Gestion sécurisée de groupes de dispositifs dans les réseaux domestiques

Nicolas Prigent*† and Jean-Pierre Andreaux*

*Thomson R&D France, Rennes
{nicolas.prigent|jean-pierre.andreaux@thomson.net}
†Supelec, Rennes

Résumé Un réseau domestique est formé d'un ensemble de dispositifs (téléviseurs, enregistreurs numériques, ordinateurs, assistants numériques personnels, etc.) mis en réseau qui s'auto-configurent et interagissent de manière transparente pour l'utilisateur afin de lui offrir des services augmentés. Une première étape dans la sécurisation de ces réseaux consiste en la définition de leur frontière [3] . Il s'agit, en d'autres termes, de connaître de manière sécurisée les dispositifs qui y appartiennent. Dans cet article, nous proposons un mécanisme totalement distribué de gestion sécurisée de groupes dynamiques dédié aux réseaux domestiques. Ce mécanisme prend en compte les évolutions possibles d'un réseau domestique (ajout ou retrait de dispositifs par exemple), ainsi que le besoin de facilité d'utilisation inhérent à ce type de réseaux.

1 Introduction

Un réseau domestique [3] est formé d'un ensemble de dispositifs (téléviseurs, enregistreurs numériques, ordinateurs, assistants numériques personnels, etc.) mis en réseau qui s'auto-configurent et interagissent de manière transparente pour l'utilisateur afin de lui offrir des services augmentés. *UPnP* [9], *HAVi* [1] et *Rendezvous* [8] sont quelques propositions actuelles de standards de réseaux domestiques.

Les réseaux domestiques doivent être sécurisés si on souhaite leur large déploiement. En effet, il existe des mobiles et de véritables opportunités pour attaquer les réseaux domestiques. Comme nous l'avons montré dans [3], la première étape pour sécuriser un réseau domestique consiste à marquer sa frontière, c'est à dire à définir quels sont les dispositifs qui appartiennent à ce réseau.

En effet, la frontière des réseaux domestiques n'est pas clairement définie. L'utilisation de média hertziens, par nature partagés, la communication entre dispositifs au travers de l'Internet, la découverte et l'échange automatique de services entre dispositifs mis en présence [8,1,9] sont autant de facteurs qui rendent floue la frontière des réseaux domestiques : un dispositif de réseau domestique échangera *a priori* des services avec n'importe quel autre dispositif compatible et présent. Or, le fait qu'il ait la possibilité de communiquer et d'échanger des services avec un autre dispositif n'implique pas qu'il en ait le droit. Hors la mise

en place d'un mécanisme de sécurité spécifique, un dispositif ne peut décider de manière sécurisée si un autre dispositif appartient au même réseau domestique et a par conséquent le droit d'échanger des services avec lui. Ce mécanisme doit prendre en compte les évolutions possibles dans les réseaux domestiques (ajout et retrait de dispositifs), leur dynamicité et leur besoin de facilité d'utilisation.

En effet, contrairement aux réseaux d'entreprises, les réseaux domestiques ne peuvent bénéficier d'administrateurs compétents et disponibles. Leurs utilisateurs n'ont, pour la plupart, ni le temps, ni les connaissances pour gérer la sécurité de leur système. Pire, ils sont souvent considérés comme le maillon faible de la sécurité [6]. Mais s'ils doivent être écartés de la manipulation d'outils de sécurité complexes, les utilisateurs des réseaux domestiques ne peuvent cependant pas se soustraire à l'expression de la politique de sécurité. Dans le cadre de la définition de la frontière, ils sont les seuls à pouvoir décider quels dispositifs appartiennent au réseau domestique, et par conséquent les plus à même de l'exprimer. De ce fait, l'expression de la frontière doit se faire de la manière la plus simple et la plus discrète possible.

Dans cet article, nous présentons un mécanisme sécurisé, facile d'utilisation et totalement décentralisé de gestion de groupes dynamiques qui permet de résoudre le problème de la frontière dans les réseaux domestiques : chaque dispositif gère localement sa propre connaissance des dispositifs qui appartiennent au même réseau domestique que lui. Il maintient cette connaissance la plus à jour possible de manière sécurisée à partir des informations fournies par l'utilisateur et par les autres dispositifs de son réseau domestique. Dans la section 2, nous présentons les différentes opérations d'évolution d'un réseau domestique, qui doivent être prises en compte par un système de gestion de frontière. Dans la section 3, nous traitons des propriétés de topologie dynamique et de connectivité erratique des réseaux domestiques, qui ont imposé le choix d'un mécanisme totalement distribué. Notre proposition est décrite en section 4.

2 Évolutions de la frontière des réseaux domestiques

Les dispositifs d'un même réseau domestique, et donc à l'intérieur de la frontière, sont autorisés par la politique à communiquer et à échanger des services. Ils sont liés par une relation de confiance : un dispositif peut légitimement considérer que les dispositifs que son autorité (c'est à dire l'utilisateur) a déclarés appartenir au réseau domestique se comporteront en accord avec la politique. De plus, il peut avoir confiance en les informations fournies par les autres dispositifs de son réseau domestique.

Notons que tous les dispositifs d'un même réseau domestique n'appartiennent pas forcément à la même personne : chaque membre de la famille dispose de ses propres dispositifs sur lesquels il fait autorité. Néanmoins, tous les utilisateurs partagent le même intérêt dans le fait d'interconnecter leurs dispositifs de manière sécurisée. Un réseau domestique dispose donc de plusieurs autorités,

mais elles partagent toutes la même politique concernant l'appartenance d'un dispositif au réseau domestique. En d'autres termes, lorsqu'un des utilisateurs insère un dispositif dans le réseau domestique, tous les utilisateurs sont d'accord sur cette insertion.

La relation de confiance entre dispositifs d'un même réseau domestique est une relation à long terme : un dispositif entre *a priori* dans un réseau domestique pour une longue durée, et le quitte *a priori* définitivement (lorsqu'il tombe en panne, qu'il est vendu, perdu ou volé). D'un point de vue fonctionnel, il existe pour un réseau domestique quatre opérations d'évolution différentes :

- l'initialisation du réseau,
- l'insertion d'un dispositif,
- le retrait d'un dispositif,
- le bannissement d'un dispositif.

Chaque réseau domestique dispose d'un état initial, lorsque le premier dispositif est installé. Lors de l'initialisation, un dispositif est seul dans son réseau domestique. Le réseau évolue par la suite au gré des insertions et des retraits des dispositifs. La sécurité d'un réseau domestique doit être assurée dès son état initial, et maintenue au fil de ses évolutions.

Lorsqu'un dispositif est inséré dans un réseau domestique, il est capable d'identifier les autres dispositifs qui y appartiennent comme étant du même réseau domestique, et eux même sont capables de l'identifier comme faisant partie du leur.

Lorsqu'un dispositif est retiré du réseau domestique, par exemple parce qu'il est vendu ou donné, l'utilisateur peut y accéder physiquement pour y faire des modifications si nécessaire. Après qu'un dispositif ait été retiré du réseau, il ne doit plus reconnaître les autres dispositifs comme faisant partie de son propre réseau, et eux même ne doivent pas le reconnaître comme étant dans le leur.

Enfin, lorsqu'un dispositif est perdu ou volé, il existe un risque qu'un individu malveillant s'en serve pour accéder aux services offerts par les autres dispositifs du réseau domestique. Pour éviter cela, l'utilisateur doit pouvoir bannir du réseau domestique n'importe quel dispositif corrompu, c'est à dire informer de manière sécurisée les autres dispositifs du réseau domestique que le dispositif corrompu n'appartient plus à leur réseau domestique. L'utilisateur n'ayant *a priori* plus aucun contrôle sur le dispositif banni, aucune hypothèse ne peut être faite à son sujet. La seule propriété qui puisse être garantie est que les autres dispositifs du réseau domestique ne le considèrent plus comme y appartenant.

Remarquons enfin que pour des raisons de survie [5] du réseau domestique, n'importe quel dispositif doit pouvoir en être retiré ou banni sans que cela nuise à la pérennité du réseau. En d'autres termes, aucun dispositif ne doit lui être indispensable. Cette propriété est particulièrement importante dans les réseaux domestiques, qui sont constitués de dispositifs auxquels les utilisateurs ne prêtent pas forcément toute l'attention nécessaire.

3 Topologie dynamique et connectivité erratique

À l'instar des réseaux *ad hoc* [**?**], les réseaux domestiques sont topologiquement très dynamiques : la manière dont les dispositifs sont interconnectés varie au cours du temps, et certains dispositifs peuvent même être temporairement déconnectés. Par exemple, lorsqu'un utilisateur emporte avec lui ses dispositifs mobiles (ordinateurs portables, téléphones mobiles, assistants numériques personnels, lecteurs audios ou vidéos de poche, etc.), ceux-ci ne sont plus à même de communiquer avec les dispositifs qu'il laisse à son domicile (téléviseurs, ordinateurs de bureau, chaînes Hi-Fi, etc.). Par conséquent, il n'y a aucune certitude que deux dispositifs d'un même réseau domestique puissent communiquer à un instant donné. Aucun dispositif ne peut être considéré toujours présent, et aucun d'entre eux ne peut jouer le rôle de point de contrôle centralisé.

Nonobstant, un réseau domestique doit pouvoir fonctionner et évoluer de manière sécurisée même si un seul de ses dispositifs est présent, et ce quel que soit ce dispositif. Par exemple, lorsqu'un utilisateur achète un PDA et n'a sur lui que son téléphone mobile (qui, pour sa part, appartient déjà au réseau domestique), il doit pouvoir immédiatement interconnecter de manière sécurisée ces deux dispositifs pour qu'ils puissent s'échanger des services. En d'autres termes, l'utilisateur doit pouvoir insérer le PDA dans le réseau domestique en utilisant le téléphone.

De même, lorsqu'un réseau domestique se retrouve physiquement partitionné à un instant donné, aucune des partitions n'est capable de communiquer avec les autres, et chaque partition peut être amenée à évoluer indépendamment. Lorsque les dispositifs peuvent à nouveau communiquer ensemble, ils doivent avoir une connaissance cohérente du réseau.

4 Gestion distribuée de l'évolution sécurisée des réseaux domestiques

Pour marquer la frontière des réseaux domestiques tout en répondant aux contraintes de topologie dynamique et de connectivité erratique, le mécanisme que nous proposons est totalement distribué : il n'y a pas d'élément central (tel qu'un serveur central d'authentification ou une autorité centrale de certification), ni d'information secrète partagée (telle qu'une clé symétrique de réseau). Chaque dispositif se considère l'élément central et gère localement sa propre connaissance du réseau domestique.

4.1 Identité prouvable

Chaque dispositif du réseau domestique dispose d'une identité prouvable, qui lui permet d'être identifié et de s'authentifier auprès des autres dispositifs de son réseau. Nous appelons "identité prouvable" une identité qu'il est facile de vérifier, mais très difficile d'usurper, et qui permet la mise en place sécurisée de matériel cryptographique. Par exemple, la clé publique d'une paire de clés

publique / privée peut être utilisée comme identité prouvable : un dispositif prétendant être identifié par sa clé publique peut signer un *challenge* en utilisant sa clé privée, et est le seul à pouvoir déchiffrer un message qui a été chiffré avec sa clé publique. De plus, en se servant de leurs identités prouvables respectives, deux dispositifs peuvent créer un canal de communication sécurisé, leur permettant notamment de mettre en place des clés de session symétriques en utilisant un protocole de *key-agreement* tel que [2] par exemple. Ces clés de session point-a-point servent aux authentifications subséquentes et pour sécuriser les communications (authenticité et confidentialité) entre les deux dispositifs.

Citons aussi CAM [13] et SUCV [14] comme étant d'autres exemples de mécanismes d'identité prouvable, utilisés notamment dans le cadre de la mobilité IPv6, et pour lesquels à chaque dispositif est associé le résumé cryptographique de sa clé publique.

Du point de vue de la sécurité, chaque dispositif connaît les autres dispositifs de son réseau domestique uniquement par leurs identités prouvables. Par conséquent, si un dispositif change d'identité prouvable, il sera considéré par les autres dispositifs (qu'ils soient de son réseau domestique ou non) comme étant un tout autre dispositif.

4.2 Connaissance locale du réseau domestique

Chaque dispositif gère localement la connaissance qu'il a des dispositifs appartenant à son réseau domestique. Pour maintenir cette connaissance à jour, un dispositif se base en premier lieu sur les informations fournies par son utilisateur / administrateur, qui initie les changements dans le réseau (ajout, retrait ou bannissement d'un dispositif). Ces opérations seront présentées dans la section 4.3. Chaque dispositif échange aussi les informations qu'il possède avec les autres dispositifs de son réseau domestique, afin que tous en ait une vision cohérente. Ces échanges d'information seront présentés dans la section 4.4.

À l'échelle d'un réseau domestique donné, un dispositif, représenté par son identité prouvable, peut être :

- **Inconnu**, si ce dispositif n'appartient pas au réseau domestique et n'y a jamais appartenu.
- **Dedans**, si ce dispositif fait actuellement partie du réseau domestique.
- **Sorti**, si ce dispositif a autrefois fait partie du réseau domestique, mais n'y appartient plus, qu'il ait été retiré ou banni.

Pour un dispositif donné, ces trois états sont strictement ordonnés dans le temps : un dispositif est **Inconnu** jusqu'à ce qu'il soit inséré dans le réseau domestique et donc **Dedans**. Il reste **Dedans** jusqu'à ce qu'il soit **Sorti** du réseau par l'utilisateur. Nous considérons qu'un dispositif (c'est à dire une identité prouvable) **Sorti** du réseau domestique ne pourra pas y être ré-inséré avec la même identité prouvable : il devra d'abord générer une nouvelle identité prouvable, et être inséré sous cette identité.

Localement, un dispositif a peut connaître un autre dispositif b qui appartient ou a appartenu à son réseau domestique dans trois états différents :

– **Confiance Mutuelle**, noté MT pour l'anglais *Mutual Trust*
– **Confiance Unilatérale**, noté UT pour l'anglais *Unilateral trust*
– **Aucune Confiance**, noté DT pour l'anglais *DisTrust*

Un dispositif a connaît un autre dispositif b comme MT lorsque a sait que b appartient à son réseau domestique et que a sait que b sait que a appartient au réseau domestique de b. a et b ont déjà été mis en présence, et a possède un certificat signé par b qui prouve que b considère a comme étant dans son réseau domestique. Remarquons que, par symétrie, ceci est aussi vrai pour b.

a connaît b comme UT lorsque a sait que b appartient au réseau domestique de a, mais n'a jamais été mis en présence de b. Par conséquent, a ne sait pas si b sait que a appartient au réseau domestique de b, et devra peut être en apporter la preuve à b, comme décrit en section 4.4. Chaque dispositif qui, à l'instar de b, est connu par a comme étant UT, a été présenté à a par un dispositif que nous nommerons c que a connaît comme MT (cf. section 4.4). c, pour sa part, connaît b comme MT ou UT. Pour chaque dispositif connu comme UT par a, a dispose d'une chaîne de certificats, fournie par c, qui prouve que, par transitivité, b considère que a est dans son réseau domestique. a présentera cette chaîne de certificats à b lorsqu'ils seront mis en présence, pour lui prouver qu'ils appartiennent au même réseau domestique, et que tout les deux se passent l'un l'autre MT.

Enfin, a connaît b comme DT si a sait que b a appartenu au réseau domestique, mais n'y appartient plus. a n'acceptera plus de certificats émis par b comme étant des preuves d'appartenance au réseau domestique.

Ces états UT, MT et DT sont une représentation locale de l'état réel du dispositif concerné au sein du réseau domestique. Un dispositif a qui connaît b comme étant MT ou UT considère que b appartient à son réseau domestique, ce qui correspond à l'état réel **Dedans**. Par contre, tout dispositif inconnu ou connu comme étant DT n'est pas considéré comme appartenant au réseau domestique. DT est l'état local connu d'un dispositif **Sorti** du réseau. Par construction, les ensembles MT, UT et DT sont disjoints : a ne peut connaître b comme étant dans deux états à la fois.

Ces états locaux représentatifs de l'état réel d'un dispositif dans son réseau domestique sont eux aussi ordonnés. Un dispositif a qui connaît un autre dispositif b comme MT ne peut pas le faire passer à UT (ils ne peuvent pas s'être déjà rencontrés, puis ne s'être jamais rencontrés). Il ne peut pas non plus le faire passer de DT à UT ou MT, car, comme nous l'avons vu, un dispositif qui a été sorti du réseau domestique ne peut pas y être réinséré.

4.3 Évolution sécurisée du réseau domestique

L'évolution sécurisée du réseau domestique est initiée sur n'importe quel dispositif a appartenant à ce réseau par l'autorité locale de a : il ou elle informe a qu'un dispositif doit être inséré, retiré ou banni. C'est la seule et unique fois que l'utilisateur est impliqué au sujet de cette évolution : par la suite, l'information

d'évolution sera transmise par a aux autres dispositifs connus par a comme étant dans son réseau domestique (cf. section 4.4). Notons toutefois que rien n'empêche un utilisateur d'informer plusieurs dispositifs différents de la même évolution du réseau domestique.

Pour éviter qu'un attaquant n'insère de fausses informations sur un dispositif (insertion, bannissement ou retrait), l'utilisateur doit s'authentifier sur le dispositif qu'il a choisi pour initier l'évolution. Le mécanisme d'authentification utilisé sur chaque dispositif est strictement local à ce dispositif, qui peut donc utiliser celui qui lui est le plus approprié (code PIN, carte à puce, biométrie, etc.). Chaque dispositif peut en outre avoir un mécanisme d'authentification totalement différent de celui utilisé sur les autres dispositifs du réseau domestique. Ainsi, il n'existe aucune identité globale de l'utilisateur à l'échelle du réseau domestique, et notre proposition est réellement décentralisée. Du point de vue de la survie, cette solution offre un avantage important : si le mécanisme d'authentification d'un dispositif est compromis (par exemple, si un code PIN est découvert), cela n'a pas d'influence directe sur les autres dispositifs du réseau domestique, et la compromission ne s'étend pas au mécanismes d'authentifications utilisés sur ceux-ci.

Initialisation
Dans son état initial, un dispositif a est seul dans son propre réseau domestique. Pendant la phase d'initialisation, a génère une nouvelle identité prouvable, et marque celle-ci comme MT dans sa base de connaissance locale. Du point de vue de la sécurité, la connaissance qu'a a de son réseau domestique est valide : a ne considère comme étant dans son réseau domestique que les dispositifs qui y appartiennent réellement (ici, lui même), et ne considère pas comme n'y étant plus des dispositifs qui y appartiennent encore. Elle est aussi cohérente avec la connaissance des autres dispositifs qu'il sait appartenir à son réseau domestique (ici, lui même).

Remarquons que, sur demande et après authentification de l'utilisateur, un dispositif peut lancer une ré-initialisation : il efface de manière irréversible son identité prouvable précédente, en génère une nouvelle, vide sa base locale de connaissance, et insère sa nouvelle identité prouvable comme MT. Après une ré-initialisation, le dispositif est dans un état équivalent à celui dans lequel il se trouve après l'initialisation. Du point de vu des autres membres de son ancien réseau domestique, un dispositif ré-initialisé n'a plus rien à voir avec celui qu'il était avant la ré-initialisation, et est donc un dispositif totalement différent.

Insertion d'un dispositif
Du fait du parti que nous avons pris de proposer une solution totalement décentralisée, un dispositif a se basera uniquement sur sa connaissance locale pour décider si un autre dispositif b appartient ou non à son réseau domestique. De ce fait, pour que deux dispositifs a et b communiquent, chacun d'entre eux doit savoir que l'autre appartient à son réseau domestique, c'est à dire le connaître comme MT ou UT. Par conséquent, l'insertion doit être exprimée sur les deux

dispositifs : lorsqu'un utilisateur insère a dans le réseau domestique de b (en agissant sur b), il doit aussi agir sur a pour y insérer b, faute de quoi a ne communiquera pas avec b. Remarquons que lorsque a et b ont déjà d'autres dispositifs dans leurs réseaux domestiques respectifs avant de s'insérer l'un l'autre, l'opération d'insertion est en fait une fusion des deux réseaux domestiques, à l'issue de laquelle les deux réseaux domestiques de a et de b n'en forment plus qu'un.

L'insertion d'un dispositif a dans le réseau domestique d'un autre dispositif b consiste à insérer l'identité prouvable de a comme étant MT dans la base de connaissance de b. De la même manière, l'utilisateur doit insérer l'identité prouvable de b comme étant MT dans la base de connaissance de a.

Bien entendu, pour des raisons de facilité d'utilisation, on ne peut demander à l'utilisateur de rentrer la chaîne hexadécimale correspondant à la clé publique du dispositif à insérer, ni même son résumé cryptographique. La littérature propose plusieurs mécanismes pour résoudre ce problème. Stajano et Anderson ont par exemple proposé le *Resurrecting Duckling* [10,11] pour permettre l'appariement sécurisé de deux dispositifs : l'utilisateur place les deux dispositifs côte à côte, et leur demande de s'apparier. Ceux-ci échangent alors, en utilisant un canal supposé physiquement sûr, les clés qu'il utiliseront par la suite pour sécuriser leurs communications. Des améliorations ont par la suite été proposées [4,12], réduisant les hypothèses sur les propriétés du canal supposé sûr.

Lorsqu'un dispositif a insère un autre dispositif b dans son réseau domestique, il le marque comme MT. De plus, en utilisant son identité prouvable, a génère et délivre à b un certificat portant sur l'identité prouvable de b et qui prouve que b appartient au réseau domestique de a. L'usage qui sera fait de ce certificat sera vu plus avant.

Retrait

L'opération de retrait consiste à retirer un dispositif du réseau domestique alors qu'il est encore disponible et sous contrôle.

Tout d'abord, l'utilisateur s'authentifie sur le dispositif concerné b, et lui demande de quitter le réseau domestique. b informe alors les dispositifs de son réseau domestique qu'il peut contacter qu'il quitte le réseau domestique définitivement en envoyant à chacun un message de retrait authentifié avec la clé symétrique qu'il partage avec lui. Lors de la réception d'un message de retrait en provenance de b (qui appartient à son réseau domestique), un dispositif a vérifie tout d'abord l'authenticité de ce message. Puis a passe b à DT dans sa base de connaissance locale. Dès lors, a ne considère plus b comme appartenant à son réseau domestique.

Puis b se ré-initialise comme décrit précédemment. Ainsi, il ne considére plus les dispositifs du réseau domestique auquel il appartenait comme étant de son réseau domestique, et eux même ne peuvent plus accéder aux services qu'il offre.

Remarquons que si aucun dispositif n'est disponible lors du retrait de b, l'utilisateur devrait, même si cela n'est pas strictement nécessaire, informer plus tard l'un des dispositifs que b a quitté le réseau, en utilisant l'opération de

bannissement expliquée ci-après. Ainsi, si la partie privée de l'identité prouvable de b est cassée *a posteriori*, un attaquant ne pourra malgré tout pas s'insérer dans le réseau en usurpant l'identité de b.

Bannissement
Le bannissement d'un dispositif b a lieu lorsque b doit être retiré du réseau domestique mais que l'utilisateur ne peut pas y accéder. Cette opération a par conséquent lieu sur un autre dispositif a appartenant au réseau domestique dont b doit être banni. Pour bannir b, l'utilisateur s'authentifie sur a, et déclare simplement que b est désormais banni. a passe alors b de UT ou MT à DT.

Remarquons que le bannissement peut être utilisé à la place du retrait. Il faut alors en plus ré-initialiser manuellement le dispositif banni.

4.4 Gestion distribuée de la cohérence des connaissances locales

Il serait particulièrement contraignant pour l'utilisateur de devoir spécifier la politique sur chacun des dispositifs du réseau domestique, car il devrait informer chaque dispositif lors de d'une insertion, d'un retrait, ou d'un bannissement.

Pour accroître la facilité d'utilisation et assurer la cohérence des connaissances locales des dispositifs du réseau domestique, chaque dispositif échange des informations avec les autres dispositifs de son réseau domestique, lorsqu'ils sont disponibles. Comme nous l'avons déjà indiqué, tous les dispositifs d'un même réseau domestique sont liés par une relation à long terme et peuvent légitimement se faire confiance quant aux informations qu'ils s'échangent sur les insertions, retraits et bannissements survenus dans le réseau.

De ce fait, la relation de confiance entre dispositifs est transitive : si a considère que b appartient à son réseau domestique et si b considère que c appartient à son réseau domestique, alors a considère que c appartient à son réseau domestique. Cette transitivité est valide car tous les dispositifs d'un même réseau domestique sont soumis à la même politique et se basent donc sur les même critères pour insérer un dispositif dans le réseau domestique. Par conséquent, lorsque a insère b dans son réseau, cette insertion est valide pour tous les dispositifs considérant que a est dans leur réseau. De même, un dispositif faisant confiance aux certificats émis par a fera confiance à ceux émis par b.

Échange d'informations entre dispositifs se connaissant réciproquement comme MT
En plus de la transitivité de la confiance entre dispositifs, la gestion de cohérence des connaissances entre dispositifs d'un même réseau domestique repose sur :

- L'ordre strict des états d'un dispositif dans un réseau domestique.
- Le fait que toute information locale d'un dispositifs reçue de l'utilisateur est supposée vraie, car l'utilisateur a dû s'authentifier sur le dispositif.

De ce fait, quand deux dispositifs du même réseau domestique ont une connaissance différente au sujet d'un troisième (par exemple, l'un le connaît comme **Sorti** alors que l'autre le connaît comme **Dedans**), celui qui connaît l'état le

plus avancé (ici, **Sorti**) est forcément le plus à jour, puisque sa connaissance a été acquise légitimement et que les états sont ordonnés. Deux cas sont possible :

- le dispositif a reçu cette information de son utilisateur légitime.
- le dispositif a reçu cette information d'un autre dispositif du réseau domestique.

Dans le second cas, ce dispositif peut l'avoir lui même reçu d'un autre dispositif du réseau domestique, ou de son utilisateur. Par récurrence, cette information provient forcément d'un dispositif du réseau domestique qui l'a reçu d'une autorité légitime.

L'échange d'informations entre deux dispositifs a et b se connaissant l'un l'autre comme MT a lieu lorsque la connaissance de l'un d'entre eux est modifié pour une cause autre que l'échange d'informations entre eux, ou quand a et b sont mis en présence après avoir été déconnectés (la connaissance de chacun ayant pu évoluer). L'échange d'informations suit toujours le même algorithme, et toutes les communications sont protégées par les clés symétriques partagées par a et b .

Tout d'abord, a et b s'échangent les identités prouvables des dispositifs qu'ils connaissent comme DT. Chacun d'entre eux marque DT chaque dispositif c qu'il ne connaissait pas en tant que tel.

a et b comparent ensuite les dispositifs qu'ils connaissent MT. Bien que l'opération soit symétrique, nous présentons, dans un souci de clarté, l'obtention des informations de b par a. Pour chaque dispositif c connu MT par b mais pas par a, a insère c comme UT dans sa base de connaissance locale. Il stocke en même temps le certificat que b a émis lorsque b a inséré a comme MT (cette étape sera décrite un peu plus loin). Ainsi, lorsque a sera mis en présence de c, il pourra fournir à c le certificat en question. b connaissant c comme MT, cela signifie qu'ils se sont déjà rencontrés, et que c considère b comme MT. Par conséquent, il acceptera le certificat comme preuve que a appartient bien à son réseau domestique, et tout deux (a et c) pourront se passer l'un l'autre MT lorsqu'ils seront mis en présence, comme présenté plus loin.

Enfin, a et b comparent les informations qu'ils ont sur les dispositifs UT. Bien que l'opération soit ici aussi symétrique, nous présentons seulement l'obtention des informations de b par a. Pour chaque dispositif c connu UT par b mais pas par a, a insère c comme UT dans sa base de connaissance locale. Il obtient aussi la chaîne de certificats dont b dispose pour c et qui prouve, par transitivité de confiance que c considère b comme étant dans son réseau domestique. a y ajoute le certificat prouvant que b considère que a est dans son réseau domestique. De ce fait, a possède désormais une chaîne de certificats qu'il pourra remettre à c lorsqu'ils seront mis en présence, et qui prouve qu'ils appartiennent au même réseau domestique. Ainsi, tout deux (a et c) pourront se passer l'un l'autre MT.

Mise en présence d'un dispositif connu comme UT

Lorsqu'un dispositif a est mis en présence d'un autre dispositif b qu'il connaît comme UT, il va fournir à b la chaîne de certificats qui prouve que a appartient

au réseau domestique de b, ainsi qu'un certificat généré en utilisant son identité prouvable, et prouvant que a considère que b est dans son réseau domestique.

Lorsque b reçoit une chaîne de certificats, il vérifie que cette chaîne commence bien par un dispositif qu'il sait être dans son réseau domestique, puis il vérifie chacun des certificats. Si la chaîne de certificats fournie par a contient un certificat émis par un dispositif **Sorti** du réseau domestique (en d'autres termes, que b connaît comme DT), b ne doit pas insérer a comme MT, pour des raisons évidentes de sécurité.

Notons néanmoins qu'il se pourrait que a appartienne en fait réellement au réseau domestique. Par exemple, a peut avoir été inséré légitimement dans le réseau domestique par un dispositif e, qui a été banni avant que a ait été mis en présence d'autres dispositifs du réseau domestique. Pour sa part, a ne sait pas que e a été banni : il connaît encore e comme MT. Dans ce cas, a connaît les dispositifs du réseau domestique comme UT, mais est inconnu d'eux. L'utilisateur doit simplement insérer explicitement a dans le réseau domestique en utilisant un autre dispositif f qui y appartient encore. Lors de l'échange d'informations par a et f, a apprend de f que e est maintenant DT, et sa connaissance locale du réseau domestique est à jour.

Si tous les certificats de la chaîne reçue par b sont valides, b marque a comme MT, stocke le certificat reçu de a, et lui envoie un certificat généré en utilisant son identité prouvable, prouvant que a est dans le réseau domestique de b. Lorsque a reçoit ce certificat, il marque b comme MT. a et b établissent alors des clés symétriques pour sécuriser leurs communications subséquentes. Enfin, ils échangent des informations au sujet des dispositifs de leur réseau domestique, comme expliqué précédemment.

5 Conclusion

Nous avons présenté dans cet article un mécanisme sécurisé, facile d'utilisation et totalement distribué permettant de marquer la frontière d'un réseau domestique. Ce mécanisme offre les différentes opérations d'évolutions nécessaires dans les réseaux domestiques, tout en tenant compte de la topologie dynamique de ces réseaux et de l'interconnexion erratique des dispositifs qui les composent.

Le rôle de l'utilisateur se limite à exprimer la politique. Celle-ci peut être exprimée simplement sur n'importe quel dispositif du réseau domestique, et sa diffusion sécurisée est ensuite prise en charge par les dispositifs composant le réseau. Ainsi, tous les dispositifs d'un réseau domestique qui peuvent communiquer à un instant donné atteignent une vision cohérente et à jour de la frontière.

Il nous semble désormais intéressant de se pencher sur la gestion de dispositifs "invités" dans le réseau domestique, c'est à dire des dispositifs qui doivent être insérés temporairement, n'ont le droit d'accéder qu'à certains services, etc. De plus, maintenant que nous avons défini le périmètre de sécurité d'un réseau dont les dispositifs sont tous placés sous la même politique, il serait intéressant de considérer les politiques divergentes à l'intérieur d'un même réseau domes-

tique. Par exemple, certains services ou certaines données à l'intérieur du réseau peuvent être réservés à un sous-ensemble d'utilisateurs. Comment dans ce cas gérer l'expression de ces règles et assurer le contrôle d'accès ?

Références

1. HAVi Inc., *The HAVi Specification*, may 2001.
2. Whitfield Diffie, Paul C. van Oorschot and Michael J. Wiener, Authentication and Authenticated Key Exchange, *Design, Codes and Cryptography*, 1992.
3. Nicolas Prigent, Christophe Bidan, Olivier Heen et Alain Durand, Sécurité des réseaux domestiques : optimaux les grands remèdes ?, *Actes du Symposium sur la Sécurité des Technologies de l'Information et des Communications (SSTIC)*, 2003.
4. D. Balfanz, D. Smetters, P. Stewart et H. Wong, Talking to strangers : Authentication in adhoc wireless networks, *Proceedings of the ISOC Network and Distributed Systems Security Symposium*, Février 2002, `citeseer.nj.nec.com/balfanz02talking.html`
5. R. J. Ellison, D. A. Fisher, R. C. Linger, H. F. Lipson, T. A. Longstaff et N. R. Mead, Survivability : Protecting Your Critical Systems, *IEEE Internet Computing*, Vol. 3 number 6, 1999.
6. S. W. Smith, Humans in the Loop : Human-Computer Interaction and Security, *IEEE Security & Privacy*, Juin 2003, IEEE Press.
7. S. Corson et J. Macker, RFC 2501 : Mobile Ad hoc Networking (MANET) : Routing Protocol Performance Issues and Evaluation Considerations, janvier 1999.
8. Erik Guttman, Autoconfiguration for IP Networking : Enabling Local Communication, *IEEE Internet Computing*, mai 2001.
9. The UPnP Initiative, *The UPnP Forum*, `http://www.upnp.org/`
10. Frank Stajano, The Resurrecting Duckling – What Next ?, *Lecture Notes in Computer Science* Vol. 2133, pp 204–211, Springer 2001, `citeseer.nj.nec.com/stajano00resurrecting.html`
11. Frank Stajano and Ross Anderson, The Resurrecting Duckling : Security Issues for Ad-hoc Wireless Networks, In *7th International Workshop on Security Protocols*, pp 172–194, 1999, `citeseer.nj.nec.com/stajano99resurrecting.html`
12. L. Feeney, B. Ahlgren et A. Westerlund, Spontaneous networking : an application-oriented approach to ad hoc networking, *IEEE Communications Magazine*, juin 2001, `citeseer.nj.nec.com/feeney01spontaneous.html`
13. G. O'Shea et M. Rose, Child-proof authentication for MIPv6 (CAM), *ACM SIGCOMM Computer Communication Review*, Vol. 31, number 2, 2001, pp 4–8, `http://doi.acm.org/10.1145/505666.505668`, ACM Press.
14. C. Montenegro et C. Castelluccia, Statistically Unique and Cryptographically Verifiable (SUCV), *NDSS'02*, Février 2002.