Architecture de sécurité dans un réseau mesh multi sauts

Amin Ben Abdallah[α], Omar Cheikhrouhou[β], Maryline Laurent-Maknavicius[α], Hakima Chaouchi[α], Maher Ben Jemaa[β]

[α]CNRS Samovar UMR 5157, GET/INT/LOR, 9 rue Charles Fourier, 91011 Evry, France

(Amin.Ben_Abdallah@it-sudparis.eu, Maryline.Maknavicius@it-sudparis.eu, Hakima.Chaouchi@it-sudparis.eu)

[β]Unité de recherche ReDCAD, Ecole Nationale d'Ingénieurs de Sfax, BP W 3038 Sfax,Tunisie.

(Omar.Cheikhrouhou@isetsf.rnu.tn, Maher.BenJemaa@enis.rnu.tn)

RÉSUMÉ. *Les infrastructures TIC sont essentielles au développement d'un pays. Les technologies de réseaux sans fil offrent de nouvelles opportunités de développer très rapidement des infrastructures TIC dans le but d'un déploiement immédiat de services utiles à la communauté. Tout l'enjeu réside dans la construction d'un réseau extensible du point de vue de sa couverture radio et qui apporte l'accès au service comme l'accès à Internet au plus grand nombre, et ce sans négliger les attentes en matière de communication propres à chaque utilisateur.*

Dans ce contexte, nous proposons d'analyser un réseau mesh sans fil dont la couverture est étendue par un réseau ad hoc doté de capacités de routage ad hoc. Les enjeux de sécurité sont liés à l'architecture d'authentification et à la confidentialité des données. Plus précisément, le couplage de PANA avec la nouvelle méthode EAP-EHash est proposée, étudiée dans un contexte ad hoc muti-sauts et finalement analysée du point de vue de la sécurité.

ABSTRACT. *IT infrastructure is one of the important pillars of any country development. Emerging wireless technologies are offering new opportunities to develop very quickly IT infrastructures in order to deploy immediately important and useful community services. One big challenge is to provide a possibility to build a network that can grow in term of coverage to offer service access such as internet access for a large number of people with different needs from the network.*

In this context, we propose to analyse a wireless mesh network extended by an ad hoc network capable to grow in an ad hoc way by using ad hoc routing capabilities. The security challenges are related first to the authentication architecture, and second to the data confidentiality. More precisely, PANA combined with a new EAP-EHash method is proposed and discussed in a multi-hop mesh network, and a security analysis is provided.

MOTS-CLÉS : *réseau mesh, réseau ad hoc, authentification, EAP-EHash, PANA*

KEYWORDS: *mesh network, ad hoc network, authentication, EAP-EHash, PANA*

A. Ben Abdallah, O. Cheikhrouhou, M. Laurent-Maknavicius, H. Chaouchi, M. Ben Jemaa, " Architecture de sécurité dans un réseau mesh multi sauts ", 8th Symposium on Networks and Services GRES 2007, Hammamet, Tunisia, Novembre 2007.

1. Introduction aux réseaux mesh multi sauts et à la problématique de sécurité

Avec l'émergence des technologies sans fil comme les réseaux ad hoc, mesh, ou les réseaux d'accès sans fil hybrides (Chaouchi, avril 2007), le choix des architectures d'accès au réseau d'un opérateur est de plus en plus large. L'une des architectures très prometteuses est l'extension d'un réseau mesh par un réseau ad hoc. Elle permet à un opérateur d'étendre rapidement et à moindres coûts la couverture géographique de son réseau, et ce, afin d'offrir l'accès à différents services situés sur son réseau filaire ou Internet. Cette architecture est particulièrement soutenue par les opérateurs sans fil propriétaires du réseau mesh. Dans cet article, nous nous intéressons à coupler les réseaux ad hoc aux réseaux mesh, cette combinaison de technologies étant ci-après appelée « réseau mesh multi sauts ».

Un réseau mesh s'appuie sur des routeurs radio fixes ou des points d'accès (par exemple WiMAX) interconnectés de façon maillée (par des canaux radios). Le réseau ad hoc sert à étendre la couverture géographique du réseau mesh en apportant ses capacités de routage ad hoc. Les terminaux mobiles se servent du réseau ad hoc pour obtenir l'accès à l'Internet ou à certains serveurs gérés par l'opérateur du réseau mesh.

Dans cet environnement, nombreux sont les problèmes de sécurité. Ces derniers sont hérités des propriétés du médium de transmission lui-même et des réseaux sans infrastructure. Parmi les vulnérabilités liées aux réseaux sans fil, on peut citer les écoutes clandestines, les usurpations d'identité, les vols de session en cours mais aussi les faux points d'accès auxquels peuvent s'associer les mobiles afin de mieux espionner leurs communications. Le caractère sans infrastructure des réseaux mesh rend le routage particulièrement vulnérable aux nœuds ad hoc égoïstes refusant de participer au routage, à l'injection de fausses informations de routage ou de faux points d'accès conduisant à des dysfonctionnements, et d'une façon plus générale aux dénis de service (DoS).

Cet article adresse principalement les interactions de sécurité entre l'opérateur et les utilisateurs dans un environnement de réseaux mesh multi sauts. Il veille à introduire deux éléments de sécurité forte, ceci dans le double objectif de garantir une bonne qualité de connexion, et de renforcer la confiance des utilisateurs dans ce type de réseau d'accès en vue d'une commercialisation possible. Ces deux éléments sont les suivants :

– **l'authentification mutuelle** forte entre les mobiles des utilisateurs et le réseau de l'opérateur. Il est tout aussi important pour le réseau d'accès d'authentifier les mobiles avant de leur donner accès aux ressources du réseau, que pour les utilisateurs de vérifier qu'ils sont connectés à un réseau d'opérateur reconnu ;

– **la protection des échanges de données** à travers un canal radio en assurant la confidentialité de données, l'intégrité et l'authentification de la source d'information.

Les acronymes utiles sont donnés dans le tableau 1.

2. Travaux de recherche liés à cette même thématique

Les problèmes de sécurité soulevés à la section 1 sont traités dans la plupart des articles de recherche sous l'angle de la sécurité au sein d'un réseau ad hoc indépendant. Très peu s'intéressent à résoudre le problème de la sécurité des réseaux ad hoc hybrides grâce au support des protocoles AAA. Parmi ces derniers, (Zhang et al., 2002) introduit une architecture qui permet d'assurer les services AAA dans tout hotspot (WLAN) en se servant d'un compte unique pour chaque client (connu par son fournisseur d'accès comme FAI habituel), mais les détails protocolaires ne sont pas fournis.

(Moustafa et all, 2006) étend le protocole 802.11i à l'environnement ad hoc multi sauts et pour cela définit une infrastructure virtuelle dans laquelle chaque cluster élit un nœud principal chargé de relayer les messages d'authentification EAP-TLS pour les nœuds hors de portée du routeur d'accès. Ces nœuds implémentent la fonctionnalité de proxy RADIUS. Tout le problème vient de la mobilité des nœuds.

Enfin, (Chaouchi, May 2007) propose une nouvelle approche AAA permettant de sécuriser l'échange de services dans le réseau ad hoc et de générer des revenus. Cette approche délègue à certains nœuds ad hoc de confiance des sous-services AAA (Aaa, aAa, aaA). La description reste pour l'instant conceptuelle.

3. Proposition d'architecture de sécurité

Une première solution de sécurisation des réseaux mesh serait d'adapter IEEE 802.1X pour permettre aux mobiles de s'authentifier auprès du routeur d'accès mesh. Cependant, cette adaptation n'est pas immédiate puisque l'authentification par 802.1X est réalisée au niveau 2 et donc le routeur d'accès identifie un mobile par rapport à son adresse MAC. Ceci implique la très forte contrainte que le mobile soit toujours directement (sans intermédiaires) associé au routeur d'accès, et donc exclut l'utilisation directe de IEEE 802.1X à un contexte multi sauts.

AR – Access Router	MITM – Man-In-The-Middle
AS - Authentication Server	PANA - Protocol for carrying Authentication for Network Access
DoS Denial of Service	PAA - PANA Agent
EP – Enforcement Point	PaC – PANA Client
IKE – Internet Key Exchange	

Tableau 1. Acronymes utiles

3.1. *Entités fonctionnelles de PANA*

L'architecture de contrôle d'accès PANA définit quatre entités fonctionnelles (cf. Figure 2) :

– **Client PANA (PaC) :** Le PaC est hébergé dans le mobile et contacte l'agent d'authentification PAA lors de l'authentification du mobile.

– **Agent d'authentification PANA (PAA) :** Le PAA dans le réseau d'accès réalise l'authentification du PaC en consultant le serveur AS d'authentification. Le PAA communique ensuite le résultat de l'authentification à l'entité EP *(Enforcement Point)* qui bloque ou autorise alors les flux issus du mobile.

– **Enforcement Point (EP) :** L'EP contrôle physiquement les flux avant de leur donner accès au réseau. Dans le cas d'un nouveau nœud non encore authentifié, l'EP bloque les flux de données, mais autorise les flux utiles à la configuration et l'authentification du mobile (ex : PANA, DHCP, PAA discovery, etc.). Une fois le mobile authentifié avec succès, tous les flux de données issus de ce mobile sont autorisés par EP.

– **Serveur d'authentification (AS) :** L'AS est chargé d'authentifier à la demande du PAA le nœud requérant l'accès au réseau. Un protocole AAA tel que RADIUS ou Diameter est classiquement utilisé entre AS et PAA.

3.2. Méthode EAP-EHash

La méthode EAP-EHash (Encrypted-Hash) (Cheikhrouhou, oct. 2006) a été conçue pour les environnements sans fil et mobiles pour satisfaire les besoins d'authentification forte et de sécurité, tout en garantissant un traitement léger adapté aux terminaux de faibles capacités (mémoire, CPU, batteries, ...). Cette méthode allie la simplicité et la facilité de déploiement de EAP-MD5 et la robustesse de EAP-TLS. En effet, EAP-EHash suppose uniquement le partage initial d'un secret, tout comme EAP-MD5 ; elle se veut simple et rapide dans la mesure où elle se base sur l'utilisation de la cryptographie symétrique et d'un mécanisme défi/réponse. Elle assure l'authentification mutuelle particulièrement utile dans les réseaux sans fil ; elle est robuste aux attaques par dictionnaire puisque le défi et la réponse sont chiffrés et elle permet la dérivation d'une clé utile pour initier le protocole IKE (cf. section 3.3). Elle est flexible dans le choix des algorithmes mis en œuvre (3DES, DES, SHA1, MD5).

3.3. Description technique

Comme le montre la figure 1, lorsqu'un nouveau nœud rejoint le réseau ad hoc, il obtient tout d'abord du serveur DHCP une adresse IP appelée « adresse pre-PANA ». Il initie ensuite des échanges PANA pour découvrir le PAA localisé sur le

routeur d'accès AR. Notons que le routeur mesh (EP/AR) et les nœuds ad hoc intermédiaires autorisent certains flux IP d'un mobile non encore authentifié tels que DHCP, PANA Discovery et PANA. Une fois l'authentification PANA réussie, le client initie le protocole IKE avec l'EP dans le but d'établir une association de sécurité IPsec. Le tunnel IPsec ainsi construit assure la protection des données sur le lien radio et le contrôle d'accès aux ressources du réseau mesh.

Pour découvrir le PAA, le PaC diffuse un message PANA-PAA-Discovery. Par défaut, le premier PAA à lui répondre par un message PANA-Start-Request est choisi par le PaC pour démarrer une phase d'authentification.

Pendant les phases d'authentification et d'autorisation, PANA encapsule les messages EAP entre le PaC et le PAA (messages PANA-Start-Request et PANA-Start-Answer), et le PAA se charge de relayer les messages EAP à l'AS par exemple en implémentant l'encapsulation de EAP dans RADIUS (cf. Figure 2). Le choix de la méthode EAP retenue dans PANA dépend des capacités du PaC et des exigences de l'AS. Par exemple, dans un environnement sans fil, on privilégiera la méthode EAP-EHash et on pourra paramétrer cette méthode en fonction du niveau de sécurité souhaité (3DES, DES, SHA1, MD5 – cf. section 3.2

Une fois l'authentification terminée, le routeur d'accès mesh (EP/AR) limite l'accès de son réseau aux mobiles autorisés. Dans un environnement multi sauts, le contrôle d'accès ne peut se faire qu'au niveau des couches réseau, voire au dessus. La suite de protocoles IPsec est donc très bien adaptée aux réseaux mesh multi sauts. IPsec contrôle l'accès au réseau mesh en authentifiant l'origine des paquets, mais aussi IPsec protège les données en apportant par exemple le chiffrement par ESP *(Encapsulating Security Payload)* utile pour se prémunir des écoutes.

Au cours des échanges IKE, PaC et EP sont amenés à s'authentifier mutuellement et nous suggérons de configurer dynamiquement un secret partagé entre PaC et EP. Deux étapes sont pour cela nécessaires. Elles font suite à l'authentification EAP qui a précédemment abouti au partage d'une clé secrète (MSK – Master Session Key) entre PaC et AS (cf. section 3.2). L'AS envoie une première clé au PAA qui s'en sert d'une part pour protéger tous ses messages PANA ultérieurs avec PaC et d'autre part pour dériver une seconde clé secrète. Cette seconde clé (IKE-PSK) est alors transmise du PAA à EP. Notons que PaC est lui aussi capable de dériver IKE-PSK puisqu'il dispose de la clé MSK.

3.4. Analyse de sécurité de la solution

La solution reposant sur la suite de protocoles IPsec satisfait nécessairement les exigences de sécurité (Kaufman, 2005). Ci-dessous sont présentées quelques attaques potentielles avec des recommandations en vue d'en améliorer la sécurité :

– **Attaque par rejeu** : Le protocole PANA inclut un mécanisme de numéro de séquence qui, assure la détection et le rejet des messages dupliqués ou mal ordonnés. Ainsi la plupart des messages PANA usurpés aboutissent-ils à leur rejet, à

moins que l'usurpateur ne réussisse à se synchroniser sur le bon numéro de séquence.

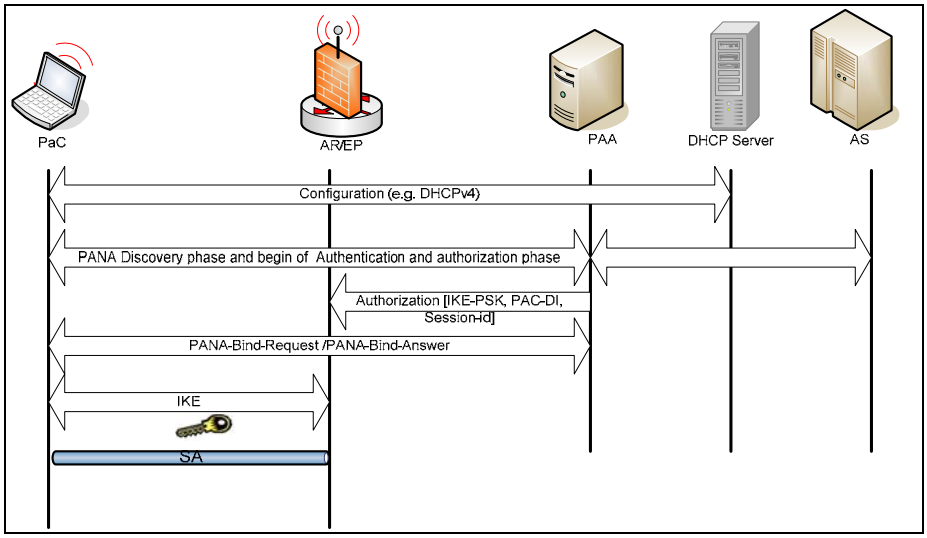

Figure 1. *Phases chronologiques (AR/EP et PAA sont séparés)*

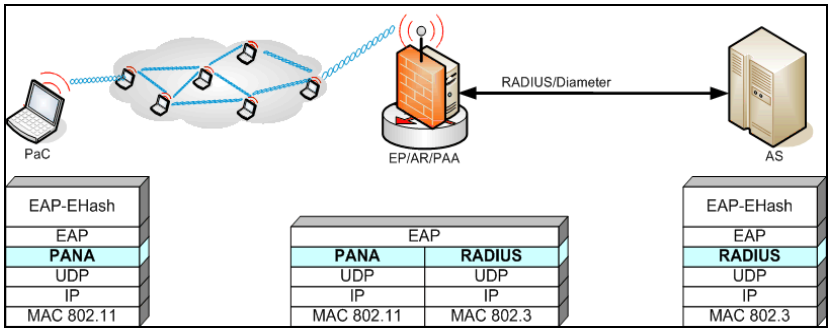

Figure 2. *Encapsulation des paquets EAP pendant l'authentification PANA (EP/AR et PAA sont colocalisés)*

– **Attaque DoS sur le PaC :** Un attaquant ne peut pas falsifier le résultat de l'authentification issu du PAA (envoyer « EAP failure » au lieu de « EAP success ») pour empêcher un nœud de joindre le réseau puisque ce message est sécurisé par l'association de sécurité PANA.

– **Perte d'intégrité des messages PANA :** L'association de sécurité PANA créée après la phase d'authentification assure l'intégrité des messages PANA et

protège aussi l'identifiant du PaC, ce qui empêche tout vol de service tel que décrit dans (Kaufman, 2005).

– **Usurpation de messages du PAA :** Pendant la phase de découverte, aucune relation de confiance n'est instaurée entre PaC et PAA. Il est donc facile pour un attaquant d'usurper un PAA voisin et d'émettre un message PANA-Start-Request demandant qu'un faible niveau de sécurité soit appliqué. Il en résultera le choix d'une méthode EAP de sécurité plus faible que prévue. Pour cette raison, il est recommandé de procéder à la négociation du niveau de sécurité (protection capability de PANA) une fois l'association de sécurité PANA établie, par exemple dans le message PANA-Bind-Request (cf. Figure 1).

– **Attaque DoS sur le PAA :** un attaquant peut saturer un PAA en l'inondant de message de découverte PANA-PAA-Discovery. Nous préconisons d'ajouter un cookie au message PANA-Start-Request émis par PAA et à retourner par le PaC dans le message PANA-Start-Answer. Un retour de ce même cookie indique au PAA qu'un PaC est actif à l'adresse indiquée et qu'il ne s'agit pas d'une adresse IP générée aléatoirement.

– **Attaque DoS sur DHCP :** Par la configuration d'une adresse IP par DHCP dans le PaC avant même son authentification EAP, on s'expose à des attaques DoS de pénurie d'adresses IP. Un attaquant peut émettre un grand nombre de requêtes DHCP aboutissant à la pénurie d'adresse et à l'impossibilité pour d'autres nœuds légitimes de se connecter.

– **Autres attaques possibles :** Les réseaux ad hoc et mesh sont très vulnérables aux écoutes passives, aux rejeux de messages, aux attaques MITM, DoS… De telles attaques sont effectivement simples de réalisation dans les réseaux ad hoc car aucun contrôle d'accès n'est aujourd'hui assuré au sein des réseaux ad hoc. Les écoutes sont facilitées, les nœuds relais pouvant simultanément relayer et espionner les paquets en transit. L'usurpation d'adresse IP est aussi facilitée car un nœud malicieux peut attendre le départ d'un autre nœud pour reprendre l'adresse IP valide ; cette attaque nécessite un MITM pour bloquer le message PANA-Termination-Request et maintenir la session active ; de plus elle restera limitée dans le temps puisque l'architecture PANA prévoit la réauthentification périodique des nœuds.

Les techniques de cryptographie demeurent efficaces dans les réseaux ad hoc pour se prémunir des écoutes, des pertes d'intégrité de messages, des usurpateurs… mais sont inefficaces contre les DoS dits « durs » provoqués par l'épuisement de batterie des nœuds ou des paquets volontairement non relayés. Les réseaux mesh souffrent d'attaques similaires, excepté le DoS dur car les routeurs mesh sont sous le contrôle d'un opérateur. Il en résulte que l'interconnexion de routeurs mesh doit être fortement sécurisée par des techniques de contrôle d'accès et de cryptographie.

4. Conclusions

En vue d'un déploiement rapide de services informatiques et de communications, les architectures mesh sans fil multi sauts sont prometteuses, mais nécessitent la mise en œuvre de mécanismes de sécurité forte, à savoir l'authentification mutuelle, le contrôle d'accès opéré par l'opérateur du réseau mesh, et la protection des échanges de données à travers le canal radio.

Le standard IEEE 802.1X pourrait évidemment être étendu pour assurer l'authentification des réseaux mesh multi sauts, mais une modification du standard n'est pas aisée en pratique. Dans cet article, une architecture de sécurité reposant sur EAP-EHash, PANA et IPsec est proposée, décrite brièvement et analysée. Cette architecture est prometteuse puisqu'elle est indépendante du medium de communication et qu'elle sera donc directement applicable aux réseaux 4G sans fil hétérogènes. Cependant, contrairement à 802.1X, PANA est sensible aux attaques DoS de pénurie d'adresses qui visent à consommer toutes les adresses IP disponibles dans le réseau de manière à rendre impossible l'accueil de nouveaux arrivants non authentifiés. Ce problème peut heureusement être résolu dans IPv4 avec l'allocation d'adresses privées temporaires et dans IPv6 grâce au large espace d'adressage disponible.

6. Références

Chaouchi H., Laurent-Maknavicius M., Ed, « La sécurité dans les réseaux sans fil et mobiles », Traité IC2, série Réseaux et télécoms, 3 volumes, Éd. Lavoisier, mai 2007, ISBN 978-2-7462-1697-6, ISBN 2 978-2-7462-1698-3, ISBN 3 978-2-7462-1699-0.

Chaouchi H., Laurent-Maknavicius M., « SAACCESS: Secured Ad hoc ACCess framework », article invité, International Conference on New Technologies, Mobility and Security NTMS'07, Paris, April-May 2007.

Cheikhrouhou O., Laurent-Maknavicius M., Ben Jemaa M., « Nouvelle méthode d'authentification EAP-EHash », *12ème Colloque Francophone sur l'Ingénierie des Protocoles CFIP'2006*, Tozeur, Tunisie, Octobre 2006.

Cheikhrouhou O., Laurent-Maknavicius M., « Sécurité des réseaux Mesh », Rapport de recherche 06001 LOR, 2006.

Forsberg D et al., « Protocol for Carrying Authentication and Network Access (PANA) », draft-ietf-pana-pana-15, May 2007.

Kaufman C., Ed., « Internet Key Exchange (IKEv2) Protocol », IETF RFC 4306, Dec. 2005.

Moustafa H., Bourdon G., Gourhant Y., « Authentication, Authorization and Accounting (AAA) in Hybrid Ad hoc Hotspot's Environments », WMASH'06, 2006, pp. 37-46.

Zhang, J., Li, J., Weinstein, S., Tu, N., « Virtual Operator based AAA in Wireless LAN Hotspots with Ad hoc Networking Support », *Mobile Computing and Communications Review*, Vol. 6, no 3, 2002, pp. 10-21.