Intégration des mots de passe à usage unique dans SIP

Rim Moalla[*+], Ahmed Serhrouchni[*], Sihem Guemara[+], Thomas Guillet[*]

[*]Institut Telecom/ParisTech
46 Rue Barrault, 75013 PARIS Cedex
France

[+]Ecole Supérieure des Communications de Tunis
2083, Ariana
Tunisie

moalla@enst.fr

RÉSUMÉ. Le protocole SIP devient de plus en plus la base des solutions de téléphonie sur IP. Ce travail porte sur le service d'authentification supporté par SIP. Ce service par ailleurs tient une place centrale pour les opérateurs comme pour les particuliers. L'authentification dans SIP est en générale basée sur un secret partagé entre un client et un proxy SIP. Ainsi, nous proposons une solution d'optimisation et de renforcement de l'authentification dans SIP. Cette solution consiste à intégrer à SIP des mots de passe à usage unique tout en préservant une interopérabilité avec le standard SIP. Cette solution a été validée par une intégration à l'API JAIN qui est un support de nombreuses plateformes basées sur SIP.

ABSTRACT. The SIP protocol is in line to become the basic of solutions for IP Telephony. This paper focuses on the authentication service supported by SIP. This service is central to both operators and individuals. Authentication in SIP is generally based on a shared secret between a client and a SIP proxy. Thus, we propose an optimized and enhanced solution for authentication in SIP. The solution consists on the integration of one time password on SIP while preserving interoperability with standard SIP. This solution has been validated by integration with the JAIN API. This API is support for multiple platforms based on SIP.

MOTS-CLÉS: SIP, Authentification, One Time Password, API JAIN, VoIP.

KEYWORDS: SIP, Authentication, One Time Password, API JAIN, VoIP.

1. Introduction et motivations

Le passage à la téléphonie sur IP se poursuit dans la quasi-totalité des infrastructures de téléphonie. Le protocole SIP (Session Initiation Protocol) [14] est par ailleurs le standard le plus émergeant pour la téléphonie sur IP. Ce qui justifie l'intérêt porté sur SIP. La sécurité de la téléphonie sur IP est devenue rapidement l'une des priorités de l'ensemble des acteurs ou des usagers de la téléphonie sur IP. Une communauté toujours plus grande s'investie et contribue aux solutions de sécurité de la téléphonie sur IP. Ces solutions portent aussi bien sur la signalisation que sur le média. Dans cette proposition nous nous intéressons uniquement à la composante signalisation et donc au protocole SIP. Nous n'avons pas comme ambition de proposer une solution totalement sécurisée, mais essentiellement renforcer le mécanisme d'authentification existant. Cette solution a été présentée par nous même dans [6] avec une validation formelle mais sans une validation concrète par une implantation et une mise en œuvre, ce qui fait l'objet de cet article. Nous avons choisi une API JAIN [12] très largement utilisée pour la conception des softphone, hardphone et des serveurs ou proxy SIP. Cette approche facilitera le déploiement de la solution que nous proposons.

L'authentification intégrée dans SIP est relative au standard [3]. C'est une authentification par mot de passe assez bien établie qui consiste à l'envoie : du mot de passe en clair ou du condensat résultat de l'application d'une fonction de hachage à un mot de passe combiné avec un nombre aléatoire reçu précédemment par le serveur. La transmission du mot de passe en clair présente des vulnérabilités notamment l'écoute et donc le rejeu. La transmission du condensat semble plus robuste mais présente également quelques faiblesses [5]. D'autres propositions sont faites [1] notamment par l'usage des certificats par l'intermédiaire des protocoles comme TLS [2] et IPsec [10]. Ces solutions par certificats présentent des avantages sur les mots de passe, néanmoins elles nécessitent des infrastructures de distribution de clé qui impactent les coûts aussi bien au niveau des performances qu'au niveau économique. Par ailleurs, l'usage des différents protocoles nécessitent des architectures particulières et des politiques de sécurité que l'ensemble des entités communicantes doivent respecter.

C'est ainsi que l'authentification par mot de passe dans SIP reste la plus usuelle actuellement. Le renforcement de cette méthode nous semble opportun. Nous avons intégré un nouveau mode d'authentification par mot de passe. D'abord en optimisant le protocole d'authentification par un envoi d'un « authentifiant » par anticipation. Ensuite en renforçant l'authentification par mot de passe en nous basant sur une méthode de génération de mot de passe à usage unique. Nous décrivons d'une manière détaillée ces différents mécanismes et leur mise en œuvre au sein de l'API JAIN.

Nous commençons par une présentation rapide de SIP et les mécanismes d'authentification associés. Ensuite nous présentons le principe des méthodes de

génération de mot de passe à usage unique avec un point particulier sur le standard HOTP (Hmac One Time Password) [11]. Dans la section qui suit, nous proposons une solution qui consiste à intégrer un mot de passe à usage unique comme protocole d'authentification. Nous terminerons par une présentation de la validation expérimentale de ces résultats par une implémentation enfin suivra une conclusion qui résume cette contribution et dresse les perspectives.

2. Le protocole SIP et mécanisme d'authentification associé

La téléphonie en général se base sur deux composantes : une qui assure la signalisation (notamment l'établissement de l'appel) et l'autre qui assure le transport des média. Le protocole SIP est une composante de signalisation pour la téléphonie sur IP. Ce protocole a été défini dans le groupe MMUSIC de l'IETF initialement comme protocole pour l'établissement, la modification, et la terminaison de session multimédia.

SIP est un protocole de niveau applicatif. Les éléments de données du protocole (PDU) SIP sont de type requêtes/réponses et sont codés en ASCII. Son fonctionnement est similaire aux protocoles HTTP [4] et MIME [15]. Ainsi ces requêtes et réponses sont composés d'en-têtes comparables à ceux des protocoles HTTP ou MIME.

Nous nous limitons dans cette partie à décrire les éléments de SIP nécessaire à cette proposition. On trouvera des descriptions complètes de SIP dans [14]. Certains en-têtes sont communs aux requêtes et réponses. Il y a donc des en-têtes qui sont spécifiques soit aux requêtes, soit aux réponses. Il y a par ailleurs des en-têtes obligatoires et des en-têtes optionnels. L'en-tête ***Call-ID*** est présent dans l'ensemble des requêtes réponses et il est suivi d'une valeur commune à l'ensemble des échanges relatifs à une session donnée. Cette valeur unique est calculée par l'entité qui établit l'appel. Deux requêtes de SIP peuvent nécessiter une authentification : -*REGISTER* qui assure l'enregistrement d'un usager afin de pouvoir le localiser lors d'un appel entrant. -*INVITE* qui assure l'établissement d'un appel.

Dans le cas de l'authentification, le proxy (ou IPBX) transmet une réponse avec un code d'erreur 401 signifiant au client de s'authentifier. Cette réponse contient des entêtes relatifs au standard [3] qui indique la méthode d'authentification à utiliser et les paramètres nécessaires pour cette authentification. Ainsi deux méthodes sont supportées l'une qu'on nomme Basic (le mot de passe est transmis en clair) et l'autre qu'on nomme Digest (on applique une fonction de hachage au mot de passe et un nonce ou challenge transmis dans la réponse, et le résultat caractérise l'authentifiant qui sera transmis au proxy). Le standard SIP exige le déploiement de méthode Digest [16]. Si on considère par exemple le cas d'enregistrement d'un client, présenté dans la figure 1, après l'envoi de la requête REGISTER, le client reçoit systématiquement une réponse avec un code d'erreur pour pouvoir s'authentifier par la suite. La transmission d'un nonce ou

attaques par rejeu. L'attaque
ification.

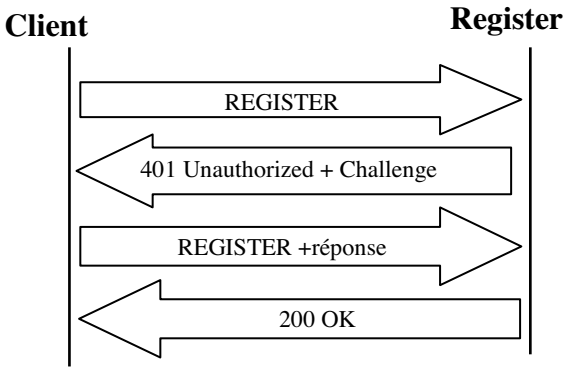

Figure 1. *Enregistrement avec authentification Digest dans SIP*

3. Les mots de passe à usage unique : HOTP

Les protocoles d'authentification basés sur les mots de passe sont les plus déployés [8]. Ce choix est justifié par la simplicité de leurs implémentations. L'authentification par les mots de passe a plusieurs faiblesses qui ont été largement établies [7]. Les mots de passe à usage unique ou en anglais les One Time Password (OTP) [7] ont été proposés pour renforcer l'authentification par mots de passe. Un mécanisme d'OTP génère, à chaque demande d'authentification, un mot de passe unique basé sur trois paramètres qui sont : une fonction de hachage, un secret et un challenge ou un compteur. La génération d'un mot de passe à usage unique nécessite une coordination entre le client (demandeur) et le serveur (vérifieur). Cette coordination peut être soit explicite basée, par exemple, sur un challenge, soit implicite basée sur un compteur ou une horloge. Les mots de passe générés par le standard de l'IETF HOTP [11] font parties de la deuxième catégorie. HOTP exige le partage d'une clé secrète (Ks) et un compteur (C) entre le client (ou prouveur) et le serveur (ou vérifieur). C'est sur la base des l'application de l'algorithme HMAC-SHA1 [9], que HOTP génère un mot de passe unique. Le challenge est donc implicite (basé sur la valeur du compteur).

Le problème de la synchronisation des compteurs est résolu par la création d'une fenêtre glissante du côté du serveur. Dans [11], plus d'explications sont données pour le problème de la synchronisation.

4. Le schéma d'authentification proposé

4.1. Principe

Les messages SIP sont formés d'en-têtes auxquels sont associés des valeurs opaques. Pour l'entête Call-ID la valeur associée doit être unique et non prédictible. Notre approche consiste à donner une sémantique à cette valeur. Nous proposons d'attribuer comme valeur au Call-ID, un mot de passe à usage unique calculé sur la base de HOTP. L'en-tête Call-ID, qui est l'identifiant unique d'un appel, assure en plus la fonction d'authentification du client.

Dans notre schéma, le client anticipe le processus d'authentification vu qu'il envoi son authentifiant dés la première requête (avant de recevoir un message d'erreur). Le serveur authentifie donc l'utilisateur sur la base du mot de passe inclus dans l'entête Call-ID. Ainsi les en-têtes d'authentification présentés dans standard HTTP [3] et repris par le protocole SIP ne sont plus nécessaires dans notre cas.

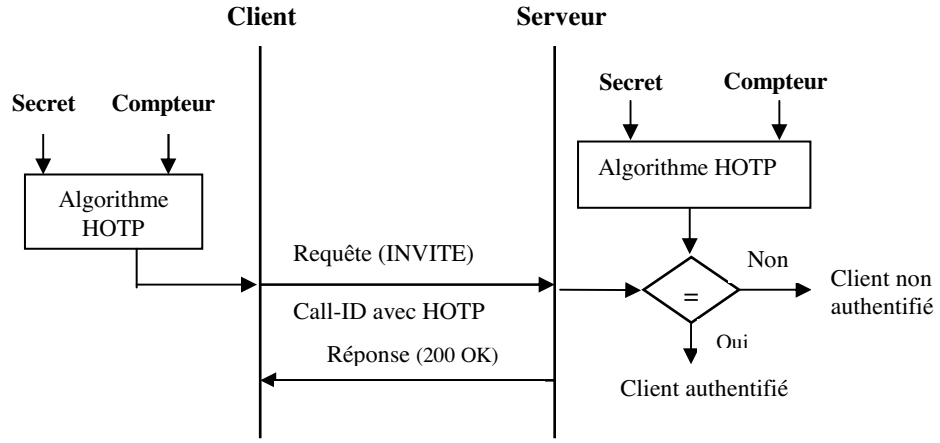

Figure 2. *Authentification dans SIP avec HOTP*

Dans un précédent article [6] nous avons validé formellement cette proposition. Comme on l'a souligné précédemment notre apport dans cet article réside dans la conception et implantation de cette approche.

4.2. Expérimentation et validation

Pour valider cette contribution, nous avons eu recourt à l'API standard JAIN SIP (Java APIs for Integrated Networks) qui est parmi les plus répandue pour SIP. L'API JAIN SIP offre une abstraction uniforme pour le protocole SIP. JAIN SIP est l'interface Java standardisée du protocole SIP pour de nombreuses applications client et serveur [12]. Elle permet de faire des transactions sans ou avec état et de contrôler le dialogue durant le déroulement du protocole SIP [13]. Elle garantit aussi l'interopérabilité [13].

Nous avons utilisé l'implémentation libre de l'API JAIN SIP disponible à partir du NIST [12]. Elle contient une implémentation de référence (RI), des exemples et quelques outils de base pour JAIN-SIP-1.2. Nos tests ont été effectués sur des plateformes diverses à base de système Unix et Windows de Microsoft.

Le code de JAIN SIP, côte client (UA), a été modifié pour générer un Call-ID avec la sémantique intégrant le mot de passe à usage unique HOTP (fig.3). La partie serveur (proxy) a été aussi modifié pour générer le mot de passe HOTP, lire et vérifier le Call-ID avec sémantique. Pour mettre en œuvre ce mécanisme, nous avons utilisé quelques fonctions disponibles en [11]. Un UA génère ses appels avec le Call-ID comprenant le mot de passe HOTP. Le serveur (proxy) extrait la chaîne du Call-ID contenant le HOTP pour authentifier l'UA SIP.

Pour éviter tout problème de compatibilité, nous avons traité et validé tous les différents cas de figures que ce soit du serveur ou du client (tableau 1).

Client modifié	Client non modifié	Proxy modifié	Proxy non modifié	Résultats
	✓		✓	Note 1
✓			✓	Note 2
	✓	✓		Note 3
✓		✓		Note 4

- Note 1 : authentification avec HTTP Digest : deux échanges.
- Note 2 : L'utilisateur est authentifié avec HTTP Digest, car le serveur ne peut pas vérifier le mot de passe contenu dans le Call-Id.
- Note 3 : Le serveur lit le Call-ID mais ne peut pas authentifier l'utilisateur. Il lui envoi un nonce et utilise donc HTTP Digest.
- Note 4 : L'utilisateur est authentifié avec HOTP en un seul échange.

Tableau 1. *Résumé des expériences*

5. Conclusion

L'authentification par mot de passe est sans aucun doute l'une des plus répandues. Ce type d'authentification est « culturellement » bien introduit et techniquement relativement « facile » à mettre en œuvre. Notre préoccupation est de ne pas bousculer cet état, mais de le renforcer. Les mots de passe à usage unique ont par ailleurs bien fait leur preuve et commence à être accepté et répandu. Nous avons introduit un HOTP : une méthode standard de génération synchrone de mot de passe à usage unique dans le protocole d'authentification de SIP. Cette approche maintient l'interopérabilité de SIP et renforce d'une manière certaine l'authentification classique par mot de passe. Nous avons utilisé des champs existants en leur donnant une sémantique pour atteindre notre objectif. La validation de cette solution par son intégration dans l'API JAIN facilitera son déploiement. Ainsi cette contribution permet un déploiement simple et une interopérabilité totale avec l'existant. Cette implantation était nécessaire pour proposer cette solution à l'IETF pour l'obtention du statut de standard.

Nos recherches futures s'orientent, vers l'authentification des requêtes « bye » et « cancel » afin de contrer les attaques de déni de service et vers l'authentification mutuelle éventuellement basée sur les mots de passe à usage unique.

6. Bibliographie

[1] EC. Cha, HK. Choi and SJ. Cho, *Evaluation of Security Protocols for the Session Initiation Protocol*, 16th International Conference on Computer Communications and Networks, Hawaii, 2007. Pages : 611-616.

[2] T, Dierks, and E. Rescorla, *The TLS Protocol Version 1.1*, RFC 3346, Avril 2006.

[3] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, and L. Stewart, *HTTP Authentication: Basic and Digest Access Authentication*, RFC 2617, Juin 1999.

[4]R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee, *Hypertext Transfer Protocol HTTP/1.1*, RFC 2616, Juin 1999.

[5] P. Gupta, and V. Shmatikov, *Security Analysis of Voice-over-IP Protocols*, Proc. 20th IEEE Computer Security Foundations Symposium 2007 (CSF '07), Juillet 2007.

[6] T. Guillet, R. Moalla, A. Serhrouchni and A. Obaid, *SIP authentication based on HOTP*, 7th International Conference on Information, Communications and Signal Processing, Macau, décembre 2009. Pages: 1-4.

[7] N. Haller, C. Metz, P. Nesser, and M. Straw, *A One-Time Password System*, RFC 2289, Fevrier 1998.

[8] S. Hallsteinsen, I. Jøstad, and D. V. Thanh, *Using the mobile phone as a security token for unified*, Proc. Second International Conference on Systems and Networks Communications (ICSNC 2007), Cap Esterel, France, August 2007.
[9] H. Krawczyk, M. Bellare, and R. Canetti, *HMAC: Keyed-Hashing for Message Authentication*, RFC 2104, February 1997.
[10] S. Kent, and R. Atkinson, *Security Architecture for the Internet Protocol*, RFC 2401, November 1998.
[11] D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, and O. Ranen, *HOTP: An HMAC-Based One-Time Password Algorithm*, RFC 4226, December 2005.
[12] National Institute of Standards and Technology (NIST). JAIN-SIP project home. https://jain-sip.dev.java.net/.
[13] P. O'Doherty and M. Ranganathan. *JAIN SIP tutorial*: serving the developer community. http://java.sun.com/products/jain/JAIN-SIP-Tutorial.pdf.
[14]J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley and E. Schooler, *SIP: Session Initiation Protocol*, RFC 3261, June 2002.
[15] B. Ramsdell, *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification*, RFC 3851, July 2004.
[16] S. Salsano, A. Polidoro and L.Veltri, *Extending SIP Authentication to exploit user credentials stored in existing authentication Databases*, 16th International Conference on Software, Telecommunications and Computer Networks, SoftCOM 2008. Split 2008. Pages 375-379.