Dépérimétrisation : futur de la sécurité réseau ou pis aller passager ?

Cédric Blancher

EADS Innovation Works, Suresnes, France,
Computer Security Research Lab,
cedric.blancher@eads.net,
http://sid.rstack.org/

Résumé Devant l'incapacité consommée des modèles de sécurité réseau classiques à fournir un niveau de protection approprié, en particulier face au nomadisme, l'idée d'aller vers une suppression assumée des barrières fait depuis quelques années son chemin au sein de la communauté de la sécurité informatique.

Le présent article vise à présenter ce qui se cache derrière le terme barbare de *dépérimétrisation* et d'en discuter les apports et les défauts pour la protection du patrimoine informationnel. La question de la faisabilité technique sera en particulier soulevée, qu'il s'agisse de l'état actuel de l'art ou en anticipation d'avancées qu'on espèerait majeures.

Tout ceci pour tenter de répondre à la question de savoir si une telle *dépérimétrisation* est une solution viable et pérenne, ou rien de plus qu'une simple lubie passagère comme le monde de la sécurité informatique en connait régulièrement. . ..

Introduction

Depuis quelques annéess, les références à la *dépérimétrisation des réseaux* se font de plus en plus fréquentes dans les discussions autour de la sécurité des réseaux informatiques. Cette idée veut que le modèle presque ancestral de sécurisation des réseaux basé sur un cloisonnement de l'infrastructure en compartiments plus ou moins étanches par un savant enchaînement de pare-feu de plus en plus puissants soit voué à l'échec pour deux raisons principales. La première tenant aux limites techniques de telles mesures de sécurité, la seconde à l'impact fonctionnel de ces barrières sur les applications courantes.

En conséquence, une approche visant à ouvrir le réseau pour limiter les barrières fonctionnelles, et à ramener la sécurité au niveau des nœuds pour en accroître l'efficacité serait aujourd'hui bien plus pragmatique et efficace.

1 Faillite du modèle périmétrique ?

L'idée de dépérimétrisation naît d'un constat apparemment récurrent que le modèle périmétrique ne serait plus adapté à la réalité de réseaux de plus en plus connectés, d'applications de plus en plus communiquantes, d'utilisateurs de plus en plus mobiles et d'informations que si trouvent plus que jamais distribuées aussi bien l'espace physique que logique. Or ce modèle de protection classique ne fonctionnant que par la mise en place de barrières au niveau du réseau, il entrave d'une part des communications qui peuvent s'avérer légitimes et ne résoud d'autre part pas le problème de la sécurisation de l'information proprement dite, laissant ce soin aux couches applicatives. Ceci est

particulièrement flagrant dans les grandes organisations ou la mise en place de systèmes connectant plusieurs acteurs indépendants, comme le propose par exemple le concept d'*extended enterprise*.

1.1 Migration vers les couches hautes

Une conséquences évidente de cette entrave au fonctionnement *normal* du réseau, c'est à dire sa capacité à acheminer des données d'un point A à un point B du réseau[1], est la migration des protocoles applicatifs au dessus de protocoles populaires et largement autorisés dans la pratique, HTTP en tête. Qu'il s'agisse de *webification* de services ou d'encapsulation plus ou moins poussée, de plus en plus d'applications ont recours au protocole HTTP en lieu et place d'un protocole de transport. Tendance largement renforcée par l'attrait pour le client léger, à savoir un poste de travail dont le jeu d'applications standards se résumerait grosso mode à un navigateur et quelques greffons.

La liste des applications ayant recours à un tel artifice est tellement longue qu'on se restreindra à quelques exemples. On pensera par exemple au protocole WebDAV[2], ou encore à la fonctionnalité *Outlook Anywhere*[3] de Microsoft Exchange. Les outils permettant d'établir des tunnels VPN capables de passer à travers les mandataires HTTP, les utilisant comme relai TCP grâce à la méthode CONNECT comme montré en figure 1 sont désormais légion. On aurait même vu des clients VPN faire de l'IPsec sur HTTP pour être encore plus *universels* que le NAT-Traversal...

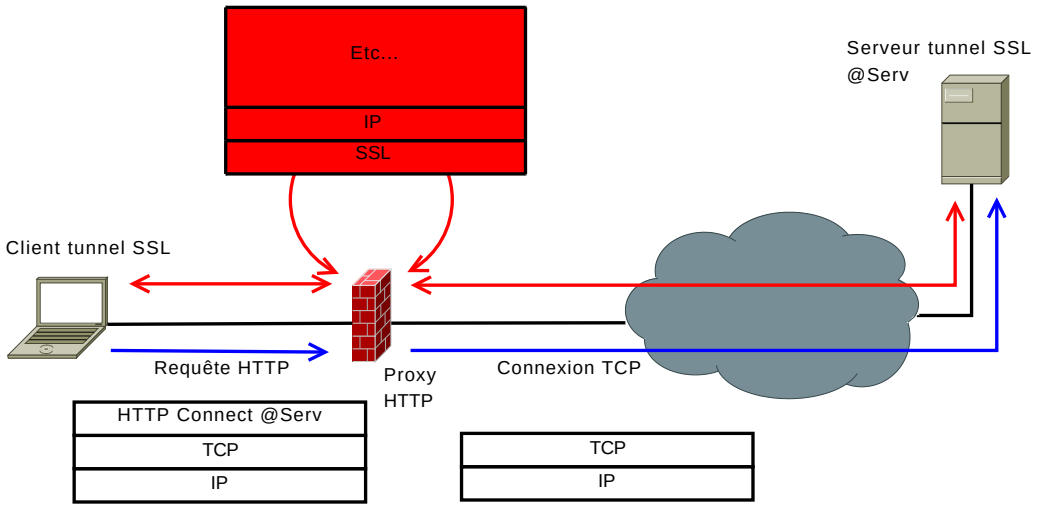

FIG. 1: Exemple de lien VPN SSL utilisant la méthode CONNECT.

Cette utilisation déviante d'un protocole applicatif pose évidemment quelques problèmes de sécurité. De même qu'on s'est rapidement aperçu qu'il ne suffisait pas de n'autoriser que les

[1] Réseau étant ici à prendre au sens large du terme.
[2] Web-based Distributed Authoring and Versioning.
[3] RPC sur HTTP.

connexions à destination du port TCP/80 pour n'autoriser que le protocole HTTP, puisqu'il est possible de détourner cette autorisation à d'autres fins, on s'est également aperçu que vérifier que le flux transitant par ce port répondait bien au protocole HTTP ne suffisait pas non plus à garantir qu'on n'y faisait que du Web. S'en est suivie une inflation dans les capacités des pare-feu à disséquer et inspecter des protocoles de plus en plus complexes au sein de flux toujours plus nombreux et rapides. Inflation encore d'actualité.

Associée à cette enchère protocolaire, on notera une sous-catégorie de logiciels utilisant ces mécanismes d'encapsulation combinés à des capacités dites de *firewall punching* pour assurer leur fonctionnement. Par *firewall punching*,on entend tout un jeu de tests permettant à l'application qui les implémente de découvrir et identifier les mécanismes de protection réseau qui la sépare d'autres agents extérieurs dans le but avoué de les contourner afin d'établir ses communications. C'est notamment le cas d'applications communiquant sur un modèle *Peer-to-Peer*, pouvant aller jusqu'à créer un véritable réseau au-dessus de réseau, permettent malheureusement le contournement de la politique réseau mise en place. On pourra citer le cas de Skype, Hamachi ou encore Teredo, ce protocole visant à fournir une capacité de communication de client à client en IPv6 au dessus d'UDP.

1.2 Challenge du nomadisme et de la collaboration

L'usage des ressources informatique se faisant de plus en plus mobile et collaborative, la question de la sécurisation des terminaux d'une part, et de l'accès concurrents aux ressources d'autre part s'est très vite posée[6].

Parmi les problématiques, on notera en particulier :
- la sécurité du terminal contre les attaques, qu'elles soient logiques ou physiques ;
- la sécurité de l'accès aux ressources mises à disposition ;
- la sécurité des échanges de données ;
- la disponibilité des ressources et leur actualisation.

En particulier, l'intégration du nomadisme et de la collaboration dans ce contexte suppose l'ouverture, et donc une exposition accrue de ressources critiques pour le patrimoine informationnel de l'organisation par rapport au modèle traditionnel.

En outre, la résolution de problèmes de nomadisme fait souvent intervenir l'utilisateur, comme par exemple pour décider du besoin de mettre en place un tunnel VPN ou non. De nombreuses configurations laissent ce choix, non pas que la volonté que le poste nomade ne fonctionne que sur ce mode, mais parce qu'on ne veut pas bloquer l'usage de ressources Internet publiques lorsque l'environnement n'est pas favorable à la mise en place du contexte protégé. En outre, des échanges sont parfois obligatoires en contexte normal pour fournir au client les autorisations nécessaires. C'est en particulier le cas des réseaux fermés par un portail captif qui supposent la fourniture d'éléments d'authentification avant de pouvoir mettre en place son lien VPN, exposant le client pendant cette phase initiale.

1.3 Sécurisation des couches basses

Jusque là limitée au contrôle des flux aux frontières, la maîtrise du périmètre a pris une nouvelle dimension avec l'essor du nomadisme. Le risque de voir des ressources agir, volontairement ou non, de façon malveillantes depuis l'intérieur même du périmètre est devenu suffisamment pesant pour que les technologies de contrôle d'accès au niveau LAN se développent, avec l'introduction dans les

couches basses de fonctionnalités de sécurité allant de l'authentification des hôtes à la connexion[4] lorsqu'il s'agit de discriminer ses propres utilisateurs des éventuels visiteurs, à un véritable examen de santé lorsqu'il s'agit deprévenir la propagation de vers via des ressources certes autorisées mais compromises...

Ces mesures à l'efficacité toute relative[19] montrent toute la fragilité du concept de périmètre face au développement de la mobilité dans un système d'information. Car la notion même de périmètre suppose l'existence d'une zone qu'on voudrait garder saine à tout prix. Dès lors qu'elle se trouve compromise, la sécurité de l'ensemble s'écroule comme un château de cartes. À moins de ne considérer aucun de ses périmètres comme de confiance, auquel cas la notion de périmètre de sécurité perd quelque peu de son intérêt.

1.4 Impacts sur l'utilisation du système d'information

L'approche périmétrique manque également de flexibilité, en particulier dans des contextes où de multiples acteurs entrent en jeu. Le déploiement d'une application nécessitant de nouvelles autorisations du flux devient alors un véritable casse-tête. On mentionne en particulier un manque de réactivité de l'approche périmétrique à grande échelle rend donc difficile l'adaptation du système d'information aux besoins des utilisateurs. Ainsi, l'approche passe très mal à l'échelle et répond de moins en moins aux besoins des utilisateurs.

Dans le même temps, ces utilisateurs se voient offert les services dont ils manquent cruellement par des acteurs extérieurs, le plus souvent gratuitement. Prenons l'exemple d'un simple accès Web à la messagerie. La mise en place de ce type de fonctionnalité est parfois considérablement retardée du fait des considérations de sécurité. Dans le même temps, n'importe quel utilisateur peut s'ouvrir un compte chez un fournisseur gratuit et y transférer l'intégralité de son courrier professionnel pour y accéder en déplacement.

On peut multiplier les exemples, comme l'accès en ligne à son agenda et son partage, le stockage de fichiers, la sauvegarde en ligne, etc. Ce sont autant d'exemples de besoins auxquels les utilisateurs répondent eux-mêmes, sans penser aux conséquences en terme de sécurité. Typiquement, on assiste ici à une dissémination à des entités inconnues du patrimoine informationnel de l'organisation.

Il est d'ailleurs intéressant de discuter ce concept de besoins des utilisateurs, dans la mesure où ces derniers ont de plus en plus tendance à confondre informatique professionnelle et informatique personnelle. La grande pénétration des technologies de communication sur le marché grand public a complètement modifié les attentes de ces derniers qui rêvent aujourd'hui de pouvoir utiliser les ressources professionnelles comme ils utilisent leurs outils personnels, oubliant souvent que les enjeux ne sont pas exactement les mêmes. Et donc de savoir dans quelle mesure la dépérimétrisation répond effectivement à un réel besoin fonctionnel, autant pour augmenter le niveau de sécurité de fonctions déjà accessibles que pour rendre possible la mise à disposition de ressources autrement jugée trop risquée.

2 La dépérimétrisation

2.1 Concept de dépérimétrisation

La dépérimétrisation est un terme barbare désignant une nouvelle approche pour la sécurisation des infrastructure informatique ne nécessitant pas ou peu d'outils de filtrage de flux, typiquement

[4] 802.1x.

de pare-feu. Cette approche s'appuie sur une sécurisation au niveau des acteurs (authentification, forte de préférence) et des données échangées (chiffrement, contrôle d'intégrité).

La délégation de ces fonctions n'est pas clairement identifiée par les tenants de cette approche. En pratique, il reviendrait à chaque application de s'assurer de l'identité de la ressource avec laquelle elle va établir une connexion, chiffrer les données, en vérifier l'intégrité ainsi que l'inocuité.

D'autres approches délèguent une partie de ces fonctions à la couche réseau, comme le modèle de sécurité poussés par les développeurs d'IPv6, en s'appuyant sur le protocole IPsec à chaque fois que cela est nécessaire, qu'il s'agisse de mettre en place des tunnels de communications[5] ou de protection de flux bien précis[6].

2.2 Le Jericho Forum

Fig. 2: Page web du Jericho Forum.

La meilleure illustration du concept de dépérimétrisation des réseaux est sans doute le discours tenu par le Jericho Forum, dont le nom fait référence au récit biblique de la prise de Jéricho par les hébreux, lorsque les murailles de la ville s'écroulèrent sous la volonté divine alors qu'ils sonnaient les trompettes. Tout un symbole... Leur approche prétend fournir aux organisation la possibilité aux organisations de se passer de pare-feu coûteux[7] en se fondant sur onze commandements[27] permettant son implémentation.

Ces commandements sont les suivants[8] :

1. la portée et le niveau des mesures de protection doivent être spécifiques et appropriés aux ressources exposées ;

[5] Approche VPN.
[6] Utilisation du mode transport
[7] Mais pas de s'en passer du tout pour autant.
[8] Traduction libre de l'auteur

2. les mécanismes de sécurité doivent être pervasifs, facilement déployables et administrables, et simples ;
3. l'environnement doit être considéré comme hostile ;
4. équipements et applications doivent communiquer en utilisant des protocoles ouverts et sécurisés ;
5. tous les équipements doivent être capable de maintenir leur niveau de sécurité dans un environnement hostile ;
6. les personnes, processus et technologies doivent pouvoir négocier des relations confiance pour chaque transaction ;
7. des niveaux d'assurance et de confiance mutuelle doivent être définis ;
8. authentification, autorisation et imputabilité doivent interopérer et prendre en compte les ressources étrangères à votre contrôle ;
9. l'accès aux données doit être soumis aux attributs de sécurité des données elles-mêmes ;
10. la confidentialité des données nécessite un partage des responsabilités ;
11. par défaut, les données doivent être sécurisées lors de leur stockage, leur transport et leur manipulation.

Si ces commandements sont on ne peut plus sensés, ils ne contredisent pas pour autant l'approche périmétriques. Il s'agit surtout de bon sens, au point que certains pourraient se voir qualifier de lieux communs.

2.3 Apports

Dans un document opposant un état des lieux (cf. figure 3 relativement pessimistes aux apports de la dépérimétrisation[31], le Jericho Forum avance les arguments suivant en faveur de leur approche :

- réduction de la complexité de l'infrastructure et des solutions de sécurité, ainsi que leur coût ;
- flexibilité des moyens permettant l'adéquation aux besoins fonctionnels ;
- augmentation du niveau de sécurité par la une diminution importante des risques opérationnels ;
- communication plus simple et plus efficace avec les partenaires extérieurs ;
- simplification de l'environnement qui devient plus facilement maîtrisable ;
- véritable défense en profondeur, des couches réseau au données elles-même.

Le principal apport serait donc la simplification du système d'information dans le but d'obtenir une gestion plus efficace de l'accès aux données, donc au patrimoine informationnel de l'organisation. Si on se prend à rêver d'un monde dans lequel la dépérimétrisation fonctionne, l'administration de la sécurité se concentrera sur la gestion d'identité et des privilèges associés, brique de base permettant au nœuds d'établier ou non les communications désirées, en contexte chiffré.

2.4 Moyens

Pour illustrer la mise en application pratique des concepts précédemment exposés,le Jericho Forum propose de nombreuses publications[32] traitant de cas de figure variés comme les environnement sans-fil[29], la voix sur IP[28] ou encore la sécurité des terminaux[30].

À cela s'ajoutent d'autres éléments listés ainsi :

- architectures sécurisées (approche top-down) ;

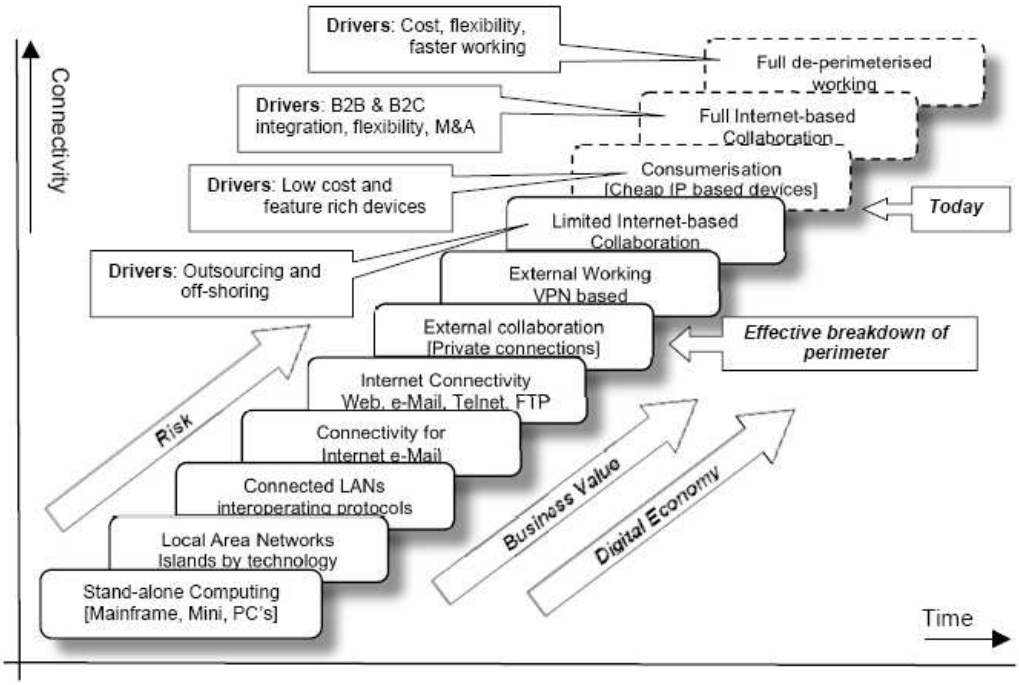

FIG. 3: Évolution des besoins de connectivité dans le temps (source : Jericho Forum[31]).

- développement sécurisé (approche bootom-up) ;
- réglementation et conformité ;
- analyse et gestion des risques ;
- gestion de la qualité de l'information ;
- architecture et méthodologies d'entreprise.

Concepts relativement connus et en rien spécifiques à la dépérimétrisation. Mettre un sens derrière certains d'entre-eux sera laissé en exercice au lecteur...

3 L'épreuve de la réalité

3.1 Implications de la dépérimétrisation

Si on applique les principes précédemment énoncés, on comprend que la sécurité d'un ensemble dépérimétrisé implique au moins deux propriétés essentielles :

- premièrement, chaque nœud de l'infrastructure doit se suffire à lui-même en terme de sécurité, qu'il soit en environnement protégé ou non (commandements n° 3 à 5) ;
- deuxièmement, chaque nœud de l'infrastructure doit être capable d'authentifier les correspondants avec qui il communique et leur accorder le niveau adéquat de confiance (commandements n° 6 à 8).

On constate d'emblée que ce sont des propriétés fortes qui sont pour le moins difficiles à garantir. Si la difficulté de garantir l'invulnérabilité d'un poste de travail isolé est relativement évidente, la

seconde propriété pourrait de prime abord presque paraître simple à réaliser. Or, si nous disposons bien de moyens d'authentification efficaces, ils ne suffisent pas pour autant à attribuer un niveau de confiance à son correspondant. En particulier lorsque le-dit niveau de confiance voudrait tenir compte de la notion d'intégrité. En effet, un équipement connu, authentifié et donc à priori de confiance peut tout à fait se révéler être un agresseur en puissance parce qu'il a été corrompu. De fait, la non réalisation de la première propriété met quelque peu à mal la seconde.

3.2 Faisabilité technique

Authentification et niveau de confiance

Commençons par la seconde propriété, qui suppose deux choses :
- la bonne authentification des parties en présence ;
- l'attribution du bon niveau de confiance pour la communication.

Si des solutions existent pour garantir une authentification forte et mutuelle des parties en présence, elles ne suffisent pas à attribuer un niveau de confiance adapté pour la réalisation de la communication. En effet, la confiance qu'on accorde à un entité donnée dépend également d'une donnée difficilement quantifiable : son intégrité. Ou pour les plus pessimistes, son degré de compromission.

Prenons l'exemple des mécanismes de contrôle d'accès au réseau de niveau 2 cités précédemment (cf. 1.3). On s'est vite rendu à l'évidence que la seule authentification des machines ne suffisait pas à protéger le périmètre. Ce mécanisme ne prenait en effet pas en compte le cas des hôtes légitimes compromis. D'où la volonté d'ajouter aux conditions d'accès la vérification d'un certain nombre de paramètres permettant de s'assurer dans une certaine mesure de la bonne santé de l'hôte.

On se retrouve ici dans une situation très similaire. Un nœud de l'infrastructure jouissant d'un niveau de confiance élevé peut tout à fait se révéler compromis et dès lors présenter une menace importante pour l'ensemble de l'infrastructure par les accès dont il dispose.

Une réponse naïve à ce genre de considération est de revenir au commandement n°3 en considérant tout son environnement comme hostile, y compris les éléments authentifiés de l'infrastructure. Malheureusement, on comprend bien que pour fonctionner, un minimum d'interaction doit avoir lieu et donc supposer au moins un minimum de confiance.

Ce qui nous amène donc à considérer la première propriété.

Survivabilité en environnement hostile

Dire qu'assurer la sécurité d'un système d'exploitation *professionnel* récent est tâche difficile est un doux euphémisme. En fait, cela relève carrément de la gageure, en particulier pour la catégorie directement concernée par les préceptes de la dépérimétrisation, les postes utilisateurs mobiles que sont les ordinateurs portables, les PDA, les smartphones et plus largement tous les moyens de communication informatique plus ou moins sophistiqués.

Il ne sera pas nécessaire de se lancer dans une longue démonstration tellement l'expérience et l'actualité récentes démontrent que l'espérance de vie d'un poste de travail en environnement hostile, et d'autant plus s'il est spécifiquement ciblé, est considérablement limitée tellement la surface d'attaque qu'il présente est importante.

Si le problème de la résistance aux attaques directes venant du réseau est relativement bien traité par l'utilisation d'outils comme les pare-feu personnels[5] et celui de la confidentialité des

échanges par l'utilisation de technologies de type VPN[9] ou de protocoles d'échange chiffrés, cela ne suffit pas à couvrir l'intégralité de la surface vulnérable du client mobile.

On pensera d'abord aux attaques réseau de bas niveau, visant les pilotes ou les piles réseau des systèmes d'exploitation. On se souviendra des travaux portant sur la recherche de failles dans les pilotes Wi-Fi[8][14] et leur exploitation en espace noyau[15] qui a touché à peu près tous les type de matériel sur au moins un des trois systèmes d'exploitation les plus répandus. On pensera également à des travaux similaires portant sur les piles BlueTooth[12] et enfin à la récente exploitation à distance d'une faille dans la pile réseau de Microsoft Windows[22].

On pensera ensuite aux attaques physiques. Si le chiffrement complet du disque dur offre une bonne protection à la fois contre le vol de données et la compromission du poste de travail, de nombreux travaux ont prouvé qu'on pouvait agir directement sur la mémoire d'un poste de travail. L'actualité récente nous a démontré une exploitation pratique de la rémanence des données dans les mémoires DRAM de nos ordinateurs[26], permettant de lire des données sensibles comme des clés de chiffrement par exemple. D'autres travaux ont également démontré la possibilité récemment remise au goût du jour d'agir sur la mémoire d'un système d'exploitation via un port FireWire[11] ou un emplacement PCMCIA[9][10], ou la capacité à lire et/ou modifier un fichier d'hibernation[21].

On étudiera alors la problématique des attaques dite "côté client" visant les applications courantes d'un poste de travail comme les suites bureautiques, les navigateur et leurs greffons, les logiciels de traitement de messagerie, les outils multimédia, etc. Des annonces de failles tombent régulièrement sur ce type de composants. Et c'est aujourd'hui un des vecteurs de compromission les plus efficaces qui soient, comme l'a encore une fois démontré le challenge Pwn2Own organisé en parallèle de la conférence Cansecwest. Comme l'an dernier, les failles qui ont permis de compromettre deux machines à jour, la première sous MacOS 10.5.2 et la seconde sous Windows Vista Ultimate SP1, prenaient pour cible des applications clientes, le navigateur Safari et le greffon Flash d'Adobe respectivement, et ce malgré les éventuelles protections déployées au niveau du système d'exploitation, Windows Vista en particulier.

Certes, nous avons à notre disposition d'autres moyens de protection locaux, comme les logiciels dits HIPS[11] ou encore les antivirus. Mais si ces dispositifs sont parfois contournables, il apparaît qu'ils augmentent également de façon notable la surface vulnérable de l'hôte qu'ils sont censés protéger. Ceci a largement été démontré dans le cas précis des antivirus, aussi bien pour ce qui est du contournement[23] que pour leur exploitation pure et simple[18], ce que certains ne manquent pas d'exploiter lors de tests d'intrusions[24]...

Il apparaît donc relativement compliqué, d'un point de vue technique, d'assurer la survie d'un nœud, et donc de lui accorder un niveau de confiance important. Cependant, les tenants de la dépérimétrisation ne manquent pas d'exemples quand il s'agit d'illustrer leur propos.

3.3 La dépérimétrisation face à la réalité

Commençons donc par analyser quelques exemples mis en avant pour illustrer les préceptes et les bienfaits de la dépérimétrisation.

Exemples pratique d'implémentation

[9] Virtual Private Network, abusivement traduit par Réseau Privé Virtuel en français
[10] Voire même via un port firewire sur carte PCMCIA...
[11] Host Intrusion Prevention Systems

FIG. 4: Modification de la mémoire vidéo depuis un iPod connecté sur un port FireWire (via une carte PCMCIA).

Durant la conférence Deepsec 2007 qui s'est tenue courant novembre 2007, Paul Simmonds du Jericho Forum est venu présenter[20] les avantages de la dépérimétrisation et a cité quelques l'exemple d'actions dans ce sens, et en particulier celui de son propre ordinateur portable comme implémentation pratique des préceptes présentés précédemment.

Parmi les exemples en question, on pourra citer :

- BP qui aurait sorti 18000 ordinateurs portable du périmètre de son LAN pour les connecter sans protection extérieur sur Internet[7] ;
- ICI redirige ses flux Internet d'un accès unifié via son WAN à des accès DSL locaux[13] ;
- KLM serait passé à des ordinateurs portables achetés et maintenus par les employés pour économiser en support informatique[17] ;
-

L'exemple de BP est assez caractéristique de l'écart entre la théorie de la dépérimétrisation et sa mise en pratique. En effet, il est clair que ces ordinateurs portables, lorsqu'ils sont connectés chez BP, ne disposent pas d'adresses IP publiques tellement le coût associé serait important. Ils sont donc connectés en adressage privé[1], ce qui les place de facto au sein d'un périmètre dans lequel ils bénéficient d'une certaine manière d'une protection en ce que leur adressage interdit les connexions directes venant d'Internet. Et même si cette protection est tout relative, il est clair qu'il n'y a pas

équivalence entre le niveau d'exposition d'une machine adressée publiquement sur Internet et une machine connectée derrière une passerelle de traduction d'adresses.

L'exemple de KLM me paraît relativement surprenant. Ne serait-ce que par le but recherché. En effet, les coûts associés à la gestion des ordinateurs par les employés eux-mêmes en terme de formation, de temps accordé à cette tâche et donc de perte de productivité qui en découle ne sont probablement pas négligeables. Mais plus loin que cela, le niveau de la menace qui pèse aujourd'hui sur le poste de travail standard est tel qu'il me semble difficile de concevoir qu'on puisse en laisser le contrôle total à des personnels inexpérimentés donc l'informatique n'est pas le métier, et encore moins la sécurité. Évidemment, cela rejoint complètement le commandement n°3 : le système d'information serait conçu pour pouvoir gérer des postes clients compromis jusqu'à la moelle. Mais qu'en est-il des informations qu'ils traitent ? Puisque c'est bien de protection de l'information qu'on parle...

Dernier exemple, le portable de Paul Simmonds. À la question de savoir quels moyens de protection locaux étaient déployés sur ce poste de travail pour en assurer la complète autonomie et s'ils ne représentaient pas une surface d'attaque supplémentaire importante, il répondra que ces derniers sont en fait déportés. S'agissant principalement de moyens antiviraux[12], ces derniers sont en fait mis en place au niveau du service de messagerie et d'un mandataire pour les flux HTTP, lesquels se trouvent sur le site mère. Les connexions à ces services sont évidemment dûment authentifiées et chiffrées en TLS.

Il est relativement surprenant, quand on parle de dépérimétrisation et de sécurité auto-suffisante, de se voir illustrer ces concepts par une dépendance vis-à-vis de moyens extérieurs d'une part, et par le remplacement du classique lien VPN tant décrié par autant de liens TLS que nécessaire. Le tout ne dispensant évidemment de moyens antiviraux locaux, ne serait-ce que pour traiter les flux chiffrés que ne pourraient pas gérer les moyens centraux. Ce mode de fonctionnement n'a plus grand chose à voir avec un ordinateur portable auto-suffisant lâché sur Internet...

Une telle implémentation ressemble donc plus à un re-centrage du périmètre sur des ressources critiques mises à disposition d'acteurs dûment authentifiés. Ces ressources faisant en outre l'objet de moyens de protections eux-mêmes centralisés, on a plus l'impression d'avoir une implémentation de client nomade léger qu'une réelle disparition d'un quelconque périmètre de protection.

La réalité technique

La réalité technique est donc nettement plus compliquée qu'on voudrait nous le faire croire. En particulier en ce qui concerne la survivabilité du poste de travail mobile pour laquelle les moyens de protection efficaces font aujourd'hui cruellement défaut.

Côté réseau, les faits sont là. L'Internet IPv4 est fragmenté, qu'on le veuille ou non. La simple utilisation de la traduction d'adresses crée à elle seule des périmètres indépendamment de toute autre considération technique. Quelle que soit la manière dont on tourne le problème, la dépérimétrisation totale n'est pas réalisable sur IPv4. Mais est-ce pour autant un problème ?...

Comme nous l'avons vu précédemment, il existe des protocoles permettant la constitutions de réseaux virtuels au-dessus du réseau physique, ce que les anglophones appellent des *overlay networks*. Un tel réseau permet à ses utilisateurs d'évoluer dans un espace dépérimétrisé, au même titre qu'un réseau local. Ce n'est ni plus ni moins qu'un nouveau périmètre, logique, au-dessus du réseau global, physique.

[12] À prendre au sens large.

Pour autant, la constitution de ces réseaux au-dessus de l'Internet IPv4 tel que nous le connaissons aujourd'hui réclame des trésors d'ingéniosité pour obtenir une connectivité et établir les liens hôte à hôte, ne serait-ce que lorsqu'ils sont situés derrière des passerelles de traduction d'adresses, comme ceux implémentés dans Teredo[4].

Applicabilité de la dépérimétrisation

La dépérimétrisation est-elle applicable à tous les besoins du système d'information ? Si les fameux commandements peuvent tous être appliqués avec bonheur pour augmenter son niveau de sécurité, il ne suffit pas de s'y conformer pour pouvoir prétendre à la suppression des pare-feu. Dans la mesure où le risque de compromission d'un système d'informatique est, comme nous l'avons vu précédemment, loin d'être négligeable, il reste tout de même fort appréciable de pouvoir isoler certaines ressources sensibles, ne serait-ce qu'au titre de la défense en profondeur, concept relativement sain qui a fait ses preuves par le passé. Or, d'une certaine manière, la dépérimétrisation des réseaux va en quelque sorte à l'encontre de ce dernier, en particulier lorsqu'il s'agit de ressources à forte valeur, typiquement les espaces de stockage documentaires.

En fait, quand on creuse le discours et les exemples choisis, on s'aperçoit que la dépérimétrisation n'est en fait applicable qu'à une partie du système d'information seulement, à savoir les postes mobiles complexes. Quel est par exemple l'intérêt de supprimer les pare-feu qui isole des DMZ dans laquelle nous trouverons serveurs web, serveurs de messagerie, de base de données, etc. ? Dans la mesure où les flux entre ces différents services sont clairement identifiés et correctement pris en charge, la présence de barrière correctement configurées ne pose pas de problème fonctionnel. Ce type de raisonnement peut être étendu à toutes les ressources fixes, pour autant qu'on puisse identifier les mécanismes de communication mis en jeu.

Certes, il existe des protocoles de communication difficiles à gérer. L'exemple de la voix sur IP et de SIP vient immédiatement à l'esprit dans la catégorie *cauchemars de firewall*[16]. Pour autant, cette difficulté tient plus à la complexité du protocole et le manque d'implémentation des mécanismes de sécurité associés[13] qu'à un problème intrinsèquement lié à l'existence d'un pare-feu. C'est typiquement le genre de cas où la dépérimétrisation devient un fourre-tout, une espèce de solution magique à tous les soucis, ce qui n'est évidemment la bonne manière d'aborder le problème.

En outre, la dépérimétrisation pose un certain nombre de problèmes comme la surveillance de l'infrastructure. Dans la mesure où l'intégralité des échanges est chiffrée, cette surveillance ne peut venir que de données exportée par les nœuds. En plus du problème de réaliser cette tâche efficacement, compte tenu des considérations précédemment évoquées, on peut se demander s'il est vraiment efficace de baser sa compréhension de l'état du système d'information sur des informations provenant d'éléments possiblement compromis ou devant être considérés comme l'étant.

Enfin, la question de savoir à qui profite réellement la dépérimétrisation reste entière. En effet, la dépérimétrisation des uns sert surtout aux autres. Si nous reprenons l'exemple cité précédemment du portable de Paul Simmonds, ce dernier ne fonctionne correctement que s'il dispose d'un moyen efficace d'établir des communications avec des ressources de son réseau mère. Ressources dont la protection derrière un ou plusieurs pare-feu ne pose pas de problème fonctionnel insurmontable. Ce qui pourrait donc l'empêcher de fonctionner correctement serait un filtrage par l'infrastructure qui l'accueille des connexions qu'il voudrait établir. On se trouve alors dans un cas typique où celui qui a besoin de dépérimétrisation n'est pas celui qui en subira les conséquences.

[13] Quand ils existent ou sont disponibles...

On pourra, à la lumière de cet exemple, s'interroger sur le partage de responsabilité dans le cadre de la dépérimétrisation. Accueillir sur ses infrastructures des éléments étrangers et leur offrir la possibilité d'utiliser les accès offerts à des fins agressives, volontaires ou non, pose un nombre certain de questions sur les responsabilités des acteurs en présence, en particulier lorsque les attentes de chacun ne sont pas compatibles. L'exemple KLM est également intéressant de ce point de vue. Si le poste de travail est celui de l'utilisateur, comment l'empêcher d'y installer des composants ou applications qui vont entraîner une baisse notable de son niveau de sécurité ? Qui sera responsable si le système d'information se fait compromettre via une telle application ? On peut évidemment se doter de chartes, de politiques et autres règles diverses pour contraindre l'utilisation de ce poste de travail. Mais ce faisant, on remet en cause l'efficacité du modèle dépérimétrisé dans la gestion d'un environnement hostile. La question du droit en environnement dépérimétrisé est extrêmement intéressante et mériterait probablement un article à elle seule. Cependant, le droit n'étant cependant pas la spécialité de l'auteur, il laissera l'étude de cet épineux problème en exercice au lecteur averti.

3.4 Impact sur le patrimoine informationnel

La dépérimétrisation pose le problème également de la maîtrise du patrimoine informationnel. Le risque de dissémination excessif de ce dernier est en effet bien réel quand on imagine un système d'information constitué de milliers de terminaux indépendants stockant chacun quelque giga-octets de données, parmi lesquelles nombre de documents confidentiels. Sans parler des supports de stockage amovibles que sont les CD ou DVD ré-incriptibles, les clés USB, les disques portables ou tout support de données mobile.

Mais plus loin que la confidentialité de ces données, qu'il conviendra de traiter à grands coups de chiffrement, se pose la question de leur disponibilité. Une réponse classique à ce genre d'interrogation est en effet le client léger comme le montre l'intérêt suscité par des technologies comme Google Docs susceptibles d'être mises à disposition des organisations sous forme d'appliance. Cependant, l'absence de connexion rend le client léger inopérant, d'où la nécessité de répliquer localement de l'information.

Donc, à mesure que l'informatique se fait de plus en plus mobile et collaborative, le patrimoine informationnel de l'organisation de trouve disséminé sur une bonne partie des acteurs du système d'information, parmi lesquels on trouvera certes des ressource internes, mais également des ressources externes comme les partenaires, les clients, les fournisseurs, etc. C'est le genre de considération qui plaide pour une centralisation importante de l'information au sein du système d'information, c'est à dire la constitution d'un périmètre fort.

3.5 Peut-on vraiment parler de dépérimétrisation ?

En fait, ce qui transpire des exemples présentés, c'est surtout que ce que d'aucuns appellent dépérimétrisation n'a rien d'une dépérimétrisation. C'est surtout une repérimétrisation[14], c'est à dire une façon différente de penser le périmètre en fonction de problématiques nouvelles.

Avec, en particulier, l'abandon d'une partie du périmètre physique au profit de la mise en place d'un périmètre logique.

[14] Que les plus intègres adaptes de la langues françaises veuillent bien pardonner l'auteur pour ses excès de barbarismes...

4 Un futur pour la dépérimétrisation ?

Quand bien même la dépérimétrisation pose de nombreux problèmes, force est de constater que le concept présente de l'intérêt, en particulier au niveau de la gestion du réseau. En effet, la possibilité d'envisager un Internet à nouveau capable de jouer son rôle, c'est à dire acheminer l'information d'un point A à un point B sur l'ensemble du réseau, laisse entrevoir à des jours meilleurs y compris du point de vue de la sécurité réseau.

4.1 Le modèle de sécurité d'IPv6

Le modèle d'un réseau entièrement routable est celui que nous promet la mise en œuvre du protocole IPv6[2]. Il ne relève cependant pas du sujet de cet article de discuter de l'éventualité de l'avènement d'IPv6 qu'on nous promet depuis des lustres, mais seulement d'envisager un contexte dans lequel un fort relâchement des périmètres réseau pourrait prendre du sens. Le modèle de sécurité proposé par IPv6 repose essentiellement sur une sécurité assurée de bout en bout, avec authentificaton et chiffrement des communications par IPsec. Ce qui semble tout à fait cohérent avec les idées avancées par la dépérimétrisation, et permet en particulier de toujours considérer le réseau comme hostile par défaut. Ce qui est de toute façon conforme à la réalité dans la plupart des situations, et finira par l'être un jour dans les autres cas de figure... Ne serait-ce que parce que nul réseau n'est à l'abri d'une compromission...

Partant de l'hypothèse que le réseau n'est plus un environnement auquel on peut faire confiance, on va vouloir protéger ses communications. C'est précisément là que la routabilité totale proposée par IPv6 prend tout son sens. Là où IPv4 pêche de part l'existence même de la traduction d'adresses, IPv6 permet de simplifier considérablement la mise en place de liens de communication protégés et donc d'en augmenter considérablement la portée et l'efficacité. Considérant un ensemble d'hôtes appartenant à un ensemble donné, on crée, en appliquant authentification et chiffrement, par IPsec par exemple, à toutes leurs communications, un nuage de communication sécurisé au-dessus du réseau physique, quelle que soit leur localisation dans ce réseau.

4.2 Le concept d'overlay networks

Un *overlay network* est un réseau de communication logique établi au-dessus du réseau physique et indépendamment de lui, comme montré sur la figure 5. C'était l'idée initiale derrière les réseaux privés virtuels, terme aujourd'hui utilisé pour désigner des tunnels sécurisés permettant de transporter des communications entre deux points. Un excellent exemple d'*overlay network* est Hamachi[15]. Ce logiciel fonctionnant sur le modèle Peer-to-Peer permet la constitution de réseaux logiques permettant à tous les participants de communiquer librement quelle que soit leur localisation dans le réseau[16]. Le seul frein à ce type de fonctionnalité tient en fait à la capacité à établir et maintenir les communications nécessaires au bon fonctionnement du système.

Or, lorsqu'on est capable d'établir des liens chiffrés simplement, la réalisation d'un véritable réseaux privé virtuel sous forme d'*overlay networks* devient possible quel que soit l'environnement d'accueil du poste de travail. Ce qui veut dire que ce type d'accès peut immédiatement le mode de fonctionnement unique du poste de travail, quel que soit son environnement d'accueil et sa localisation physique.

[15] `https://secure.logmein.com/products/hamachi/vpn.asp`
[16] Ou presque...

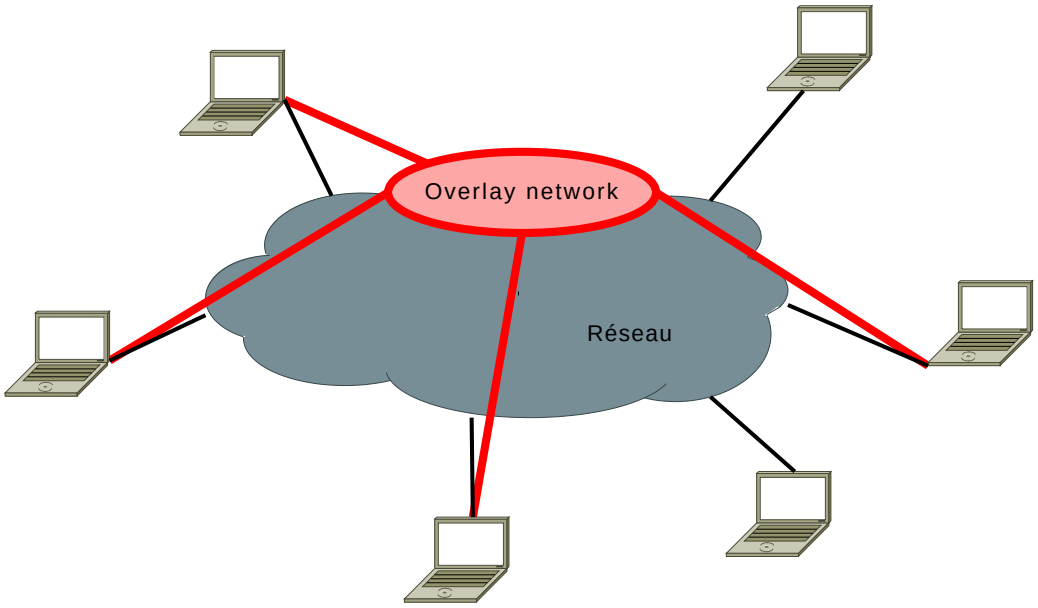

FIG. 5: Exemple d'overlay network au-dessus d'un réseau classique.

4.3 Mobile IPv6

En outre, un modèle de réseau entièrement routable et dépérimétrisé autorise non seulement la mise en place de fonctionnalités comme la mobilité, mais en plus de la sécuriser correctement. C'est par exemple le cas de Mobile IPv6[10] dont la standardisation commence à aboutir et les implémentations à devenir réellement utilisables, y compris au-dessus d'un accès IPv4 grâce à mécanismes de transition comme 6to4[3] ou Teredo[4].

Mobile IPv6 est une extension du protocole IPv6 permettant d'assurer la mobilité des hôtes au sein du réseau. Cette mobilité se traduit en pratique par l'attribution au nœud d'une adresse fixe indépendante de sa localisation sur laquelle il peut être joint dès lors qu'il est connecté. Cette fonctionnalité est à rapprocher du numéro de téléphone attribué à un abonnement GSM qui permet, pourvu que les options adhoc aient été souscrites, de joindre l'utilisateur quelle que soit sa localisation dans le monde. L'autre fonctionnalité intéressante associé à cette mobilité est la survie des connexions au changement de médium, autorisant le déplacement de l'hôte d'un réseau physique à un autre sans interruption des communications.

Comme illustré en figure 6, le nœud mobile négocie un lien IPsec avec un relai appelé *Home Agent* placé dans le réseau mère. Ce dernier est chargé de rediriger les communications à destination de l'adresse IP statique du nœud mobile vers son addresse IP physique courante. Le nœud mobile informe le Home Agent de ses changements d'adresse IP physique au moyen de messages appelé *Binding Updates* protégés.

En l'état actuel des travaux, Mobile IPv6 ne fonctionne qu'à travers le réseau mère, par le truchement du *Home Agent*. Ce mode de fonctionnement n'est certes pas optimal, mais il permet permet au nœud mobile d'établir des communications avec n'importe quel nœud du réseau IPv6, qu'il supporte ou non les extensions de mobilité. Des mécanismes d'optimisation sont en cours de

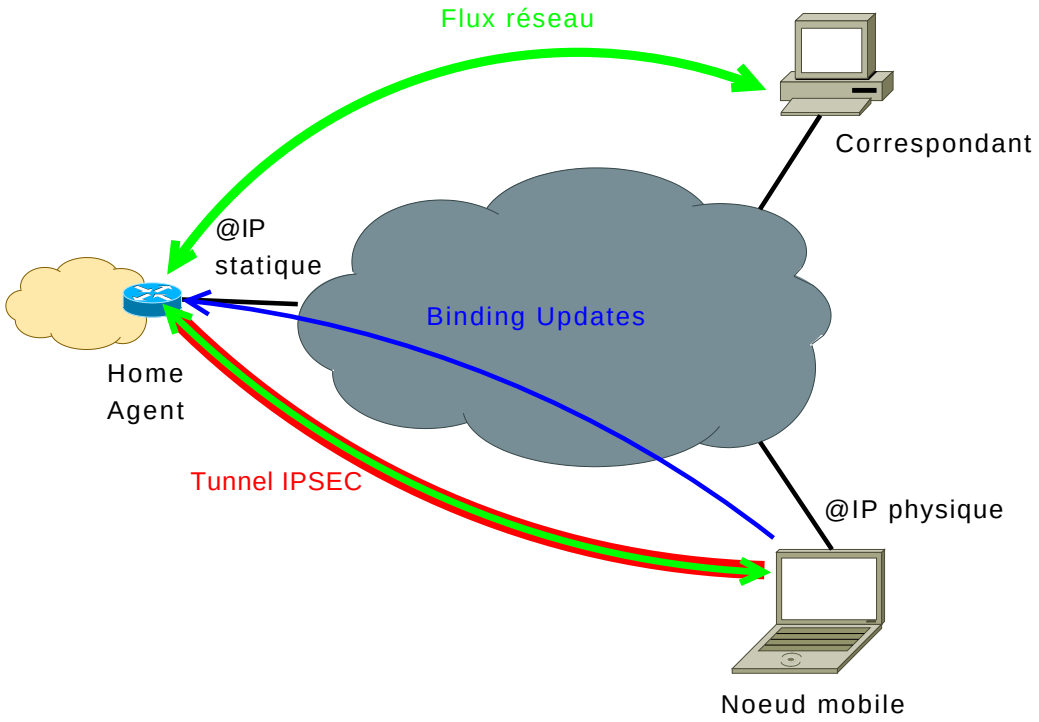

FIG. 6: Fonctionnement de Mobile IPv6.

développement pour permettre à deux nœuds supportant ces extensions de communiquer directement, sans avoir à passer par le *Home Agent*, fonctionnement aboutirait alors à un véritable *overlay network* de type *Peer-to-Peer*.

Dans ce mode, le premier paquet que les correspondants externes enverront transitera toujours pas le *Home Agent*. Cependant, lorsque le nœud mobile recevra ce paquet via le tunnel IPsec, il aura alors le choix de continuer la conversation sur ce mode, ou d'informer son correspondant de son adresse IP physique à l'aide d'un *Binding Update* pour continuer la communication en direct, comme illustré en figure 7.

Un hôte configuré pour fonctionner en Mobile IPv6 a donc la même vision du réseau où qu'il se trouve. Parallèlement, il est toujours joignable de la même manière par l'ensemble de l'infrastructure à laquelle il appartient du fait de la transparence des mécanismes de mobilité.

4.4 Et la dépérimétrisation dans tout ça ?

Considérant la dépérimétrisation comme une façon différente de penser les périmètres de sécurité, il pourrait bientôt être possible d'appliquer ce concept au niveau du réseau sans pour autant augmenter la surface d'exposition des éléments concernés par l'utilisation de mécanismes comme ceux précédemment décrits.

Reste que ces mécanismes n'adressent en rien les problèmes de sécurisation du système d'exploitation et des couches applicatives, puisque limités à la seule protection des flux réseau...

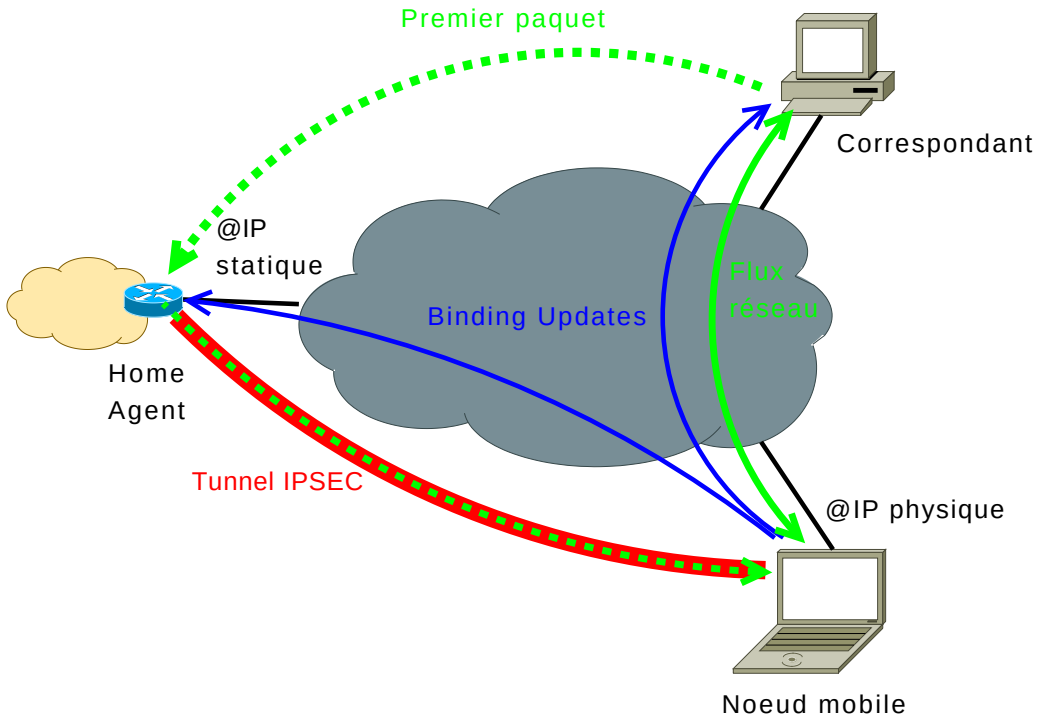

FIG. 7: Fonctionnement optimisé de Mobile IPv6.

5 Conclusion

Le concept de dépérimétrisation totale tel qu'on nous le présente généralement n'est clairement pas applicable aujourd'hui. L'infrastructure réseau telle que nous la connaissons aujourd'hui est beaucoup trop fragmentée et l'efficacité des mécanismes de sécurité n'est pas suffisante pour assurer l'autonomie totale d'un poste de travail. Il s'agit donc d'un doux rêve qui n'est pas prêt de se réaliser, en tout cas dans un futur proche.

En outre, ce modèle n'est pas applicable à l'intégralité du système d'information. Selon l'adage comme quoi les pare-feu ne seraient que la réponse des administrateurs réseau au problèmes de programmation, on pourrait se prendre à imaginer un monde idéal sans faille de programmation qui pourrait se passer de barrière. Mais d'une part ce monde idéal n'existe pas[17] et d'autre part la fonction du pare-feu n'est pas d'apporter une solution aux failles de programmation ! La pare-feu, dans sa fonction de compartimentation et de réduction de la surface exposée, reste tout à fait pertinent pour la protection de nombreuses ressources du système d'information.

Une approche plus raisonnée qu'on pourrait qualifier de repérimétrisation semble nettement plus pragmatique et bénéfique, parce que cohérente avec l'utilisation qui est aujourd'hui faite du

[17] Et n'existera probablement jamais.

réseau. En fait, l'argument du Jericho Forum comme quoi la dépérimétrisation serait inévitable[18] est très probablement vrai en ce qui concerne l'infrastructure réseau. L'explosion de la mobilité et des besoins de collaboratifs internes comme externes ne sera pas absorbable par un modèle uniquement périmétrique. Il est donc nécessaire d'envisager la sécurité réseau différemment pour les parties concernées du système d'information.

En fait, il est raisonnable de penser que le discours sur la dépérimétrisation soit volontairement extrême, dans le but de faire réfléchir les gens sur la manière d'envisager la sécurité dans un contexte qui a profondément changé ces dix dernières années.

Références

1. Y. Rekhter, B. Moskowitz, D. Karrenberg, GJ. de Groot, E. Lear : RFC 1918 - Address Allocation for Private Internets. IETF (1996)
`http://tools.ietf.org/html/rfc1918`
2. S. Deering, R. Hinden : RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification. IETF (1998)
`http://tools.ietf.org/html/rfc2460`
3. B. Carpenter, K. Moore : RFC 3056 - Connection of IPv6 Domains via IPv4 Clouds. IETF (2001)
`http://tools.ietf.org/html/rfc3056`
4. Microsoft : Teredo Overview. Microsoft TechNet Library (2003)
`http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/teredo.mspx`
5. C. Blancher : Atouts et limites des pare-feu personnels. SSTIC 2003
`http://actes.sstic.org/SSTIC03/Firewalls_personnels/`
6. C. Blancher : Mobilité, quand tout ordinateur peut devenir cheval de Troie. SSTIC 2004
`http://actes.sstic.org/SSTIC04/Mobilite/`
7. G. Wearden : BP declares war on the LAN. ZDNet UK (2006)
`http://news.zdnet.co.uk/security/0,1000000189,39253439,00.htm`
8. J. Cache, D. Maynor : Device Drivers. Black Hat US 2006
`http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Cache.pdf`
9. D. Hulton : Cardbus Bus-Mastering : 0wning the Laptop. Shmoocon 2006
`http://www.shmoocon.org/2006/presentations.html`
10. A. Ébalard, G. Valadon : La sécurité dans Mobile IPv6. SSTIC 2006
`http://actes.sstic.org/SSTIC06/Securite_MIPv6/`
11. A. Boileau : Hit by a Bus : Physical Access Attacks with Firewire. Ruxcon 2006
`http://www.ruxcon.org.au/files/2006/firewire_attacks.pdf`
12. K. Finistere, T. Zoller : Bluetooth Hacking revisited. Hack.lu 2006
`http://2006.hack.lu/images/7/70/Zoller_hack_lu_2006.pdf`
13. C. Saran : ICI set for big savings by switching internet traffic to DSL. ComputerWeekly.com (2006)
`http://www.computerweekly.com/Articles/Article.aspx?liArticleID=220002`
14. L. Butti, J. Tinnes : Recherche de vulnérabilités dans les drivers 802.11 par techniques de fuzzing. SSTIC 2007
`http://actes.sstic.org/SSTIC07/WiFi_Fuzzing/`
15. S. Duverger : Exploitation en espace noyau sous Linux 2.6. SSTIC 2007
`http://actes.sstic.org/SSTIC07/Exploitation_Espace_Noyau/`

[18] "Like it or not deperimeterisation will happen ; the business drivers already exist within your organisation, it's already started and it's only a matter of how fast, how soon and whether you decide to control it" [31]

16. N. Dubée : VoIP, une opportunité pour la sécurité ? SSTIC 2007
`http://actes.sstic.org/SSTIC07/VOIP_Opportunite_Securite/`

17. JP. Kamath : KLM to save £2m through laptop self-support plan. ComputerWeekly.com (2007)
`http://www.computerweekly.com/Articles/Article.aspx?liArticleID=225574`

18. S. Alvarez, T. Zoller : The death of defense in depth ? (Revisiting AV software). Hack.lu 2007
`http://hack.lu/index.php/List#The_death_of_defense_in_depth.3F_Revisiting_AV_software.29`

19. C. Blancher : Authenticated Access to Network, Are Identity-based Security Schemes Going to Save Our LANs ? Bellua Cyber Security Asia 2007
`http://sid.rstack.org/pres/0710_BCS_NetworkAuth.pdf`

20. P. Simmonds : The Business Case for removing your perimeter Deepsec 2007
`http://wiki.deepsec.net/images/e/ea/Deepsec2007_Simmonds-Keynote.pdf`

21. N. Ruff, M. Suiche : Enter Sandman (why you should never go to sleep). Pacsec 2007
`http://dragos.com/PacSec2007/psj07ruffsuiche-en.pptx`

22. Microsoft : Vulnérabilité liée au traitement des protocoles TCP/IP/IGMPv3 et MLDv2 dans le noyau Windows. Microsoft TechNet - Bulletins de sécurité (2008)
`http://www.microsoft.com/france/technet/security/bulletin/ms08-001.mspx`

23. A. Jaquith : Not Dead But Twitching - Antivirus Succumbs to the Scourge of Modern Malware. Source Boston 2008

24. S. Eren : Information Operations Source Boston 2008
`http://www.immunitysec.com/downloads/SinanEren_BHFED2008.pdf`

25. C. Blancher : De-perimeterization, Dream or Nightmare for Network Security ? Source Boston 20008
`http://sid.rstack.org/pres/0803_Source_Deperimetrisation.pdf`

26. JA. Halderman, SD. Schoen, N. Heninger, W. Clarkson, W. Paul, JA. Calandrino, AJ. Feldman, J. Appelbaum, EW. Felten : Lest We Remember : Cold Boot Attacks on Encryption Keys.
`http://citp.princeton.edu/memory/` (2008)

27. Jericho Forum : Jericho Forum Commandments.
`http://www.opengroup.org/jericho/commandments_v1.1.pdf` (2006)

28. Jericho Forum : Position Paper - VoIP in a de-perimeterised world
`http://opengroup.org/jericho/VoIP_v11.0.pdf` (2006)

29. Jericho Forum : Position Paper - Wireless in a de-perimeterised world
`http://opengroup.org/jericho/Wireless_v1.0.pdf` (2006)

30. Jericho Forum : Position Paper - End Point Security
`http://opengroup.org/jericho/EPS_v1.0.pdf`

31. Jericho Forum : Business rationale for de-perimeterisation.
`http://www.opengroup.org/jericho/Business_Case_for_DP_v1.0.pdf` (2007)

32. Jericho Forum : Publications.
`http://opengroup.org/jericho/publications.htm`