

Comment bâtir une architecture de sécurité Internet ?

Hervé Schauer et Olivier Perret
Herve.Schauer@hsc.fr, Olivier.Perret@ensta.fr

Octobre 1995

Résumé

L'objectif de notre conférence est, d'une part, de montrer pourquoi les produits de sécurité Internet ne sont pas nécessaires aux universités, et d'autre part de proposer une architecture leur permettant de se protéger.

Les produits de sécurité qui fleurissent sur le marché, sont peu souples voire incomplets, et rendent en réalité l'exploitation de la sécurité Internet aussi complexe qu'auparavant.

Il s'agit donc d'apprendre à utiliser des composants classiques et standards du marché : routeurs et machines Unix, pour bâtir une sécurité, adaptée aux besoins des utilisateurs tout en améliorant la résistance aux intrusions qui se multiplient. La conférence proposera une architecture, des matériels applicables à tous, et les règles de filtrage IP.

Les schémas et références bibliographiques sont disponibles sur le Web.

1 Les principes de base

Les concepts de base sur lesquels s'articule une architecture de sécurité Internet sont le filtrage IP et le relayage des services, qu'il convient de bien distinguer.

1.1 Le filtrage IP

C'est lui qui permet de filtrer le trafic à la base, de part et d'autre d'un routeur ou d'une machine reliée à deux réseaux. Ce filtrage portera sur les communications en général, sans distinction de service.

Il peut être simple ou double selon qu'il est assuré par une machine ou une machine associée un routeur. Dans le cas où l'on dispose de 2 machines, l'une assurera le relayage des services et le contrôle du routage et sera branchée sur un brin propre et filtré tandis que l'autre assurera le filtrage.

Le filtrage est pour le moment une opération complexe demandant une bonne connaissance du protocole TCP/IP. On vend d'ailleurs des produits de sécurité dont la seule fonction est d'offrir une

interface graphique de configuration du routage IP. Mais, depuis que le filtrage se généralise, des outils de génération automatique de filtres, sont sur le point d'apparaître. Ils utiliseront un langage de description simple et limiteront ainsi les risques de fausse manœuvre que l'on rencontre avec les interfaces graphiques. De plus, en formalisant avec un langage de description, on pourra envisager la vérification du contenu des filtres.

Le routeur devient donc un élément indispensable de la sécurité. Il remplit véritablement une fonction à ce niveau, qu'il faut distinguer de sa fonction traditionnelle de communication avec l'extérieur ou de constituant du réseau privé. Il est du même coup plus utilisé, mieux maîtrisé et donc plus exposé aux agressions et au détournement de ses propres failles. D'où l'intérêt de placer les autres fonctions de sécurité (relayage, authentification,...) sur une autre machine.

1.2 Le relayage des services

Le relayage des services est assuré par des démons sur une machine. Pour chaque service, ils assurent à la fois les fonctions client et serveur auxquelles ils ajoutent essentiellement des fonctions d'authentification et de filtrage de contenu.

Leur but est de centraliser les requêtes de la façon la plus transparente possible pour faciliter le contrôle de l'authentification et l'audit. Il s'agit donc d'ouvrir des services sous contrôle, contrairement au filtrage dont l'usage est plutôt d'interdire des services incontrôlables.

Le principe du relayage est utilisé par certains services depuis leur origine. C'est le cas du mail (SMTP), des news (NNTP) du serveur de noms (BIND), ou de l'heure (NTP). L'idée d'utiliser le relayage à des fins de sécurité est récente (Usenix 1992), mais a séduit immédiatement les développeurs, en particulier sur les nouveaux services comme HTTP (utilisé sur le World Wide Web). Il a aussi été intégré dans *telnet*, *ftp* et *XWindow*, et moyennant certaines contraintes dans *lpd* (*impression*), *archie* (*recherche de fichiers*), *ping*, *finger*, *whois* et quelques SGBD de type client/serveur.

Il est bien entendu que dans cette étude le relayage n'apporte de la sécurité que s'il offre une possibilité d'authentification. Les nombreux avantages du relayage exploités par des services comme NIS, les serveurs de licences, le Mbone, les RPC et les services UDP en général ne relèvent pas de la sécurité. C'est d'ailleurs un problème pour ces services; le relayage n'est donc pas une fin en soi.

1.3 Avantages de la séparation des tâches

L'avantage d'utiliser un démon est qu'il permet d'utiliser une procédure d'authentification plus souple ou plus performante que celle du système d'exploitation.

L'avantage de centraliser les services et le filtrage sur une ou deux machines est de faciliter le contrôle du flux, de son volume comme de son contenu. Sur un relais WWW, on pourra par

exemple utiliser un cache qui garde une copie des pages fréquemment consultées ce qui améliorera les performances.

L'avantage de séparer le filtrage et le relayage sur deux machines est d'une part de soulager une machine qui aurait à assurer les deux tâches, et d'autre part de n'exposer à l'extérieur qu'une machine au système limité n'ayant pas de faille connue ou difficile à détourner (routeur sans OS classique), obligeant le pirate à s'attaquer au logiciel de relayage dont le source est connu.

Dans tous les cas, l'administration de la sécurité du réseau est restreinte à une ou deux machine et peut donc facilement être déléguée. Elle permet aussi de distinguer facilement l'autorisation d'accès au réseau local, parfois bâclée, de l'autorisation d'accès à Internet, plus sensible et moins urgente. On pourra plus facilement imposer la signature d'une charte d'utilisation.

Du point de vue de l'administrateur de sécurité, le fait de centraliser ses tâches sur quelques machines lui permet de garantir la sécurité sans s'inquiéter de l'activité des utilisateurs sur le réseau local et de l'état de leur machine. On constate en effet que les intrusions passent souvent par des machines mal administrées ou nouvellement installées.

2 Les produits existants

2.1 Disponibilité

Les produits existants sont essentiellement américains ou canadiens. Leur disponibilité en Europe est donc très variable. Le support technique encore plus.

2.2 Adéquation au besoin

Ces produits correspondent généralement à un des composants d'une solution de sécurité Internet;

- Soit ils assurent le paramétrage d'un routeur ou d'une machine utilisée comme telle.
- Soit ils contiennent des logiciels de relayage.

Malheureusement, ils répondent rarement à ces deux besoins. On trouve ainsi de bons logiciels de configuration de filtre qui n'offrent aucun service de relayage. Ce ne sont que des interfaces graphiques de configuration de routeurs. Quand ils ne font vraiment que ça, on les appelle des cliquodromes, car leur seul intérêt est de permettre à l'opérateur de cliquer au lieu de taper une commande. A moins d'être cliquomane, ces logiciels sont à éviter car en cas de fausse manœuvre, il est beaucoup plus difficile d'évaluer les conséquences d'un cliquage, dont on connaît mal l'étendue que d'une commande classique et documentée.

On peut la rapprocher de ce classique de l'administration système : La différence entre les dégâts provoqués par un incompetent et ceux d'un pirate est que le pirate, lui connaît leur étendue.

À l'opposé, les bons produits de relayage sont souvent difficiles à configurer pour un néophyte. Ils nécessitent en fait une connaissance certaine du routage IP et des problèmes techniques de sécurité.

2.3 Limites

La plupart des logiciels commerciaux ne sont disponibles qu'en binaire. C'est déjà difficilement acceptable pour des logiciels dédiés à la sécurité ; c'est encore plus délicat quand on sait que la plupart de ces logiciels sont importés.

Mais d'une manière générale, la faiblesse d'un garde-barrière clef en main, c'est qu'il ne résoudra jamais le problème de l'organisation de la sécurité. Il faut pour cela une méthodologie globale comprenant un cycle d'analyse, de décision et de formation des utilisateurs, qui doit correspondre à la « Politique de Sécurité Informatique » du site ».

3 Méthodologie globale

Une solutions complète doit donc intégrer :

- Le filtrage IP ;
- Le relayage applicatif avec authentification ;
- La méthodologie d'exploitation.

3.1 La méthodologie de mise en place et d'exploitation

C'est elle qui formalise l'exploitation de la solution de sécurité Internet. Elle précisera en particulier quels sont les filtrages à effectuer, d'où découleront les règles de filtrage et directement les tables de routage.

Elle précisera aussi les services autorisés et les conditions d'accès à ces services, ce qui correspond à la liste des relais et à leur configuration. C'est elle qui décidera du type des systèmes d'authentification utilisés (mot de passe à usage unique ou mot de passe classique)

De plus elle permet de garantir le maintien de la sécurité dans le temps, grâce à des procédures d'agrément et de contrôle.

3.2 Pérennité de la sécurité

La sécurité s'amenuit naturellement au fil du temps. En plus de la lassitude naturelle ses exécutants sont confrontés souvent à des risques inconnus : A chaque nouvelle version de machine,

à chaque modification de la configuration. Il est donc impératif de planifier des contrôles parmi ceux qui sont possibles sur la machine, dont :

- vérification des filtres, et de la liste des relais ;
- mise à jour des listes d'utilisateurs (autorisations) ;
- surveillance des mots de passe (crackage, ancienneté...) .

Ces contrôles seront d'autant plus efficaces que leur déclenchement sera automatique (l'ordinateur ne se lasse jamais), relativement aléatoire (imprévisible par les pirates), et autoritaire (prioritaire au niveau système). Mais ce n'est jamais à la machine de le décider.

3.3 La décision de la sécurité

Enfin l'une des graves erreurs vis-à-vis de la sécurité informatique est de croire que la machine se suffit à elle-même et qu'elle doit assurer sa propre sécurité ou au moins celle de ces utilisateurs. C'est négliger que la sécurité est l'affaire de ses utilisateurs qui doivent rester libres de fixer les règles d'utilisation de leurs machines. Dans une entreprise, c'est l'objet de la politique de sécurité informatique de l'entreprise, qui ne peut être acceptée que si elle émane directement de sa direction.

Conclusion

Depuis longtemps, les systèmes ouverts offrent aux utilisateurs tous les éléments de base de la sécurité (contrôle d'accès discrétionnaire, audit, relayage, ...) Il leur manquait une certaine adaptation aux besoins des utilisateurs au niveau de la configuration et de l'administration pour en faire des outils de sécurité. Ces outils sont maintenant disponibles.

Cependant, les outils de sécurité Internet commerciaux ne correspondent guère aux besoins des réseaux d'enseignement et de recherche car ils répondent aux besoins d'utilisateurs peu expérimentés (pas de relayage mais beaucoup de filtrage) ou ayant peu de besoins (peu de filtrage, mais beaucoup de relayage de services existants), ce qui n'est pas leur cas.

En revanche, en définissant clairement l'usage qu'il veulent faire d'Internet par une politique de sécurité, et en utilisant les outils de filtrage et de relayage qui existent depuis quelques années, ils ont les moyens de mettre en place une sécurité satisfaisante, qui protège leurs utilisateurs sans les priver de leur outil de travail.