Sécurité des réseaux mobiles autonomes

Mohamad ALJNIDI
TELECOM PARIS - Département INFRES
CNRS - LTCI (UMR 5141)
37/39, rue Dareau - 75014 Paris
Email: aljnidi@enst.fr

I. Introduction

Les réseaux mobiles introduisent d'autres formes de menaces de sécurité par rapport aux réseaux filaires traditionnels. Par exemple, la portée des connexions sans fil d'un terminal mobile augmente les possibilités d'espionnage passif. La mobilité, elle aussi, crée d'autres challenges de sécurité dans les réseaux mobiles par rapport aux réseaux sans fil statiques. On en cite par exemple l'identification d'un terminal mobile dans un réseau GSM, et surtout quand il passe d'un réseau à un autre. En outre, si le réseau mobile est sans infrastructure prédéfinie, comme les réseaux mobiles ad hoc par exemple, certains fonctions de sécurité commencent à s'avérer plus compliqués et à avoir plus de dimensions, comme le cas de l'authentification mutuelle entre terminaux mobiles. Avec les différents efforts faits pour trouver des solutions de sécurité pour les réseaux sans fil statiques et les réseaux mobiles à infrastructures prédéfinies, plusieurs recherches ont été lancées pour étudier la sécurité dans d'autres environnements plus sophistiquées comme ceux des réseaux ad hoc [3], des réseaux spontanés [2] et des réseaux domestiques et SOHO (Small Office/Home Office) [5]. La plupart de ces recherches se concentrent sur la topologie variante et les caractéristiques des noeuds et des technologies réseaux sous-jacentes. Nous croyons qu'il faut considérer en plus les conditions environnementales et fonctionnelles du réseau étudié. Par exemple, dans un réseau militaire, il faut étudier l'adaptation du système de sécurité aux changements potentiels non prévus des règles d'autorisation quand le rôle d'un noeud change instantanément lors d'une opération d'attaque dans un champ de bataille. Comme exemple de recherche pareil, une étude d'une conception générique de sécurité pour des réseaux ad hoc auto-organisables est donnée dans [7]. Nous allons dans la suite présenter notre recherche qui prend en compte de telles considérations. Nous commençons par expliquer nos objectifs, ensuite nous parlons des exigences de sécurité des réseaux étudiés, et enfin nous montrons rapidement une de nos solutions de sécurité.

II. Objectifs de recherche

Notre objectif est de proposer un ensemble de solutions de sécurité pour certains réseaux mobiles ne possédant pas des infrastructures prédéfinies. Les conditions environnementales et fonctionnelles de ces réseaux mobiles imposent que leurs systèmes et applications aient des propriétés d'informatique autonome (Autonomic Computing [1]). C'est pourquoi nous les appelons "Réseaux Mobiles Autonomes" (RMA dans la suite). Une définition intéressante et plus générique des réseaux autonomes est donnée dans [6] avec plus de détails des fonctionnements souhaités de tels réseaux.

On s'intéresse à des réseaux RMA évolutifs. Ils peuvent évoluer d'une façon ad hoc au niveau de la composition en noeuds, et au niveau de la topologie. Néanmoins, on suppose qu'un réseau parmi eux est caractérisé par un foyer ou les noeuds se réunissent provisoirement, et que des relations de dépendance existent entre les noeuds. La dépendance peut être due à un manque de capacités de calcul ou de stockage chez certains noeuds, ou à une hiérarchie préexistante. Nos scénarios d'implémentation s'appuient sur plusieurs champs d'application ayant des exigences différentes et présentant des difficultés diverses : les réseaux domestiques, les réseaux bureautiques (SOHO), les réseaux de services d'urgence et les réseaux militaires en champ de bataille. On a déjà trouvé des solutions pour les réseaux domestiques [4], qui présentent les scénarios les moins sophistiqués. L'existence d'un foyer et la dépendance entre noeuds facilitent la tâche de recherche de solutions de sécurité, car cela diminue les besoins de décentralisation. De ce fait, le rôle d'autorité peut être donné à certains noeuds sous une forme évolutive, et one peut dire qu'on est dans un cas de quasi-centralisation. Par contre, un autre type de challenge se montre ; Les réseaux mentionnés ci-haut ont des utilisateurs qui sont normalement non experts en informatique en général et surtout en sécurité. Certains réseaux parmi eux nécessitent des réactions rapides, et transparentes par rapport aux utilisateurs, en réponse aux changements d'environnement, et surtout les événnements de sécurité. Les réseaux que nous avons choisi pour étudier sont donc des réseaux RMA quasi-centralisés, dans lesquels il faut intégrer un Système Autonome de Sécurité (SAS dans la suite).

En effet, nous cherchons à définir les parties suivantes d'un SAS: 1) Une architecture de sécurité pour un Noeud Mobile Autonome (NMA dans la suite) - 2) Un modèle de confiance caractérisant la topologie variante du réseau - 3) Des protocoles d'authentification mutuelle entre noeuds - 4) Des processus de déploiement de politiques d'autorisation spécifiées avec des langages de haut niveau - 5) Des mécanismes d'établissement et de classification de relations sécurisées selon le modèle de confiance et les capacités de calcul et de stockage des noeuds impliqués - 6) Des processus d'autogestion sécurisée des évolutions du réseau - 7) Des applications d'administration autonome du SAS.

III. Exigences de sécurité

On peut représenter la fonctionnalité d'autonomie que nous visons dans nos solutions de sécurité par les exigences suivantes: 1) Un SAS doit pouvoir s'adapter aux changements d'environnement de sécurité. Par exemple, lors d'une attaque réussite d'usurpation d'identité d'un NMA, le processus d'autoadministration du SAS doit détecter l'attaque et lancer certaines fonctions autonomes pour d'abord contrer l'attaque et faire des réparations, ensuite pour modifier certaines configurations de certains mécanismes, et enfin pour optimiser certains services de sécurité - 2) Les mécanismes de sécurité du SAS doivent pouvoir se configurer. Par exemple, le mécanisme d'établissement de relations sécurisées redéfinit les paramètres à considérer après un spoofing détecté par le processus d'autoadministration du SAS - 3) Les services de sécurité du SAS doivent pouvoir s'optimiser. Par exemple, le service d'autorisation optimise sa politique de sécurité du bas niveau après la détection d'un canal caché par le processus d'autoadministration du SAS. Cette optimisation autonome est fait d'une façon transparente par rapport aux utilisateurs qui ont spécifié les politiques initiales de haut niveau - 4) Un RMA intégrant un SAS doit donc pouvoir se protéger contre des attaques internes ou externes ou lors d'un mal fonctionnement, et se réparer si jamais l'autoprotection n'empêcherait pas un certain problème d'avoir lieu.

IV. Modèle de sécurité

On va décrire ici le modèle de sécurité qu'on a déjà défini pour les réseaux domestiques [4] :

Le réseau domestique est, suivant ce modèle, un ensemble de communautés de dispositifs. Une relation mutuelle de confiance totale relie les dispositifs d'une seule communauté. Sachant que les dispositifs du réseau sont classifiés en Dispositifs Puissants (DP) et Dispositifs Simples (DS) selon leurs capacités de calcul et de stockage, un DP de la communauté est sélectionné pour être le NMA jouant le rôle de l'autorité principale de la communauté. Toutefois, n'importe quel autre DP de la communauté peut être désigné à un certain moment comme une autorité temporaire qu'on appelle autorité déléguée. La perte ou la panne d'une autorité est détectée automatiquement, et le SAS désigne un autre DP comme remplaçant (auto-réparation [1]). On suppose qu'il y a un DP au moins dans le réseau. Cela garantie qu'il y aura toujours un DP à utiliser comme autorité principale ou déléguée, peut-être pour plusieurs communautés, et surtout dans les cas d'urgence. La mission d'une autorité déléguée est de s'occuper temporairement des tâches de l'autorité principale de sa communauté pendant une période ou elle et d'autres dispositifs sont loin du foyer pour une durée supérieure à un maximum T prédéfini. T est la plus grande durée pour laquelle un dispositif est autorisé de s'éloigner du foyer. Autrement dit, on peut exporter un sous-réseau domestique avec une copie du SAS.

On définie 9 évolutions sécurisées du réseau ; 2 évolutions au niveau du modèle de confiance: intégration ou révocation d'une communauté. 3 évolutions au niveau infrastructure de gestion de sécurité: remplacement d'autorité, délégation d'autorité et annulation de délégation. Enfin, 4 évolutions au niveau composition en noeuds: insertion, suppression, bannissement et réinsertion. Une opération autonome très importante dans un tel type de réseaux, et qui représente une partie essentielle de notre recherche, est la coordination entre autorités. Par exemple, les autorités collaborent pendant et après une évolution sécurisée afin de synchroniser leurs données de gestion de sécurité (auto-optimisation [1]).

Des relations sécurisés de type RAA (Relation Autorité-Autorité) sont créées automatiquement après l'intégration d'une communauté, et des relations de type RAD (Relation Autorité-Dispositif) sont automatiquement créées après l'insertion ou la réinsertion d'un dispositif (auto-configuration [1]). La création et la distribution de clés et/ou de certificats se passent automatiquement immédiatement après l'établissement d'une RAA ou une RAD.

En outre, une relation sécurisée peut être créée entre n'importe quels deux dispositifs du réseau s'ils sont déjà dans le périmètre de sécurité grâce à une insertion ou une réinsertion, mêm s'ils n'appartiennent pas à la même communauté. Quand une telle relation est créée entre deux dispositifs, ils peuvent communiquer d'une façon sécurisée en utilisant leurs clés ou certificats et indépendamment de n'importe quel autre dispositif dans le réseau. Des protocoles d'authentifications, qui peuvent faire intervenir des autorités selon les capacités des dispositifs impliqués, sont nécessaires pour établir une relation de type RPP (relation entre deux DPs), de type RPS (relation entre un DP et un DS) ou de type RSS (relation entre deux DSs).

Des politiques d'autorisation sont échangées dans le cadre d'une RAA, et pendant l'établissement d'une relation sécurisée entre deux dispositifs de deux communautés différentes. On catégorise de telles relations sécurisées comme Relations à Basse Confiance (RBC). L'autre cas est celui d'une Relation à Haute Confiance (RHC) établie entre deux dispositifs de la même communauté, comme une RAD par exemple. Les DPs peuvent stocker des politiques d'autorisation, tandis qu'un DS demande des preuves certifiés de permissions à son interlocuteur pendant des communications dans le cadre d'une RBC.

References

[1] J.O.Kephart and D.M.Chess. The vision of autonomic computing. *Computer*, 36(1):41–52, 2003.

[2] L.M.Feeney, B.Ahlgren, and A.Westerlund. Spontaneous networking: an application-oriented approach to ad hoc networking. *Communications Magazine, IEEE*, 39(6):176–181, 2001.

[3] L.Zhou and Z.J.Haas. Securing ad hoc networks. *IEEE Network*, 1999.

[4] M.Aljnidi and J.Leneutre. Autonomic security for home networks. In *First International Workshop on Self-Organizing Systems, IWSOS 2006*, Passau, Germany, 2006.

[5] N.Prigent, C.Bidan, J-P.Andreaux, and O.Heen. Secure long term communities in ad hoc networks. In *First ACM workshop on Security of Ad Hoc and Sensor Networks*, Fairfax, Virginia, 2003.

[6] S.Schmid, M.Sifalakis, and D.Hutchison. Towards autonomic networks. In *First International IFIP TC6 Conference on Autonomic Networking, AN 2006*, Paris, France, 2006.

[7] T.Messerges, J.Curkier, T.Kevenaar, L.Puhl, R.Struik, and E.Callaway. A security design for a general purpose, self-organizing, multi-hop ad hoc wireless network. In *First ACM workshop on Security of Ad Hoc and Sensor Networks*, Fairfax, Virginia, 2003.