of endpoints. Other non-VoIP specific threats have been identified in the *VoIP P2P architecture* [9] as well as in the *VoIP web-based architecture* where automated WebPhone account creation may lead to the same undesirable consequences as in WebMail. For the latter, the CAPTCHA[3] protection has showed its limits [10], and even if enhancements are proposed [11], the balance between CAPTCHA robustness and usability is tricky to find [12].

In parallel to these threats, targeted DoS attacks threaten highly the VoIP protocols because of their complexity and the need to keep dialog and call context. Another VoIP specific threat foreseen is SPIT (SPam over Ip Telephony), due to the low cost of VoIP calls and the possibility to automate the call broadcasting (two characteristics which do not exist in the PSTN). Call automation is possible from soft-phones, thus primarily in VoIP P2P and web-based architectures but now also in operator architectures with new mobile endpoints. Nevertheless, SPIT prevention in the intra-domain context is much easier than in the inter-domain one because the administrator is able to authenticate the endpoints and usually stands in the signalling path. This way, detection algorithms as proposed in [13] are efficient, provided detection thresholds are correctly tuned.

2.2 Inter-domain Context

Initially, VoIP inter-domain call establishment was envisioned in the same way as e-mail. This first approach, noted "open model" hereafter, presents many security risks whose origins are explained by one of the Internet founders in [14]. Thus VoIP interconnections are currently set up in a more conservative way, called "closed model" (or private federation) hereafter. Before browsing these two models, we must highlight the strong regulation constraint that applies to VoIP as opposed to many web services like e-mail or social networks which are seen as "best-effort" services and thus much less regulated (up to now). According to [15], VoIP regulation poses severe constraints, especially in the inter-domain context and may turn some models off.

[3] Completely Automated Public Turing test to Tell Computers and Human Apart.

2.2.1 Open-Interconnection Model

This model is promoted mainly by IETF and assumes that IP connectivity between endpoints, proxies or domains is sufficient to establish multimedia communications. In theory, the calling endpoint (or proxy) triggers a DNS lookup based on the callee identifier to localize one of the incoming proxies in the receiving domain. It then sends the INVITE request to the receiver proxy, without any preliminary relationship needed between the sending and the receiving domains.

The first major issue here is that VoIP identifiers are designed to convey a domain part but as, explained in [16], because of the large hard-phone installed base and of the PSTN predominance, most VoIP calls originate from or terminate in a PSTN cloud. Consequently caller (or callee) identifiers lack the domain part, so inter-domain calls are tricky to route and also to verify for the receiving domain which may be misled with spoofed caller identifiers. Authors of [16] acknowledge that a public-ENUM-like system is required to turn an E.164 phone number into a routable SIP URI, but they argue that such a system will never emerge.

Other security threats related to this model are summarized in [17]; they concern the identification and localization functions of the receiver, the DoS risks over interconnection points, the tapping or degradation of signalisation or media flows conveyed over Internet and the SPIT risks. The accumulation of DoS and SPIT risks over the interconnection points is called the "pinhole problem" in [16] and constitutes the second major issue with this model.

Concerning the SPIT threat, a parallel was quickly drawn with SPAM in [18]. This synthesis shows that SPIT and SPAM have common motivations and origins[4]. By the way, similar protection principles (except content filtering) may apply: white or black lists checking, circles of trust, CAPTCHA or mathematical puzzle submission, payment at risk. These first mechanisms generally increase the complexity of the protocol exchanges and require the sources to be authenticated and stable. Unfortunately, it was shown that hackers were able to quickly change the sources of theirs attacks [19]. Another prevention technique called "consent-based" performs preliminary notification before the establishment of a first call to fetch the agreement of the receiver, thus solving the "introduction problem" explained in [18]. Finally, marking mechanisms can be used, based on several call criteria, to evaluate the probability that this one may be SPIT [20], [21]. Most of the above protection principles apply equally to the closed model described in next chapter.

Among the pro-active security mechanisms, *SIP Identity* [22] was proposed for the open-interconnection model. It is built on the same principles as the IETF DKIM protocol for e-mail: the sending domain signs the SIP INVITE request with a signature calculated over the key fields of the request and the receiver is able to verify the request integrity and to authenticate the sending domain[5]. However, we foresee several limitations with this protocol:

---

[4] Mainly the difficulty to authenticate sources, the possibility to address interconnection points from the Internet and the existence of compromised endpoints botnets.

[5] Beforehand, the receiving domain has to fetch the sending domain public key.

- The sender's public key fetching and checking, as well as the signature verification are resource consuming steps for the receiver that may expose him to DoS risk[6].
- The signature validity authenticates the sending domain but does not guarantee that the caller's phone number (or identity) has not been spoofed.
- Since the INVITE request has no confidentiality protection, it can not convey a session key to encrypt the media flows.

To solve this last limitation, IETF proposals ZRTP or DTLS-SRTP which perform a key handshake in the media plane (after the call signalling is established) may be used but they are challenging as regards to legal requirements[7] and moreover they require integrity protection at the signalling level for end-to-end security, as explained in [24]. When restricting the study scope to VoIP signalling security, TLS (or IPSec) may be used for hop-by-hop security and media key encryption. However, this approach leaves the E.164 phone number problem unresolved and requires the establishment of secure link prior to sending the INVITE request. As a result, specific security protocols like IETF MIKEY have been standardized for the establishment of secure multimedia sessions (without relying on lower layers security). The MIKEY protocol enables the key exchange to be integrated in the VoIP signalling and it supports several authentication modes. A more detailed analysis of MIKEY, along with other multimedia key exchange protocols (SDES, ZRTP, DTLS-SRTP), can be found in [24]; this study shows the DoS risks on several of these protocols.

2.2.2 Closed-Interconnection Model

In order to limit the risks identified in the open model, the first VoIP domains interconnections were performed through the PSTN, i.e. using contract between operators, secured links and more generally architectures isolated from the Internet.

In parallel, the 3GPP consortium has specified architectures to offer the same level of security and QoS as in PSTN but with IP protocols. These architectures are thus based, as in PSTN, on trusted links and secured interconnections between at least two domains, the model being designed to support any number of peers. The relevant standards are the IMS (IP Multimedia Subsystem); they specify a set of VoIP functions which reuse as much as possible the existing VoIP and security protocols (SIP, SDP, RTP, IPSec, and Diameter). The IMS defines the VoIP access for both mobile and fixed endpoints, as well as the roaming functions.

Within the IMS, security issues listed above are solved: the confidentiality and integrity of media and signalisation flows are guaranteed with IPSec tunnels. The user authentication is done in each domain and E.164 information is shared between domains to enable secure call routing and caller identification. Finally, protection against DoS attacks relies on topology hiding functions that make the interconnection points addressable only from the partner domains. In return, the IMS security model presents an inherent complexity which may have performance impacts, according to [26], especially in the core network.

[6] Some performance enhancements were proposed in [23] based on elliptic curves algorithms.
[7] This is explained in section 7.5.3 of [25] dealing with media plane security.

3 Analysis of Token or Ticket Based Security Mechanisms

In the remaining of this article we only consider the security protocols applying at the VoIP signalling level and in this section we focus on a specific class of security mechanisms based on tokens or tickets, which may be generated with a cryptographic function. These mechanisms address some of the issues identified previously, especially the "introduction problem" explained in [18], the routing/verification of E.164 phone numbers and also the "pinhole problem" explained in [16] which is the accumulation of DoS and SPIT risks over the interconnection points. They may apply to several of the architectures seen previously, especially the open-interconnection model which has the highest risks.

3.1 Out-of-Band Token Exchange

This mechanism [27] addresses the SPIT threat and also the introduction problem. It recognizes that black lists have limited effectiveness and that white lists are useful only if the first call from a new person is not systematically blocked. It assumes people usually have at least one previous contact before placing a VoIP call, such as e-mail or electronic business cards exchange. During this "cross-media relation", users exchange information which is then inserted as an authentication token in the VoIP call establishment request.

A first type of information is a VoIP identifier (e.g. SIP_URI) that the caller offers to potential callees. The callee stores this token and later uses it to label and filter any incoming call from this caller. Alternatively, a second type of information is weakly-secret value provided by a callee to potential callers who then insert it also in the SIP INVITE request. In both cases this can be considered as a "consent-based" approach.

The main advantage of this mechanism is the simplicity of token checking for the callee which limits the DoS risks and is efficient against blind calls. On the other hand, the callee has to store or distribute many tokens in a secure way to prevent spoofing. Since tokens have mid to long-term validity, any token theft will have disturbing consequences for the callee. Finally, obtaining and inserting tokens with non-VoIP endpoints may be a constraint for a lot of users.

3.2 Return Routability Test (RRC)

This mechanism [28], in association with SIP Identity [22], aimed to solve the risk of caller identifier spoofing. Its objective is to determine if a domain rightfully "owns" an E.164 phone number which appears in association with this domain name in the SIP caller identifier field of an INVITE request. Although the corresponding IETF draft has expired, this mechanism is mentioned here as an historical approach.

The basic idea is that when the callee receives a SIP INVITE request with an E.164 phone number in the caller identifier field, it sends an out-of-dialog verification request towards that E.164. The verification request contains the claimed E.164 caller identifier and a unique random token (nonce). Upon receipt of this request, the caller (or sending proxy), if it is legitimate for this E.164 number, sends back an acknowledgement containing the received token and the domain signature according to [22].

The callee then has to check that the signature in the acknowledgement response and the one in the SIP INVITE request are from the same domain.

The tricky point here is that the correct routing of the verification request to the E.164 calling number relies on SIP routing and thus leads to the already explained phone number routing problem. From this point, it appears that a trusted third party is necessary at least for secure routing and verification of phone numbers identifiers and this principle is retained in the following mechanisms.

3.3 Secure Call Establishment with KMS Like Trusted Third Party

This mechanism was initially proposed within 3GPP [25] and then in IETF [29] as an extension to the MIKEY protocol; it is designed for integration in VoIP signalling. It follows Kerberos protocol basis and assumes each VoIP entity (A and B) has a pre-shared secret with KMS (Key Management Server) which is the trusted third party.

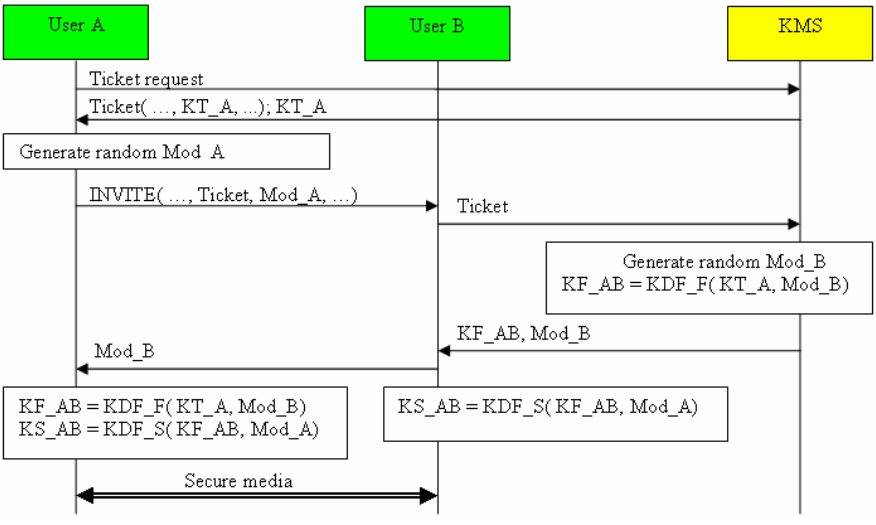

Fig. 1. Session signalling (from 3GPP TR33.828 source)

As shown in Figure 1, entity A authenticates to KMS which returns a ticket containing the master key KT_A encrypted for entity B along with the same key encrypted for entity A. Entity A includes this ticket with a random value Mod_A in the call establishment request sent to B. Then B forwards the ticket to KMS for checking. If the ticket is valid, KMS chooses a random value Mod_B and derives the session key KF_AB from KT_A and Mod_B. Then Mod_B and KF_AB (encrypted) are sent to B which forwards Mod_B to A. Entity A then derives KF_AB and both entities simultaneously compute the session key KS_AB.

In this approach, endpoint authentication and location as well as call routing are under KMS responsibility which guarantees the security of the whole exchange. However, in-band keys exchange creates large tickets and has a negative impact on transport. Also, we anticipate that entity B and KMS are both exposed to DoS attacks

because entity B has no means to check if the request from entity A is valid and will indiscriminately forward invalid tickets to KMS while creating a new context on its side.

3.4 Hybrid Model

The very recent proposal *VIPR* [16] merges VoIP, P2P, PSTN technologies and benefits from the PSTN historical reliability to establish secure routing and authentication information.

In brief, each node of the P2P network is a call agent (CA) for a given VoIP domain. Each CA publishes in the P2P DHT all the user identifiers held by the domain. Once a PSTN call is completed, the calling CA contacts the called CA in the receiving domain[8] and uses the previous PSTN call information as pre-shared secret. In return, the called CA creates (and sends to the calling CA) a cryptographic token bound to the callee and the calling domain. This token also contains VoIP routing information (SIP URI) to reach this destination and is then inserted into future VoIP calls from this calling domain to this specific callee.

The main advantage of this model is to achieve secure phone numbers routing and verification, thus avoiding caller identity spoofing and associated SPIT risk. Also, the mechanism is gradual since the more PSTN calls are established, the more tokens are granted and the more VoIP calls can be further initiated. In return, we anticipate several issues. First, each domain must publish in the DHT all its user identifiers; this raises rather the same "philosophical" problems as ENUM adoption and also some scalability issues with large domains. Secondly, each domain needs to store securely a large amount of (call) tokens which is roughly proportional to its number of users. Moreover, since token validity is assumed to be endless, this requires robust cryptographic functions and very strong keys protection. Finally, this model relies on PSTN routing each time a new destination is called, that is to say *endlessly*.

4 Proposed Enhancements

4.1 Framework Objectives and Positioning with Regards to State of the Art

The SIDE (Secure Inter-Domains Exchange) framework described in this section is a secure VoIP call establishment mechanism, operating at the signalling level, and aimed at open inter-domain interconnections. Its main objective is to reduce DoS and SPIT risks on the receiver side, i.e. to optimize the steps related to authentication and establishment of a master key between far end entities. Complementary objectives are: support for sporadic communications, with no need to set up a secure connection before placing the SIP INVITE request, support for endpoint roaming through visited domains and compatibility with current VoIP architectures (especially UDP transport). It also addresses the usual security requirements of integrity and confidentiality protection. Because of the paper size constraint we only provide an overview of this mechanism without proving its security properties.

[8] The contact address of the called CA is provided by the DHT based on callee identifier.

The SIDE framework borrows some principles from the mechanisms presented in section 3 and aims at improving them. From [27], it keeps the idea of identification token inserted in the SIP INVITE but removes the need of "cross-media relation" to obtain the token; also the token validity is limited to only one call for security reasons. From [28], it keeps the principle of a nonce token returned by the callee domain upon reception of the "call establishment request". This nonce token is indeed necessary for the caller to compute the session key and to further create a valid SIP INVITE request. From *KMS* approach [29], it keeps the principles of session establishment based on a trusted third party and the use of symmetric cryptography (as opposed to [22]) for performance purpose. However, the protocol exchange is organized in a different way as [29] to reduce the DoS risks on the receiving domain. Also the session key is not conveyed in the signalling exchange thus reducing the messages size and the cryptanalysis risks. From *VIPR* approach[16], it keeps the principle of (at least) one trusted third party per VoIP domain which is responsible for endpoint authentication, call routing and verification. The need for a trusted third party appeared all along the paper both for security reasons and for call routing, but it is also necessary for regulatory constraints [15] such as legal call interception. As opposed to [16], the proposed framework does not require the storage of a huge amount of cryptographic tokens.

4.2 Design Principles

The following principles were retained for design:

- *Inter-domain initial exchange*: this phase is performed only once between each pair of domains and enables them to exchange their lists of SIDE Primary Server (SPS), a Shared Master Key (SMK) and a couple of other parameters such as the maximum number of simultaneous transactions. Each domain shall declare at least one SPS which is considered as a trusted third party and is in charge of transactions authorization. SIDE Intermediary Servers (SIS) may also be involved in transactions but do not need to be declared thus making the management easier. The initial phase is under the control of the receiving domain which does not need to check *a posteriori* for the sending domain policies as in [22]. In the same way as existing protocols (TLS, IKE, MIKEY), the SMK is based on Pre-Shared Key (PSK) session establishment.
- *Call notification*: before triggering the SIP-INVITE request, a notification request is first sent to the receiving side to query consent. Since this request is much lighter than SIP-INVITE it saves processing for the receiving domain, especially if the call is declined. Furthermore, information is exchanged in clear during the notification phase, in the form of a Nonce-Token (NT), to compute the Transaction Master Key (TMK). Eventually, pre-routing may be achieved during this phase to direct the SIP INVITE request to the right entity in the receiving domain, thus saving processing in intermediary entities.
- *Insertion of an Identification-Token* (IT) inside the SIP-INVITE request which authenticates a given transaction and can be checked straightaway by the receiver[9], thus limiting DoS risks.
- *Use of symmetric cryptographic* algorithms for performance considerations.

[9] Checking of the received IT value is done by comparison to the pre-computed expected value.

4.3 Overview of the Protocol Exchange

Figure 2 shows the sequencing of a SIDE transaction, that is the protocol exchange leading to the acceptation of the SIP-INVITE request with the Identification-Token by the receiving entity[10]. We assume the inter-domain initial exchange has been previously completed and led to the establishment of the SMK secret value between the two domains.

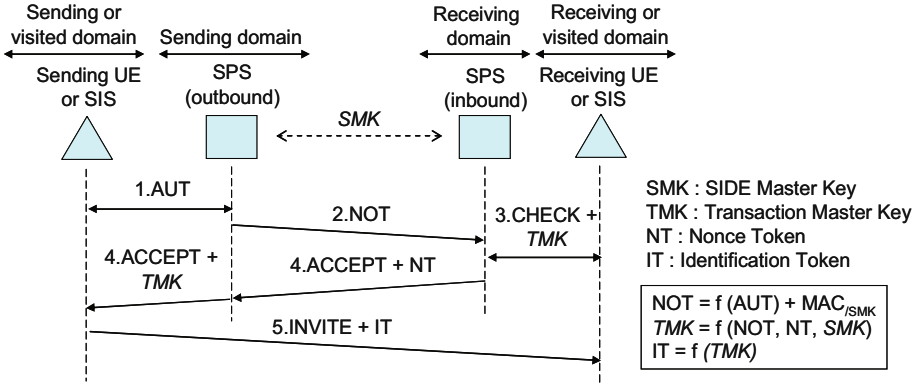

Fig. 2. SIDE protocol exchange overview

Step 1: The user endpoint (UE) or SIS in the sending domain detects an inter-domain call request and sends a transaction authorization request (AUT) towards the SPS. This request is based on the underlying SIP INVITE information and contains the call main characteristics, especially caller and callee identifiers, contact and media addresses. Optionally, the SPS requires and triggers user endpoint authentication.

Step 2: If SPS accepts the AUT request, it sends a notification request (NOT) towards one of the SPS in the receiving domain it previously learnt from the *Inter-domain initial exchange*. The NOT request combines AUT information with sending SPS information and a MAC (Message Authentication Code) based on the SMK key.

Step 3: If the NOT request is valid (MAC check) and the receiving SPS accepts the transaction it then computes the TMK value which is based on the information contained in the NOT request, the SMK key and a random value NT (Nonce-Token) created for this transaction. Prior to accepting the transaction, the receiving SPS may check white or black lists, query UE consent, or apply any other relevant filtering. If the transaction is accepted, the callee is sent the TMK value along with the transaction characteristics.

Step 4: The receiving SPS notifies its consent to the sending SPS; the answer includes the NT value and a MAC based on SMK key for integrity protection. Since the NT value is short and does not need to be encrypted, there is a significant advantage compared to [29] where the ticket is much longer and the keys it conveys have to be

[10] And the subsequent sharing of the TMK secret between the initiator and the responder.

encrypted. Upon receipt of the NT value, the sending SPS computes the TMK key and forwards it to the sending entity.

Step 5: The sending entity derives the IT (Identification-Token) value from the received TMK value and inserts it into the SIP-INVITE request it sends towards the receiving entity. The IT value in itself is not sufficient to ensure the INVITE request integrity, thus a MAC code based on a key derived from TMK should be added. The receiving entity checks the IT value of the SIP-INVITE request from a pre-calculated list and retrieves the corresponding TMK key it now shares with the caller; it also verifies the MAC value. The IT check is trivial for the receiving entity in contrast to [29] where the KMS has to be contacted to verify the ticket and extract the corresponding key.

5 Conclusions

In the first section we identified the current stakes in VoIP security showing that the risks are limited in intra-domain context but become higher in the inter-domain context due to possible DoS or SPIT on the interconnection points and the difficulty to authenticate network sources and validate caller identifiers. Whereas the closed-interconnection model removes most of these risks it may have difficulties in supporting more sporadic any-to-any services. The open-interconnection model requires efficient security mechanisms which have been analysed in sections 2 and 3. Finally the paper presented a very general overview of the SIDE framework which is inspired from the mechanisms presented in section 3 while bringing some enhancements. Future work around this framework includes: prototyping, performance analysis, formal verification of security properties and finally design of an alternate mode not requiring notification for each call.

Acknowledgments. The authors would like to thank Henry Gilbert, Joaquin Garcia-Alfaro, Nora Cuppens and Frédéric Cuppens for their helpful comments as well as Sarah Cook for her help with the English wording.

References

1. Blake, E.A.: Network Security: VoIP Security on Data Network-A Guide. In: Information Security Curriculum Development Conference (2007)
2. Feijoo, C., Gomez-Barroso, J.L., Rojo-Alonso, D.: A European Perspective of VoIP in Market Competition. Communications of the ACM (November 2008)
3. Abdelnur, H., et al.: Assessing the security of VoIP Services. In: The 10th IFIP/IEEE Symposium on Integrated Management (2007)
4. Griffin, S., Rackley, C.: Vishing. In: InfoSecCD'08: Proceedings of the 5th annual conference on Information security curriculum development (2008)
5. Endler, D., Collier, M.: Hacking VoIP Exposed. McGraw-Hill Osborne Media, New York (2006)
6. VoIPSA: VoIP security and privacy threat taxonomy. Public Realease 1.0 (October 2005)
7. Jennings, C., et al.: A SIP Usage for RELOAD. IETF Draft draft-ietf-p2psip-sip-03 (October 2009)

8. Coarfa, C., Druschel, P.: Performance Analysis of TLS Web Servers. ACM Transactions on Computer Systems, TOCS (2006)
9. Sit, E., Morris, R.: Security considerations for peer-to-peer distributed hash tables. In: Druschel, P., Kaashoek, M.F., Rowstron, A. (eds.) IPTPS 2002. LNCS, vol. 2429, p. 261. Springer, Heidelberg (2002)
10. Yan, J., Ahmad, A.: A Low-Cost Attack on a Microsoft CAPTCHA. In: Proceedings of the 15th ACM conference on Computer and communications security (2008)
11. Athanasopoulos, E., Antonatos, S.: Enhanced CAPTCHAs: Using Animation to Tell Humans and Computers Apart. Communications and Multimedia Security (2006)
12. Yan, J., Ahmad, A.: Usability of CAPTCHAs Or usability issues in CAPTCHA design. In: Symposium On Usable Privacy and Security (SOUPS) (July 2008)
13. Mathieu, B., et al.: SPIT mitigation by a network level anti SPIT entity. In: VSW'06: Third annual security workshop (2006)
14. Cerf, V.G.: Spam, Spit and Spim. Communications of the ACM (April 2005)
15. Hill, J.: The Storm Ahead: How CALEA will turn VoIP on its head. In: InfoSecCD '06: 3rd annual conference on Information security curriculum development (2006)
16. Rosenberg, J., Jennings, C.: Verification Involving PSTN Reachability: The ViPR Access Protocol (VAP). Draft IETF draft-rosenberg-dispatch-vipr-vap-00 (November 2009)
17. Niccolini, S., et al.: SPEERMINT Security Threats and Suggested Countermeasures. Draft IETF draft-ietf-speermint-voipthreats-01 (July 2009)
18. Rosenberg, J., Jennings, C.: The Session Initiation Protocol (SIP) and Spam. IETF RFC5039
19. Pathak, A., et al.: Botnet Spam Campaigns Can Be Long Lasting: Evidence, Implications, and Analysis. In: SIGMETRICS '09: Measurement and modeling of computer systems (2009)
20. Nassar, M., et al.: Holistic VoIP intrusion detection and prevention system. In: IPTComm '07: Principles, systems and applications of IP telecommunications (2007)
21. Fiedler, J., et al.: VoIP defender: highly scalable SIP-based security architecture. In: IPTComm '07: Principles, systems and applications of IP telecommunications (2007)
22. Peterson, J., Jennings, C.: Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP). IETF RFC4474 (August 2006)
23. Rebahi, Y., et al.: Performance analysis of identity management in the Session Initiation Protocol (SIP). In: ACS International Conference on Computer Systems and Applications, AICCSA (2008)
24. Floroiu, J., Sisalem, D.: A comparative analysis of the security aspects of the multimedia key exchange protocols. In: Principles, systems and applications of IP telecommunications, IPTCom (2009)
25. IMS Media Plane Security. 3GPP TR33.828-161 (December 2009)
26. Tonesi, D.S., Salgarelli, L., Tortelli, A.: Securing the signaling plane in beyond 3G networks: analysis of performance overheads. Security and Communication Networks (2009)
27. Ono, K., Schulzrinne, H.: Have I Met You Before? Using Cross-Media Relations to Reduce SPIT. In: Principles, systems and applications of IP telecommunications, IPTCom (2009)
28. Wing, D.: SIP E.164 Return Routability Check (RRC). IETF draft-wing-sip-e164-rrc-01 (February 2008)
29. Mattsson, J., Tian, T.: MIKEY-TICKET: An Additional Mode of Key Distribution in MIKEY. IETF draft-mattsson-mikey-ticket-00 (October 2009)