Institut Eurécom
2229, Route des Crêtes
BP 193
06904 Sophia Antipolis
FRANCE

Rapport de Recherche 94-010

Demande de Brevet:

"Methode de Calcul d'Alias pour Utilisateur Mobile"

Didier Samfat

15 Aout 1994

Didier Samfat
E-mail: samfat@eurecom.fr
Tel: (+33) 93 00 26 31
Fax: (+33) 93 00 26 27

Contents

Abstract

La mobilité des utilisateurs est un service qui devient de plus en plus important de nos jours et est offert aussi bien par les réseaux fixes que par les réseaux téléphoniques cellulaires. Les besoins en sécurité qui en découlent en sont accrus et plus particulièrement la protection contre le pistage de l'utilisateur mobile. En effet, si aucune précaution n'est prise, l'écoute de la voie radio par un tiers fournit à ce dernier des renseignements quant à l'identité et aux déplacements de l'utilisateur mobile lors de la procédure d'accès au réseau. De ce fait, aucune entité a part l'utilisateur et son autorité administrative ne doit connaître la réelle identité ou la localisation de l'utilisateur durant son déplacement. Les réseaux mobiles existants soit ne traite pas le problème soit proposent des solutions qui ne sont pas satisfaisantes lorsqu' une parfaite confidentialité de l'identité est exigée.

Ce rapport decrit un algorithme permettant d'affecter un alias à un utilisateur mobile à chaque fois que ce dernier accède au réseau fournissant un haut degré d'intimité tout en étant indépendant de l'équipement utilisé. L'algorithme proposé permet une identification instantanée et non-ambigue de l'utilisateur par son authorité administrative (la réelle identité de l'utilisateur n'étant connue que de son autorité administrative). De ce fait, grâce à cette méthode, ni un intrus et ni aucune autre entité du réseau ne peut pister les déplacements de l'utilisateurs.

"Methode de Calcul d'Alias pour Utilisateur Mobile"

Didier Samfat
Institut Eurécom, Sophia-Antipolis, France
samfat@eurecom.fr

1 Introduction

Dans les environements mobiles, il arrive fréquemment qu'une entité X (un utilisateur ou un téléphone cellulaire) affiliée à une administration locale A_x, apparait dans un nouveau domaine géré par une administration différente A_y et désire obtenir des services. Ainsi, comme A_y ne connait pas l'identité de X, il doit autentifier X et obtenir une preuve de sa solvabilité. Il existe déjà plusieurs solutions connues a ce problème [1, 7, 4].

De manière générale, lors de la procédure d'accès au réseau mobile, X doit fournir une identification et la prouver. Cependant, si aucune précaution n'est prise, un tiers non-autorisé peut capter cette identification (par le biais le la voie radio ou à travers le réseau de signalisation) dévoilant ainsi la réelle identité de l'utilisateur ainsi que ses divers déplacements. Par conséquent la confidentialité de la localisation de l'utilisateur ainsi que de son identité deviennent une nécessité primordiale afin de fournir une intimité aditionnelle aux utilisateurs mobiles. De ce fait, seule l'autorité locale (A_x) doit être informée de l'itinéraire et de l'identification de X; l'autorité A_y doit uniquement obtenir une "autorisation" pour X. Les solutions offertes par les environements mobiles existants sont soient insuffisantes ou trop spécifiques pour assurer cette propiété.

2 Insuffisances des Solutions Existantes

Dans le cas GSM [1], la confidentialité de la localisation est assurée par l'affectation d'une identification temporaire (TMSI) lors de la phase d'autentification. Cependant, lorsque l'utilisateur accède au réseau dans un nouveau domaine pour la toute première fois, il est obligé de communiquer sa réelle identité (IMSI) en **clair** (non-chiffrée). De plus, si l'utilisateur est continuellement "traqué" par un tiers, il est possible pour ce dernier de correller l'IMSI avec les TMSI successivement affectés.

Une dernière remarque concernant GSM est que le réseau fixe est supposé sûre et de ce fait, l'identité de l'utilisateur est transféré en clair permettant aux autres autorités administratives de connaître la veritable identité de l'utilisateur.

L'approche de CDPD [7] repose sur le cryptage de l'identité du mobile. Avant que le mobile communique son identité, il engage avec l'autorité concernée un protocol , basé sur le modèle de Diffie-Hellman [5], qui permet aux deux entités de partager une clé secrète commune. Ensuite, l'utilisateur transmet cette identité cryptée avec la nouvelle clé partagée.

Cette solution présente deux problèmes. La première vient du fait que l'autorité du domaine visité connait la réelle identité du mobile. Même si dans le contexte de CDPD ce

fait est acceptable, de manière générale l'intimité de l'utilisateur mobile doit être préservée même lorsqu'il accède au réseau dans une nouvelle zone de localisation. Il est seulement necessaire et suffisant pour la nouvelle autorité d'avoir la confirmation de la solvabilité de l'utilisateur mobile par son autorité locale. Le deuxième problème concerne la nature même du protocol de Diffie-Hellman: un intrus se faisant passer pour la nouvelle autorité peut patager une clé secrète avec le mobile et donc de découvrir son identité en la déchiffrant avec la clé obtenue.

Une dernière remarque concerne le réseau UPT [8] qui a souligné le problème de la confidentialité de l'identité de l'utilisateur. Contrairement à GSM et CDPD, UPT n'a pas de solution concrète pour ce problème.

3 Avantages de la Méthode

Afin d'assurer une certaine anonymité à l'utilisateur mobile, la solution de base consite à affecter un alias à celui-ci lorsqu'il se déplace dans des zones de localisations éloignées. La methode proposée permer de générer de tels alias et possède en plus (contrairement aux solutions existantes) les caractéristiques suivantes:

- *Utilisation de l'alias une seule fois.* L'utilisation d'un alias statique à long terme peut permettre à un intrus qui traque les déplacements de l'utilisateur d'effectuer une corrélation entre cet alias et l'identité réelle de l'utilisateur. De ce fait, il est préferable d'utiliser un alias différent à chaque procédure de sécurité.
- *Aucune relation directe entre alias.* Aucune relation (corrélation) ne peut être effectuée entres les alias générés.
- *Séparation des domaines.* Même avec la conspiration de toutes les differentes autorités administratives (excepté l'autorité locale de l'utilisateur) il est impossible de découvrir l'identité réelle de l'utilisateur.
- *Utilisation de l'alias pendant l'autentification.* Dans un souci d'optimisation, l'algorithme proposée permet d'utiliser les alias en même temps que la procédure d'authentification contrairement à GSM et CDPD.

4 Description de la Méthode

La méthode proposée possède les caractéristiques décrites précedemment. En outre, elle permet de réconcilier deux notions paradoxales: l' authentification et la confidentialité de l'identité. En effet, pour autentifier une entité, celle-ci doit présenter une identité et prouver qu'elle connait un secret que seule l'identité proposé possède. Alors que la confidentialité de l'identité consiste à garder cette identité secrète.

Le principe fondamentale de la methode consiste à utiliser la technique des clés publiques qui implicitement contient une identité, contrairement aux clés secrètes partagées auxquelles il faut toujours fournir en plus une identité non-ambigüe au destinataire.

4.1 Notation

La notation suivante est utilisée pour la description de la méthode:

- Uid – Identification Universelle de l'utilisateur U avec son autorité locale
- AS_h – Autorité administrative de l'utilisateur
- AS_r – Autorité administrative du domaine visité
- P_h, S_h – Paire de clé publique et clé secrête de AS_h
- P_r, S_r – Paire de clé publique et clé secrête de AS_r
- N_u – Nombre aléatoire généré par l'équipement de l'utilisateur
- N_r – Nombre aléatoire généré par AS_r
- $P_x(A)$ – Chiffrement du message A avec la clé publique P_x
- MA_X – Message d'authentification calculé par X
- $\oplus$ – Opération de "ou-exclusif" (XOR)

4.2 Methode de calcul d'alias

Lorsqu'une entité A veut communiquer son identité à une autre entité B sans qu'un tiers ne puisse le découvrir, elle doit calculer un alias. Le principe de la méthode est le suivant:

1. L'entité A génére un nombre aléatoire N_a
2. A calcule un alias en utilisant la clé publique de B: $P_b(N_a, N_a \oplus A)$
3. Lorsque B reçoit cet alias, elle le déchiffre avec sa clé secrète S_b, obtient N_a et $N_a \oplus A$.
4. Finalement, B obtient l'identité de A en faisant $N_a \oplus N_a \oplus A$.

A noter que lorsque B reçoit $P_b(N_a, N_a \oplus A)$, elle sait déjà que cette expression a été calculée avec sa clé publique et donc n'a pas à connaître une identité et la clé secréte correspondante.

4.3 Authentification et Confidentialité de l'Identité

Le protocole ci-dessus permet de cacher l'identité de U et de AS_r d'un tiers. La condition de base est que la clé publique de AS_h soit stockée au niveau de l'equipement de l'utilisateur (smart-card, téléphone mobile). A noter que la relation entre l'utilisateur et son autorité est devoilée dans ce protocole; néanmoins, ceci peut être éviter si l'utilisateur obtient P_r de AS_r ou d'une autre entité du réseau. La description du protocol est la suivante:

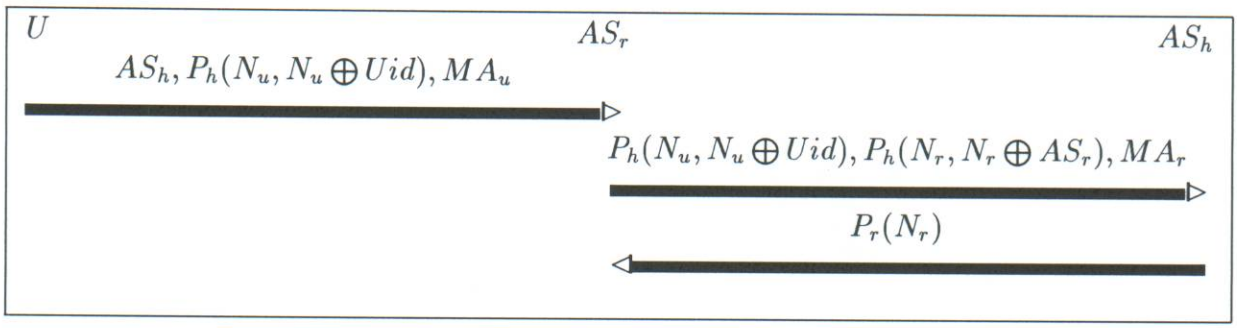


Figure 1: Protocole d'Authentification Intraçeable pour Utilisateur Mobile

1. L'utilisateur génére un nombre aléatoire N_u, calcule son alias $P_h(N_u, N_u \oplus Uid))$ est le transmet avec le message d'autentification à AS_r.

2. Lors de la réception du message initiale AS_r calcule son alias de la même manière puis son message message d'autentification et transmet le tout à AS_h.

3. Quant AS_h reçoit le deuxième message du protocole il déchiffre l'alias de U puis celui de AS_r en utilisant S_h. Ayant les identités réelles de U et de AS_h, il est capable de chercher les clés secrètes correspondantes pour verifier les différents messages d'authentification (MA_U, MA_r).

4. La transmission de $P_r(N_r)$ à AS_r permet de garantir à celui-ci du succès de l'authentification.

5 Applications de la Methode de Calcul d'Alias

Les application potentielles de l'algorithme sont nombreuses lorsque le besoin de cacher l'identité d'une entité est néçessaire. Ainsi, la méthode proposée peut être appliquée à n'importe quel protocol d'autentification que ce soit dans les domaines bancaires ou des réseaux mobiles. La condition de base est que l'entité puisse obtenir la clé public de l'entité destinatrice.

L'implémentation industrielle de l'algorithme dans le cas des réseaux mobiles est imédiate. En effet, deux possibilités sont envisageables: soit la clé publique de l'entité réceptrice est transmise par le biais d'un protocole spécifique à l'entité émetrice, soit elle est stockée dans une carte à puce ou dans une zone mémoire de l'équipement de l'entité émettrice. Dans tous les cas, un composant de l'équipement de l'entité émettrice devra pouvoir générer un nombre aléatoire, effectuer l'opération de ou-exclusif et chiffrer le tout avec une clé publique. Ces opérations sont parfaitement réalisables avec les technologies d'aujourd'hui.

References

[1] M. Rahnema, *Overview of the GSM System and Protocol Architecture*, IEEE Communications Magazine, April 1993.

[2] J. Steiner, C. Neuman, J. Schiller, *Kerberos: An Authentication Service for Open Network Systems*, Proceedings of USENIX Winter Conference, February 1988.

[3] R. Molva, G. Tsudik, E. Van Herreweghen, S. Zatti, KryptoKnight *Authentication and Key Distribution Systems*, Proceedings of ESORICS'92, November 1992.

[4] R. Molva, D. Samfat, G. Tsudik, *Authentication of Mobile Users*, IEEE Network Magazine, Special Issue on Mobile Communications, March/April 1994.

[5] W. Diffie and M. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory, November 1976.

[6] National Bureau of Standards, *Federal Information Processing Standards*, National Bureau of Standards, Publication 46, 1977.

[7] *Cellular Digital Packet Data (CDPD) System Specification*, Release 1.0, July 19, 1993.

[8] European Telecommunications Standards Institute, *Universal Personal Telecommunications*, ETSI NA7 WP1, November 1992.

[9] D. Chaum, A. Fiat and M. Naor, *Untraceable Electronic Cash*, Proceedings of Crypto'88, August 1988.

[10] D. Chaum, *Security Without Identification: Transactions Systems to Make Big Brother Obsolete*, CACM Vol. 28, No. 10, October 1985.

[11] RSA Data Security Inc., *The RC4 Encryption Algorithm*, Document No. 003-013005-100-000-000, March 12, 1992.

[12] M J.Beller, L F. Chang, Y. Yacobi *Security for Personal Communications Services: Public-Key vs. Private Key Approaches* Proceedings of 2nd International Symposium on Personal, Indoor and Mobile Radio Communications, October 1992.

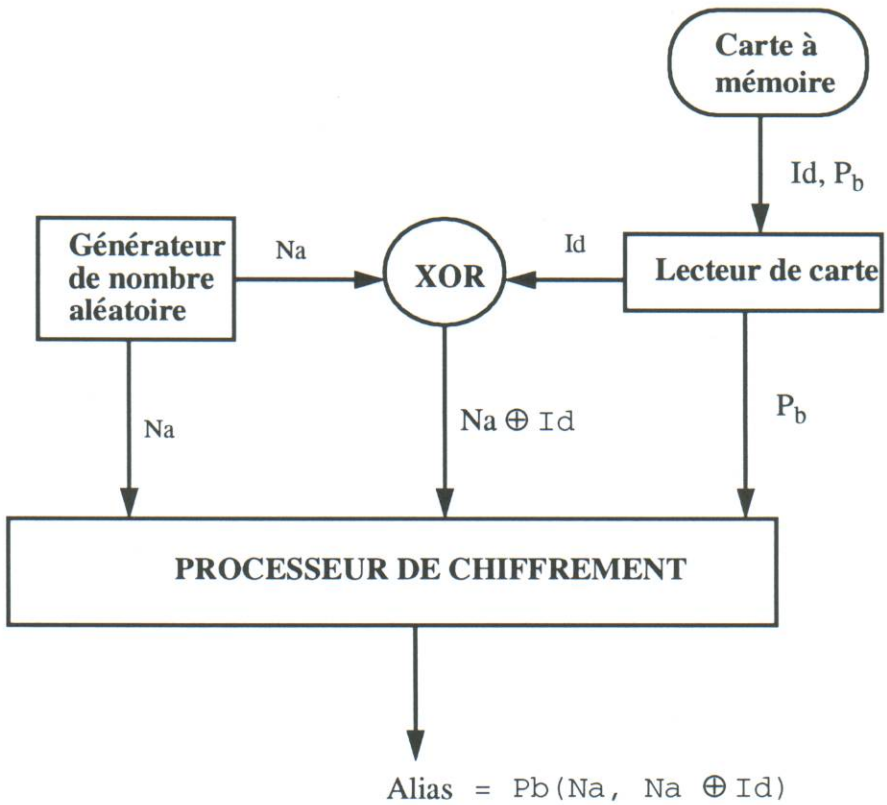
[13] W. Diffie, P.C.V. Oorschot, M.J. Wiener *Authentication and Authenticated Key Exchanges in Designs, Codes and Cryptography* Kluwer Academic Publishers, 1992.

Annexe: Shémas Synoptiques

Le type de chiffrement basé sur les clés publiques est très utilisé en France. Cette méthode de cryptage est parfaitement adaptée aux systèmes par carte à mémoire. Le couple chiffrement à clé publique et carte à mémoire est mis en oeuvre dans de nombreux systèmes de réseaux de haute sécurité.

De ce fait, l'implémentation industrielle de la méthode de calcul d'alias **peut** se faire grâce a l'utilisation d'une carte à mémoire et d'un module dédié au chiffrement.

1.0 Shéma Synoptique de l'Émetteur A.



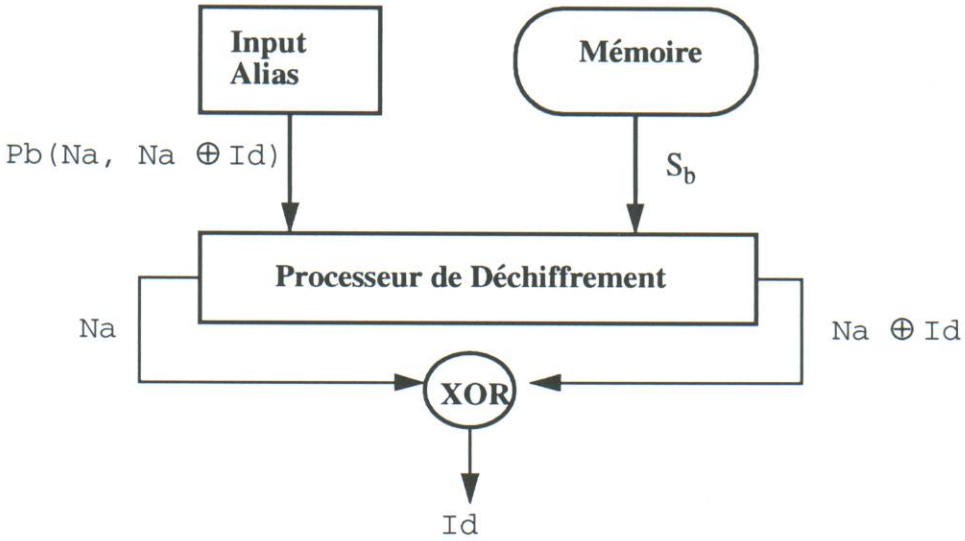
L'utilisation de la carte à mémoire n'est pas obligatoire. Une zone mémoire (ROM par exemple) peut aussi être utilisée.

1.1 Description

1. L'utilisateur introduit sa carte à mémoire dans le lecteur, qui lit son identification (Id) et la clé publique du destinataire (P_b) - l'autorité administrative de l'utilisateur dans le cas des réseaux mobiles.
2. Au niveau de l'équipement de l'utilisateur (ex: téléphone mobile), une générateur de nombre aléatoire génére le nombre Na.

3. Na et Id sont communiqués à l'opérateur logique XOR et donne en sortie Na ⊕ Id
4. Na, Na ⊕ Id et Pb sont ensuite fournis en entrée au processeur de chiffrement qui calcul l'alias pour l'utilisateur.

2.0 Shéma Synoptique du Récepteur.



Dans le cas de l'autentification des utilisateurs mobiles, l'entité réceptrice peut être une machine dédiée qui possède déjà une zone mémoire ou une base de donnée contenant sa clé secrète.

2.1 Description

1. Lors de la réception de l'alias, le récepteur récupère sa clé secrète et communique le tout au processeur de déchiffrement.
2. En sortie on obtient le nombre aléatoire Na et Na ⊕ Id. Ces 2 variables sont fournies en entrée à l'opérateur logique XOR
3. L'identité de l'utilisateur est obtenue en sortie du XOR.