# Sécurité des réseaux domestiques : optimaux les grands remèdes ?

Nicolas Prigent[1], Christophe Bidan[2], Olivier Heen[1], and Alain Durand[1]

[1] *Thomson R&I France, Rennes
{nicolas.prigent|olivier.heen|alain.durand}@thomson.net
[2] **Supélec, Rennes
christophe.bidan@supelec.fr

**Résumé** Au carrefour de l'informatique traditionnelle et du *consumer electronics*, les réseaux domestiques promettent de nouveaux usages et de nouveaux horizons pour le grand public. Ils ne pourront tenir ces promesses si leur sécurité n'est pas assurée. Cet article montre en quoi les solutions initialement élaborées pour un environnement professionnel offrent peu de sécurité en environnement domestique ou contraignent trop le réseau et son utilisateur. Puis il aborde quelques pistes récentes vers une sécurisation spécifique.

## 1 Réseaux domestiques

De plus en plus accessibles, de moins en moins coûteux, les équipements et réseaux informatiques se sont largement démocratisés : selon Médiamétrie [9], 38% des foyers français sont équipés d'un ordinateur et 25% disposent d'une connexion à l'Internet.

Les réseaux domestiques, au carrefour de l'informatique et de l'électronique grand public, sont la prochaine évolution attendue.

Un réseau domestique consiste en l'interconnexion d'équipements domestiques hétérogènes (ordinateurs, téléviseurs, assistants numériques personnels, matériel Hi-Fi, appareils électroménagers, etc.) dans le but de proposer des services augmentés aux utilisateurs. Cette interconnexion permet par exemple d'accéder aux contenus ou services multimédias présents sur le réseau depuis tout équipement en faisant partie et doté de capacités suffisantes. L'accès peut se faire soit depuis l'intérieur du domicile (sur des média filaires ou non), soit depuis l'extérieur via l'Internet. La synchronisation automatique entre les équipements domestiques fixes et les réseaux personnels (*PAN, Personnal Area Network*) de chacun des habitants est un autre exemple de service augmenté offert par les réseaux domestiques.

### 1.1 Origines

Les réseaux domestiques trouvent leur origine dans le projet *Ubiquitous Computing* (informatique omniprésente) mené par Marc Weizer au Xerox Parc à la fin des années 80.

Ce projet s'appuie sur le constat suivant : chaque fois qu'une technologie devient primordiale, son utilisation devient transparente pour l'utilisateur[3]. Weizer [11] affirme que, pour devenir omniprésente et véritablement utile, l'informatique doit devenir transparente : les ordinateurs doivent être enfouis dans les objets du quotidien, communiquer, se configurer et fournir des services sans que l'utilisateur s'en aperçoive. Les ParcTabs [8] sont un exemple historique parmi tant d'autres [1] de mise en oeuvre de l'*Ubiquitous Computing*.

Les réseaux domestiques sont une forme particulière d'*Ubiquitous Computing* se focalisant sur les lieux de résidence et leurs habitants. Plusieurs visions coexistent actuellement. Elles sont basées soit sur des technologies informatiques, soit sur des technologies issues de l'électronique grand public.

### 1.2 Technologies actuelles

Une première approche envisage les réseaux domestiques comme une évolution des LANs autour d'un élément fédérateur : l'ordinateur domestique. C'est l'approche de solutions telles que *Universal Plug'n Play (UPnP)* et *Rendezvous*. Elles permettent de gérer automatiquement l'installation et la configuration de nouveaux appareils fonctionnant sur IP et celle des services associés (partage de fichiers, d'imprimantes, de connexions à l'Internet) de manière transparente pour l'utilisateur.

Une autre approche est plutôt héritée de l'électronique grand public [7] : Bell et Gemmell prédisent l'avènement d'une nouvelle manière de gérer l'interaction des différents équipements audiovisuels chez le particulier. Les dispositifs sont tous connectés entre eux par un bus numérique (typiquement un bus IEEE 1394) au travers duquel ils échangent contenus, accès et traitements. Via ce bus, les téléviseurs, enregistreurs numériques, chaînes Hi-Fi, etc. s'interconnectent facilement et adaptent conjointement leur configuration. La technologie HAVi (*Home Audio-Video Interoperability*) par exemple permet ce type d'interactions.

Les deux approches ne s'excluent pas mutuellement, et certains efforts de recherche s'orientent aujourd'hui vers des approches hybrides.

### 1.3 Caractéristiques

Pour remporter l'adhésion du grand public et rendre pleinement les services attendus, les réseaux domestiques doivent respecter un certain nombre de contraintes. En particulier, l'accent doit porter sur l'automatisation des procédures d'installation et de configuration complexes permettant aux dispositifs de collaborer. A titre d'exemple, on peut citer l'obtention d'une adresse valide sur le réseau, la déclaration de la disponibilité sur un bus ou dans une cellule hertzienne, l'annonce des services proposés, etc.

Plus globalement, les réseaux domestiques doivent :

[3] L'écriture, par exemple, est devenue "transparente" pour une grande partie de la population : nous lisons chaque jour énormément de messages (publicités, marques, panneaux) sans nous en rendre compte.

– Permettre une grande hétérogénéité.
– Tolérer des comportements très dynamiques.
– Fonctionner en l'absence d'administrateur.

### 1.3.1 Hétérogénéité

Alors que les réseaux informatiques classiques sont formés de composants similaires (principalement des ordinateurs) comparables en termes de puissance, de stockage, de mémoire, de bande passante, etc., les réseaux domestiques sont composés de dispositifs hétérogènes. Ils comportent aussi bien du matériel Hi-Fi que des dispositifs mobiles et du matériel informatique. Cette hétérogénéité a des conséquences sur les réseaux domestiques : à titre d'exemple, on ne peut demander au petit processeur placé dans un lecteur MP3 de réaliser les mêmes opérations qu'un ordinateur de bureau. D'autres dispositifs tels que les assistants numériques personnels présentent de meilleures capacités de traitement mais souffrent d'un stockage limité.

Une autre différence porte sur l'hétérogénéité des moyens de communication. Grâce à IP, les réseaux informatiques classiques sont extrêmement homogènes : une technologie de communication physique est choisie, les appareils sont équipés de cartes réseau en conséquence, et l'administrateur effectue les tâches de configuration. À l'inverse, les moyens de communication utilisés par les réseaux domestiques sont hétérogènes dans la mesure où les appareils domestiques sont fournis tels quels : un enregistreur numérique n'utilise pas la même connectique qu'un assistant numérique personnel, et encore moins les mêmes protocoles de communication.

### 1.3.2 Dynamicité

Les réseaux domestiques sont aussi particulièrement dynamiques, et ce à plusieurs titres.

Tout d'abord, un réseau domestique donné évolue dans le temps en fonction des dispositifs qui le constituent. Il commence avec le premier appareil communicant que l'utilisateur achète et évolue au gré des achats, ventes, pannes, pertes, etc.

Un réseau domestique est aussi physiquement dynamique. Les éléments qui le composent ne sont pas interconnectés en permanence : les appareils peuvent être mobiles, sous tension ou non ; les canaux de communication peuvent être bruités ou temporairement indisponibles.

Plus généralement, aucune supposition ne peut être faite sur la disponibilité d'un dispositif dans le réseau à un instant donné. Par conséquent, aucun constituant du réseau domestique ne doit être indispensable au fonctionnement global. C'est une grande différence par rapport aux réseaux informatiques classiques, pour lesquels on peut raisonnablement estimer que certains des dispositifs sont disponibles en permanence (solutions haute disponibilité, locaux sécurisés, courant secouru, supervision).

### 1.3.3 Absence d'administrateur

Enfin, les utilisateurs des réseaux domestiques sont très différents de ceux des réseaux informatiques. L'utilisateur d'un réseau informatique a souvent bénéficié d'une formation adaptée. Les appareils sont pour lui des outils de travail et il est prêt à suivre quelques procédures fastidieuses pour les maintenir en fonction. Pour les opérations complexes, un administrateur possède le niveau d'expertise adapté et des ressources dédiées.

*A contrario*, l'utilisateur d'un réseau domestique interagit avec des objets du quotidien. Il n'a généralement bénéficié d'aucune formation particulière et peut tout ignorer du fonctionnement d'un réseau. Quand bien même il disposerait de compétences adaptées, il ne consacrera probablement pas les ressources nécessaires pour configurer, administrer, et superviser régulièrement le sien.

Les réseaux domestiques présentent donc des différences essentielles par rapport aux réseaux informatiques traditionnels, résumées dans le tableau ci-dessous.

| **Réseaux informatiques** | **Réseaux domestiques** |
|---|---|
| Dispositifs similaires. | Dispositifs hétérogènes. |
| Moyens de communication rationalisés. | Moyens de communication hétérogènes. |
| Évolutions du réseau rares et maîtrisées. | Évolutions du réseau fréquentes et non-rationnelles. |
| Interconnexion supposée permanente des dispositifs. | Interconnexion erratique des dispositifs. |
| Utilisateurs formés et actifs. | Utilisateurs non-formés et passifs. |
| Administrateurs. | Pas d'administrateur. |

**Tab. 1.** Différences entre réseaux informatiques et réseaux domestiques .

En quoi ces différences influent-elles sur les besoins et les modèles de sécurité ? Des solutions de sécurisation éprouvées pour les réseaux informatiques classiques sont-elles toujours valides en environnement domestique ?

## 2 Besoins de sécurité

Les réseaux domestiques seront attaqués s'ils recèlent de la valeur (contenus, ressources, usages), et ce avec succès s'ils présentent des faiblesses exploitables.

### 2.1 Menaces

Aujourd'hui, il existe déjà des menaces contre les ordinateurs personnels connectés à l'Internet, qui peuvent être considérés comme des réseaux domes-

tiques limités. Les attaques auparavant uniquement portées contre les sociétés et les centres militaires ou universitaires frappent maintenant les particuliers [17].

Les mobiles pour attaquer de tels équipements domestiques sont nombreux :

- Le jeu : de nombreux attaquants sont simplement des passionnés d'informatique souhaitant étrenner leurs connaissances des réseaux et des systèmes [2].
- Le vandalisme.
- Le vol des contenus (données, films, musiques, images, etc.) de l'utilisateur.
- L'atteinte à la vie privée de l'utilisateur, par exemple en accédant à ses e-mails, ou en surveillant le trafic IP arrivant à son ordinateur.
- Le vol de ressources (bande passante, CPU ou disque) : certains pirates déposent par exemple des données, légales ou non, sur les ordinateurs qu'ils ont attaqués, et les rendent accessibles *via* un serveur `FTP` ou `HTTP`.
- Le rebond vers d'autres cibles plus importantes : une fois que l'attaquant a pris le contrôle d'une machine, il peut s'en servir pour en attaquer d'autres, réduisant ainsi le risque d'être découvert.
- L'utilisation dans le cadre d'une attaque par refus de service distribué (*DDoS, Distributed Denial of Service*).

Ces mobiles sont toujours valides, et sont probablement accentués dans le cas des réseaux domestiques complets, notamment dans le cas de l'atteinte à la vie privée : en permettant aux utilisateurs de gérer l'intégralité de leurs informations personnelles (e-mails, photos et films personnels, données bancaires et commerciales, etc.), les réseaux domestiques seront profondément liés à leurs vies quotidiennes. Ils seront donc une cible de choix pour quiconque voudra porter atteinte à la vie privée de leurs propriétaires, réaliser des opérations bancaires à leurs dépens, etc.

Si, en plus de mobiles, un attaquant dispose d'opportunités pour attaquer les réseaux domestiques, ceux-ci seront effectivement attaqués. La seule présence d'ordinateurs dans les réseaux domestiques rend des attaques connues techniquement possibles. Les attaques contre les ordinateurs domestiques sont actuellement très courantes, et d'autant plus faciles que ces ordinateurs utilisent majoritairement la même architecture et le même système d'exploitation. En utilisant des outils d'attaque automatisés exploitant des failles connues des logiciels ou des systèmes d'exploitation les plus courants, l'attaque d'une machine peut se faire d'un simple clic.

En outre, les ordinateurs domestiques bénéficiant rarement d'un administrateur compétent, ils sont en général moins bien protégés que leurs homologues professionnels : leurs utilisateurs n'appliquent que très rarement les mises à jour de sécurité. Ainsi, des vulnérabilités pour lesquelles il existe pourtant des correctifs perdurent [5]. À cela s'ajoute l'installation chaotique d'applications éventuellement corrompues par des logiciels malicieux (virus et autres chevaux de Troie).

Les ordinateurs personnels ne sont pas les seules cibles à considérer. En effet, tout équipement communiquant peut faire l'objet d'attaques, à l'instar de celles réalisées contre des dispositifs fonctionnant sous des systèmes d'exploitation embarqués.

Lors de la conférence Black-Hat 2002, Davis et Higbee [6] ont présenté une attaque utilisant des dispositifs électroniques grand public disposant d'interfaces Ethernet ; Ils ont transformé une console DreamCast de SEGA et un assistant personnel I-Paq de Compaq en analyseurs de réseau en se servant de portages spécifiques de Linux[4], puis les ont utilisés pour contourner un *firewall*.

Plus récemment, une attaque portant contre le Nokia 6210 a été publiée [3]. Ce téléphone mobile offre un service de gestion de cartes de visite électroniques *vCard*, qui peuvent notamment être échangées par SMS. En envoyant une *vCard* au format incorrect par SMS, un attaquant peut provoquer un dépassement de tampon [13], causant un refus de service sur le téléphone.

Si ces attaques contre des dispositifs particuliers restent pour l'instant l'apanage de spécialistes, il est très probable que des outils d'attaque automatisés existeront contre l'ensemble des dispositifs lorsque les réseaux domestiques seront largement déployés.

Les éléments portatifs présentent également un risque important de perte, de vol, ou de modification à l'insu de la victime. Outre le préjudice immédiat en cas de vol, il y a une augmentation du risque d'attaque avec privilèges si l'appareil n'est pas révoqué rapidement.

Il existe donc simultanément des mobiles et des opportunités d'attaques contre les réseaux domestiques : toutes les conditions sont réunies pour qu'ils soient attaqués avec succès. Seule la mise en œuvre de mesures de prévention spécifiques permettra de réduire le risque à un niveau acceptable pour les utilisateurs.

### 2.2 Frontière

Une première étape vers la sécurisation des réseaux domestiques consiste en la définition et la mise en place d'une frontière. La frontière d'un réseau domestique marque la séparation entre les équipements placés sous la responsabilité de l'utilisateur et le monde extérieur. Son implémentation doit présenter les services de sécurité suivants :

- Authentification des dispositifs : les dispositifs situés à l'intérieur de la frontière peuvent s'authentifier comme tels.
- Confidentialité des communications : seuls les éléments situés à l'intérieur de la frontière ont accès aux messages circulant dans le réseau domestique.
- Authenticité des communications : les dispositifs du réseau domestique peuvent vérifier si un message provient bien d'un dispositif situé à l'intérieur de la frontière.

[4] La Dreamcast se base sur un processeur Hitachi SH4, et l'I-Paq sur un StrongARM. Un portage de Linux existe pour chacune de ces architectures.

Le problème à résoudre réside dans l'établissement d'une frontière offrant ces services et maintenable au gré des évolutions du réseau domestique, en accord avec les caractéristiques d'hétérogénéité, de dynamicité et d'absence d'administration.

En premier lieu, la frontière doit être non-ambiguë. Un utilisateur connaît les dispositifs appartenant au réseau domestique. La frontière doit refléter cette appartenance : deux dispositifs mis en présence doivent pouvoir déterminer avec certitude s'ils appartiennent au même réseau domestique.

La frontière doit aussi suivre l'évolution du réseau domestique. Un réseau domestique commençant par le premier appareil communiquant acquis par l'utilisateur, la frontière doit être initialisable. Elle doit aussi être incrémentale et décrémentale : un utilisateur peut ajouter un élément au réseau domestique, comme il peut aussi exclure un dispositif d'un réseau, éventuellement en l'absence de ce dispositif (révocation en cas de vol).

Enfin, la frontière doit être tolérante au fractionnement, pour supporter la dynamicité physique du réseau domestique. En particulier, deux partitions d'un même réseau domestique peuvent évoluer séparément, et doivent pouvoir synchroniser leurs évolutions respectives (par exemple l'acquisition d'un nouveau dispositif par l'une des parties) lorsqu'elles seront de nouveau réunies.

## 3 Insuffisance des solutions traditionnelles

Une approche pour mettre en œuvre la frontière et sécuriser les réseaux domestiques consiste à se servir des solutions existant dans les réseaux informatiques. Actuellement, trois types de solutions y sont utilisés :

1. Le cloisonnement.
2. Les solutions centralisées.
3. La protection des communications.

### 3.1 Cloisonnement

Les solutions de cloisonnement se servent de l'organisation physique du réseau pour en assurer la sécurité. Pendant longtemps, ces solutions étaient les plus répandues pour sécuriser les réseaux informatiques : seuls les ordinateurs physiquement connectés au médium étaient considérés comme faisant partie du réseau, à l'exclusion de tous les autres. Dans la mesure où seuls des utilisateurs légitimes pouvaient accéder physiquement au réseau, celui-ci était réputé sûr. Plus tard, lorsque ces réseaux ont été interconnectés, la mise en place d'un *firewall* permettait de délimiter, au moins partiellement, la frontière du réseau local vis-à-vis de l'Internet.

La situation est différente dans les réseaux domestiques : la possibilité d'accéder au médium ne suffit pas à décider de l'appartenance au réseau, du fait notamment

de l'utilisation éventuelle de réseaux sans fil[5]. De plus, la très grande dynamicité physique des réseaux domestiques, ainsi que la possibilité d'usages multi-sites (correspondant au besoin de relier les résidences principale et secondaire notamment) réduisent grandement l'intérêt d'un *firewall* classique.

### 3.2 Solutions centralisées

Une autre manière de définir l'appartenance à un groupe dans les réseaux informatiques repose sur des solutions centralisées : un serveur en ligne est capable d'authentifier les dispositifs autorisés, à l'image de Kerberos.

Ces solutions sont difficilement envisageables pour les réseaux domestiques. Du fait de leur dynamicité, on ne peut pas supposer qu'un dispositif est joignable en permanence : certains dispositifs pouvant se retrouver momentanément déconnectés (par exemple, un assistant numérique personnel, un ordinateur portable, un téléphone mobile, etc.), l'utilisation d'un dispositif central de sécurité les empêcherait de fonctionner.

Une alternative consisterait à utiliser un serveur centralisé n'ayant pas à être joignable en permanence car il serait capable de certifier les dispositifs en se servant d'algorithmes de cryptographie asymétrique. Un dispositif appartenant au réseau domestique disposerait donc d'un certificat signé par ce serveur, ainsi que de la clé publique de celui-ci, lui permettant de vérifier les certificats.

Cependant, si cette alternative permet l'authentification mutuelle de deux dispositifs même lorsque ceux-ci ne peuvent communiquer avec le serveur central, elle requiert malgré tout que celui-ci soit présent lorsqu'il s'agit de faire évoluer le réseau, et n'est donc pas totalement adaptée.

### 3.3 Protection des communications

Construire un Réseau Privé Virtuel (*Virtual Private Network* ou *VPN*) entre les dispositifs du réseau domestique pourrait être une autre manière de mettre en place la frontière d'un réseau domestique. Un VPN simule un réseau privé en utilisant la cryptographie pour sécuriser les communications : les messages qui circulent entre les membres du VPN sont chiffrés et authentifiés. IPSec est aujourd'hui le protocole le plus utilisé pour la mise en place de VPNs sur l'Internet. D'autres protocoles sont aussi utilisés : TLS/SSL (*Transport Layer Security / Secure Socket Layer*) est une proposition générique de sécurité au niveau Socket, alors que SSH (*Secure Shell*) est dédié à la sécurisation des protocoles d'interpréteurs de commande à distance.

Les protocoles de réseaux locaux sans-fil bénéficient eux aussi de mécanismes pour assurer la sécurité des communications. IEEE 802.11 par exemple a successivement connu différents mécanismes de sécurité, WEP étant le plus déployé.

[5] Les attaques par *war-driving* et l'engouement récent pour le *war-chalking* sont particulièrement symptomatiques de cet état de fait.

La sécurité des communications est donc un axe de recherche qui a déjà été largement exploré. De nombreux algorithmes de chiffrement et autres protocoles de communication existent et ont jusqu'à présent bien résisté aux attaques. Bien que ces mécanismes soient une partie essentielle de la sécurité des VPNs, ils n'en sont qu'un aspect. En effet, la mise en place et la gestion d'un VPN entre les différents dispositifs d'un réseau requièrent de longues et complexes étapes d'installation et de configuration. La sécurité résultante est donc fortement dépendante de la compétence de l'administrateur [16].

Cette très forte implication de l'utilisateur dans la configuration de la sécurité n'est pas acceptable pour les réseaux domestiques. À quoi bon en effet disposer de réseaux qui s'auto-configurent dynamiquement s'il faut consacrer beaucoup de temps à la génération des clés, à leur gestion, à leur mise en place, etc.

De plus, les utilisateurs, et *a fortiori* les utilisateurs des réseaux domestiques, sont souvent considérés comme le maillon faible de la sécurité. Parce qu'ils ne sont pas formés aux règles de la sécurité, il peuvent être victimes du *social engineering*.

Enfin, les utilisateurs ne doivent surtout pas être impliqués dans la gestion de la sécurité de leur réseau domestique. En effet, l'expérience montre [10] que lorsqu'on laisse la sécurité entre les mains des utilisateurs, ils ont tendance à y préférer la facilité d'utilisation. Ils n'activent pas les mécanismes de sécurité, ou utilisent des modes de sécurité faibles (mots de passe triviaux par exemple).

## 4 Vers des réseaux domestiques sécurisés

Les solutions traditionnelles utilisées pour les réseaux informatiques ne peuvent donc être utilisées simplement pour sécuriser les réseaux domestiques, qui présentent des particularités incompatibles avec les pré-requis des mécanismes à implémenter.

### 4.1 Compromis

La mise en œuvre de la sécurité dans les réseaux domestiques doit être imposée, faute de quoi les utilisateurs ne l'activeront pas. À titre d'exemple, citons WEP qui malgré ses défauts apporte une sécurité minimale, et qui est pourtant rarement déployé.

Contrairement à d'autres services, la configuration de la sécurité ne peut pas être entièrement automatisée : les tâches d'autorité doivent être prises en charge par l'utilisateur, qui est le seul à pouvoir décider des dispositifs appartenant à son réseau domestique.

Jusqu'à présent, nous avons supposé que l'utilisateur n'était jamais impliqué dans la configuration du réseau et de sa sécurité. Cependant, un compromis entre la facilité d'utilisation et la sécurité est indispensable.

Par opposition aux réseaux domestiques, les *réseaux domestiques sécurisés* doivent :

- Supporter une grande hétérogénéité.
- Autoriser des comportements extrêmement dynamiques.
- *Assurer par défaut un certain niveau de sécurité.*
- Fonctionner sans administration, *à l'exception de l'expression de l'autorité par l'utilisateur.*

De la même manière qu'ils déchargent l'utilisateur de l'installation des dispositifs et de leur configuration sur le réseau, les réseaux domestiques sécurisés doivent décharger les utilisateurs des manipulations fastidieuses concernant la mise en œuvre de leur sécurité : la tâche d'administration est réduite à une tâche d'autorité. Du point de vue de la frontière, l'utilisateur doit simplement indiquer les dispositifs qui font partie du réseau domestique, et ne doit pas être impliqué dans la manipulation de matériel cryptographique, de fonctions de chiffrement, de mots de passe complexes, etc.

Plusieurs travaux ont déjà été publiés dans le domaine des réseaux *ad hoc* et de l'*Ubiquitous Computing* ayant pour but de mettre en œuvre des mécanismes de sécurité en ne requérant qu'une très faible implication de l'utilisateur.

### 4.2 Premiers résultats

Frank Stajano expose dans [1] la problématique de la sécurité pour l'*Ubiquitous Computing* et l'état de l'art des propositions de sécurité. Il décrit notamment le modèle du "*Resurrecting Duckling*" [14] qui permet de mettre aisément en place des relations sécurisées point-à-point temporaires.

Dans ce modèle, chaque dispositif peut être alternativement dans deux états différents : vierge ou marqué. Un dispositif $B$ passe de l'état vierge à l'état marqué lorsqu'un autre dispositif $A$ le "marque de son empreinte" et en prend le contrôle. Pendant cette opération, $A$ transmet à $B$ *via* un canal sûr (par exemple un contact physique, lorsque l'utilisateur place les deux dispositifs l'un contre l'autre) ses données cryptographiques, qui permettront par la suite de communiquer de manière sécurisée. Tant qu'il reste marqué, $B$ obéit à $A$, et ne peut plus être marqué par aucun autre dispositif. Le passage de l'état marqué à vierge se fait lorsque $A$ "libère" $B$ et lui ordonne de se ré-initialiser. $B$ regagne alors son état initial, et sa relation temporaire avec $A$ est dissoute.

Dans le modèle initial, les relations sont strictement point-à-point. En particulier, seul l'appareil ayant marqué l'autre peut lui restituer son état vierge, ce qui renforce légèrement la sécurité au prix d'une contrainte d'ergonomie.

Dans [12], Stajano étend le modèle du "*Resurrecting Duckling*"en permettant à un dispositif $A$ marquant un dispositif $B$ de lui transmettre optionnellement une politique de sécurité en même temps que les informations cryptographiques. Ainsi, il peut par exemple l'autoriser à échanger des informations avec d'autres dispositifs, et éventuellement à accepter des politiques de sécurité venant d'autres dispositifs.

Divers travaux se sont inspirés du "*Resurrecting Duckling*", dans le domaine des réseaux *ad hoc* notamment. Balfanz et al. [4] s'en servent pour garantir la

sécurité des communications entre des dispositifs devant interagir ponctuellement (par exemple, un ordinateur portable et une imprimante "publique" dans un aéroport). Ils proposent notamment différents algorithmes permettant la transmission du matériel cryptographique en utilisant un canal de communication présentant des propriétés plus faibles que le "*Resurrecting Duckling*". Par exemple, l'un d'entre eux ne requiert pas que le canal soit confidentiel.

Feeney et al. [15] proposent quant à eux d'utiliser des canaux de communication localisés pour sécuriser les "réseaux spontanés". Un réseau spontané est formé de dispositifs (typiquement des ordinateurs portables et des assistants numériques personnels) mis en présence temporairement en vue d'activités collaboratives. Pour assurer l'authenticité et la confidentialité des communications entre ces dispositifs, les participants s'échangent au début de la réunion (par exemple par infrarouge) une clé de session générée aléatoirement. Comme ils ne manipulent jamais directement de matériel cryptographique et n'en ont même pas connaissance, la mise en œuvre de la sécurité ne nuit pas à la facilité d'utilisation.

Le gestionnaire de sécurité (*security manager*) de Bluetooth est une autre approche, plus industrielle, de la prise en charge de la sécurité par les dispositifs. Chaque module Bluetooth dispose d'un gestionnaire de sécurité qui libère l'utilisateur de la plus grande partie de la gestion des données cryptographiques. Il assure tout d'abord le contrôle d'accès au dispositif local et à ses ressources. Tout autre dispositif souhaitant y accéder doit connaître une information secrète (d'une longueur maximale théorique de 16 octets, mais en pratique souvent réduite à un code PIN de 4 chiffres). Le gestionnaire de sécurité vérifie que le dispositif à l'origine de la requête connaît ce secret, et, le cas échéant, lui permet d'accéder à la ressource.

Le gestionnaire de sécurité se charge aussi de sécuriser les communications avec les autres dispositifs Bluetooth, en générant avec chaque dispositif une clé partagée obtenue par dérivation de l'information secrète (i.e. le code PIN) nécessaire pour accéder à la ressource. Cette clé servira à assurer l'intégrité et la confidentialité des messages.

Enfin, le gestionnaire de sécurité mémorise les opérations de sécurité (contrôle d'accès et mise en place de clé partagée) déjà réalisées. Ainsi, l'utilisateur d'un dispositif $A$, demandant à accéder à plusieurs reprises à un service fourni sur le dispositif $B$, ne rentre le code PIN requis par le gestionnaire de sécurité de $B$ qu'une fois. Par la suite, $B$ sait que $A$ est autorisé à accéder au service.

Toutes ces propositions visent la mise en œuvre d'une sécurité transparente pour l'utilisateur. Toutefois, il n'existe pour l'instant aucune proposition permettant de mettre en œuvre une frontière telle que nous l'avons définie. Une recherche plus poussée est donc nécessaire.

## 5 Conclusion

Il est maintenant clair que lorsque les réseaux domestiques seront démocratisés, ils seront victimes d'attaques multiples :

- Héritées des attaques informatiques classiques concernant la partie IP / PC.
- Liées à des conditions de voisinage concernant les communications sans fil.
- Liées à la valeur des contenus multimédias et à leur manipulation dans un contexte *consumer electronics*.
- Liées à l'utilisation des appareils et des services par des non-administrateurs.

Ils doivent donc être sécurisés pour en faciliter l'adoption. L'établissement d'une frontière délimitant le réseau domestique est la première étape d'une sécurisation raisonnée et acceptable.

Les solutions de sécurité éprouvées en contexte professionnel ne sont pas adaptées en contexte domestique, soit parce qu'elles sont inopérantes en l'état (*firewall* IP), soit parce qu'elles contraignent trop fortement le réseau (serveur centralisé), soit encore parce qu'elles requièrent un utilisateur expert.

Il s'agit donc de mettre en place un mécanisme permettant d'établir et de maintenir la frontière de manière transparente à l'utilisateur.

Plusieurs travaux ont déjà proposé des mécanismes permettant de mettre aisément en œuvre des relations sécurisées entre différents dispositifs. Toutefois, ces relations sont le plus souvent point-à-point, et/ou temporaires. À notre connaissance, aucun résultat n'a été publié sur la gestion de groupes dynamiques à long terme.

Dans cet esprit, nous menons actuellement des recherches pour permettre la mise en place distribuée d'une frontière garantissant la cohérence du réseau domestique après des opérations de fractionnement et de fusion, et autorisant la révocation d'appareils volés ou compromis, tout en tenant compte de la facilité d'accès à ces fonctions par des non-administrateurs.

## Remerciements

Les auteurs tiennent à remercier Jean-Pierre Andreaux, Eric Diehl et Valérie Gayraud pour leurs contributions précieuses. Ils tiennent aussi à remercier les relecteurs, et particulièrement Nicolas Fischbach, pour leurs remarques pertinentes et constructives.

## Références

1. Frank Stajano, *Security for Ubiquitous Computing*, John Wiley and Sons, 2002, *ISBN 0-470-84493-0*, *http ://www-lce.eng.cam.ac.uk/ fms27/secubicomp/*
2. The Honeynet Project, *Know Your Enemy*, Addison Wesley, 2001.

3. *www.@stake.com*, @stake security advisory, Nokia 6210 DoS SMS Issue, 2003, *http ://www.atstake.com/research/advisories/2003/index.html#022503-1*
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, 2002, *citeseer.nj.nec.com/balfanz02talking.html*
5. William A. Arbaugh, William L. Fithen et John McHugh, *Windows of Vulnerability : A Case Study Analysis*, IEEE Computer", IC-33, no 12, pp 52-59, 2000.
6. Chris Davis et Aaron Higbee, *DC Phone Home*, BlackHat Conference, 2002.
7. Gordon Bell et Jim Gemmell, *A call for the home media network*, Communications of the ACM, Vol. 45, no. 7, 2002, pp. 71–75, *http ://doi.acm.org/10.1145/514236.514237*, ACM Press.
8. R. Want, B. N. Schilit, N. I. Adams, R. Gold, K. Petersen, D. Goldberg, J. R. Ellis et M. Weiser", *An overview of the* `PARCTAB` *ubiquitous computing experiment*, IEEE Personal Communications, Vol. 2, no. 6, pp. 28-33, 1995, *citeseer.nj.nec.com/want95overview.html*
9. Médiamétrie, *Les Baromètres Multimédia*, Février 2003, *http ://www.mediametrie.fr/web/resultats/barometre/resultats.php ?id=632*
10. J. Jeff, Y. Alan, R. Ross et A. Alasdair, *The Memorability and Security of Passwords – Some Empirical Results*. Technical Report No. 500, Computer Laboratory, University of Cambridge, 2000, *http ://www.ftp.cl.cam.ac.uk/ftp/users/rja14/tr500.pdf*
11. Mark Weiser, *The computer for the 21st century*, ACM SIGMOBILE Mobile Computing and Communications Review, Vol. 3, no. 3, 1999, pp. 3–11, *http ://doi.acm.org/10.1145/329124.329126*, ACM Press.
12. Frank Stajano, *The Resurrecting Duckling – What Next ?*, Lecture Notes in Computer Science, Vol. 2133, pp. 204–211, 2001, *citeseer.nj.nec.com/stajano00resurrecting.html*
13. Aleph One, *Smashing the Stack for Fun and Profit*, Phrack, Vol. 49, 1996, *http ://www.phrack.org/show.php ?p=49&a=14*
14. Frank Stajano et Ross Anderson, *The Resurrecting Duckling : Security Issues for Ad-hoc Wireless Networks*, 7th International Workshop on Security Protocols, pp. 172–194, 1999, *citeseer.nj.nec.com/stajano99resurrecting.html*
15. L. Feeney, B. Ahlgren et A. Westerlund, *Spontaneous networking : an application-oriented approach to ad hoc networking*, IEEE Communications Magazine, June 2001, *citeseer.nj.nec.com/feeney01spontaneous.html*
16. Bruce Schneier, *Secrets and Lies : Digital Security in a Networked World*, John Wiley & Sons, 2000.
17. CERT Coordination Center, Carnegie Mellon University, *CERT/CC Overview Incident and Vulnerability Trends*, 2002, *http ://www.cert.org/present/cert-overview-trends/*