La sécurité des réseaux

(c) Guillaume Desgeorge 2000
guill@guill.net
http://www.guill.net/

Pourquoi les systèmes sont-ils vulnérables?
Les mécanismes de sécurité sur un exemple de réseau
Cryptographie : chiffrement et signature
Le commerce électronique
Les firewalls
Les serveurs proxy
Les VPN
Les systèmes de détection d'intrusions

Pourquoi les systèmes sont vulnérables

Cette page est inspirée entre autre d'un article de Dorothy Denning qui s'appelle " Protection and defense of intrusion " et qui a valeur de référence dans le domaine de la sécurité des réseaux.

Qu'est que la sécurité ?

Faire de la sécurité sur un réseau consiste à s'assurer que celui qui modifie ou consulte des données du système en a l'autorisation et qu'il peut le faire correctement car le service est disponible.

Quelques chiffres

Après un test de 12 000 hôtes du Département de la défense américaine, on retient que 1 à 3% des hôtes ont des ouvertures exploitables et que 88% peuvent être pénétrés par les relations de confiance.
Notons que seules 4% de ces attaques sont détectés et que 5% de ces 4% sont rapportées.
Enfin, notons que le nombre de voleurs d'informations a augmenté de 250% en 5 ans, que 99% des grandes entreprises rapportent au moins un incident majeur et que les fraudes informatiques et de télécommunication ont totalisés 10 milliards de dollars pour seuls les Etats-Unis.
1290 des plus grandes entreprises rapportent une intrusion dans leur réseau interne et 2/3 d'entre elles à cause de virus.

Pourquoi les systèmes sont vulnérables ?

- La sécurité est cher et difficile. Les organisations n'ont pas de budget pour ça.
- La sécurité ne peut être sûr à 100%, elle est même souvent inefficace.
- La politique de sécurité est complexe et basée sur des jugements humains.
- Les organisations acceptent de courir le risque, la sécurité n'est pas une priorité.
- De nouvelles technologies (et donc vulnérabilités) émergent en permanence.
- Les systèmes de sécurité sont faits, gérés et configurés par des hommes (errare humanum est !).
- Il n'existe pas d'infrastructure pour les clefs et autres éléments de cryptographie.
- L'état interdit la cryptographie dans certains cas (exportation, par exemple) dans certains pays, ce qui empêche

le cryptage systématique au niveau du système d'exploitation.

Pourquoi un système ne peut être sûr à 100%

Il est impossible de garantir la sécurité totale d'un système pour les raisons suivantes :
- Les bugs dans les programmes courants et les systèmes d'exploitation sont nombreux.
- La cryptographie a ses faiblesses : les mots de passe peuvent être cassés.
- Même un système fiable peut être attaqué par des personnes abusant de leurs droits.
- Plus les mécanismes de sécurité sont stricts, moins ils sont efficaces.
- On peut s'attaquer aux systèmes de sécurité eux-mêmes…

Méthodes utilisées pour les attaques

- La négligence interne des utilisateurs vis à vis des droits et autorisations d'accès.
- Se faire passer pour un ingénieur pour obtenir des infos comme le mot de passe.
- Beaucoup de mot de passe sont vulnérables à une attaque systématique.
- Les clefs de cryptographie trop courtes peuvent être cassées.
- L'attaquant se met à l'écoute sur le réseau et obtient des informations.
- IP spoofing : changer son adresse IP et passer pour quelqu'un de confiance.
- Injecter du code dans la cible comme des virus ou un cheval de Troie.
- Exploitation des faiblesses des systèmes d'exploitation, des protocoles ou des applications.

Outils des attaquants

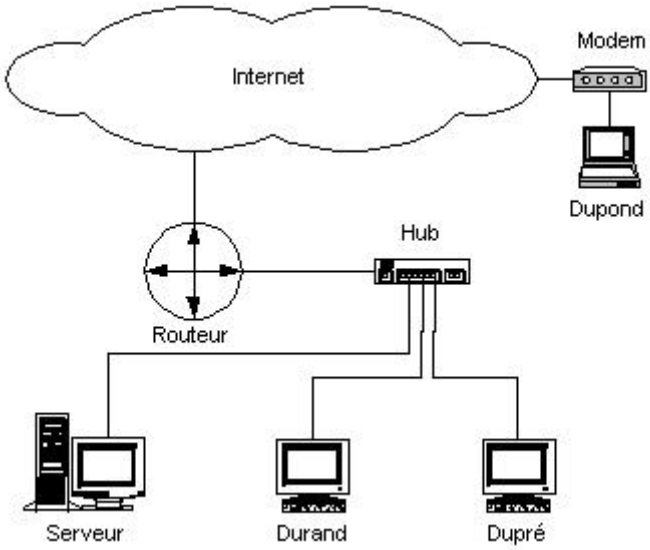
- Programmes et scripts de tests de vulnérabilité et d'erreurs de configuration (satan).
- Injection de code pour obtenir l'accès à la machine de la victime (cheval de Troie).
- Echange de techniques d'attaques par forums et publications.
- Utilisation massive de ressources pour détruire des clefs par exemple.
- Les attaquant utilisent des outils pour se rendre anonyme et invisible sur le réseau.

Principales technologies de défense

- Authentification : vérifier la véracité des utilisateurs, du réseau et des documents.
- Cryptographie : pour la confidentialité des informations et la signature électronique.
- Contrôles d'accès aux ressources (physiquement aussi).
- Firewalls : filtrage des trames entre le réseau externe et le réseau interne.
- Audit : études des fichiers de log pour repérer des anomalies.
- Logiciels anti-virus (2/3 des attaques sont des virus).
- Programmes de tests de vulnérabilité et d'erreurs de configuration (satan).
- Détection d'intrusion : détection des comportements anormaux d'un utilisateur ou des attaques connues.

Exemple pour la sécurité

Cette page essaie, par un exemple concret et volontairement très simple, de montrer les menaces qui pèsent sur un réseau et les méthodes pour minimiser ces menaces. On va étudier le réseau classique suivant :



Description du réseau à sécuriser

Nous avons un réseau d'entreprise, comportant un routeur, permettant l'accès à Internet. Sous ce routeur se trouve le réseau interne, composé simplement d'un hub, reliant un serveur et des stations de travail. Sur ce serveur se trouve des informations sensibles qui pourrait intéresser l'espion d'une autre entreprise. On y trouve aussi des bases de données utilisées par plusieurs employés dans diverses applications, comme Durand et Dupond. Dupond est un commercial qui sillonne la France. Il peut se connecter au serveur de n'importe où grâce à Internet.

Identifier les informations à protéger

Le serveur contient des informations sensibles : si personne ne consulte régulièrement ces informations, il n'y a aucune raison de les laisser sur le serveur connecté au réseau... Il ne faut pas tenté le diable, et les informations confidentielles ne resteront sur le réseau qui si c'est nécéssaire!
Une base de données est utilisée par plusieurs employés mais contient des informations confidentielles. Dans ce cas, le serveur doit garder ces informations. Il faudra mettre sur le serveur un sérieux contrôle d'accès pour assurer l'authentification des utilisateurs qui ont besoin de ces données. Les autres requêtes seront rejetées, même si elles proviennent d'employés de l'entreprise. Chaque ordinateur ne sera accessible qu'avec un login et un mot de passe.
Le serveur contient des informations confidentielles : il faut que le serveur soit physiquement protégé... Rien ne sert de sécurisé le réseau pour empêcher l'espionnage si quelqu'un peut s'emparer du disque dur!

Politique de sécurité

Une fois que les informations sensibles sont repérées, il s'agit de choisir une politique de sécurité. On fait du café, on s'installe dans la belle salle de réunion, et on discute... pour se mettre d'accord sur la politique de sécurité : on choisit ce qui est autorisé et ce qui est interdit. Les outils mis en place par la suite respecteront cette politique de sécurité, et devront même la refléter.

Sensibilisation des utilisateurs

Une politique de sécurité doit se faire avec les utilisateurs : ils doivent comprendre cette politique et respecter un certain nombre de règle en relation avec cette politique. Par exemple, il parait évident qu'ils ne doivent communiquer leur login et mot de passe à personne, pas même leurs collègues. De même, il est bien connu qu'il ne faut pas ouvrir les fichiers attachés au email venant de personnes inconnus où dont le contenu est suspect. Des notes d'informations devront sensibiliser les utilisateurs. Ces règles s'appliquent à tous, y compris à l'administrateur du réseau...

Les virus

Deux tiers des attaques se font par virus : chaque poste doit disposé d'un logiciel anti-virus mis à jour régulièrement!
Les virus se transmettent principalement par disquettes, mais peuvent aussi se faire par mail. Les fichiers les plus susceptibles d'en contenir sont bien sûr les éxécutables (.com, .exe), mais également tous les documents pouvant contenir des macros (Microsoft Office est un nid à virus! Méfiez-vous surtout des macros Word)...

Sécurité minimum

Tout ceci est le minimum en matière de sécurité. Ils ne coutent quasiment rien. On les reprend un par un :
- authentification des utilisateurs par login et mot de passe.
- suppression des informations confidentielles des machines reliées au réseau si elles n'ont pas besoin d'y être.
- protection physique des machines contenant des informations sensibles (locaux fermés à clef).
- contrôle pour l'accès aux informations sensibles, avec un login délivré uniquement pour ceux qui en ont besoin.
- sensibilisation des utilisateurs aux problèmes de sécurité.
- installation d'un logiciel anti-virus à jour sur chaque poste.

Le problème des accès distants

Les données qui circulent sur Internet peuvent, à priori être vues de tous. Cela dit, il faut voir si quelqu'un irait jusqu'à écouter le réseau pour obtenir les informations manipulées par Dupond. Pour sécuriser la liaison, même en passant par Internet, il faut utiliser ce qu'on appelle un VPN. Avec une liaison VPN (Virtual Private Network), les données sont chiffrées, et personne, à priori, ne peut les lire. Tous ce passe exactement comme si Dupond étant directement connecté à l'entreprise sans passer par Internet, d'où le nom de réseau privé virtuel.

Firewall et proxy

Afin d'éviter que des attaques puissent venir d'internet par le routeur, il convient d'isoler le réseau interne de l'entreprise. La méthode la plus connue est le firewall et le serveur proxy, mais il n'y a pas que ça... Par exemple, sur les routeurs, il est possible de faire du filtrage de paquets ou de la translation d'adresse pour qu'une personne de l'extérieur ne puisse ni accéder, ni voir ce qu'il y a à l'intérieur.
Un firewall est une entité qui fait cette opération de filtrage. On va pouvoir analyser les données qui rentre et les interdire si elles ne proviennent pas de quelqu'un de connu ou si elles ne répondent pas à une requête interne. Le firewall, placé à l'entrée du réseau, constitue ainsi un unique point d'accès par où chacun est obligé de passer...
Le serveur Proxy, lui, permet de faire le relais au niveau des applications pour rendre les machines internes invisibles à l'extérieur. Si personne à l'extérieur ne peut voir les machines internes, l'attaques est beaucoup plus difficile, car l'attaquant est aveugle! N'oubliez quand même pas que 80% des attaques proviennent de l'intérieur du réseau et non de l'extérieur...

Logiciel de détection systématique d'erreurs

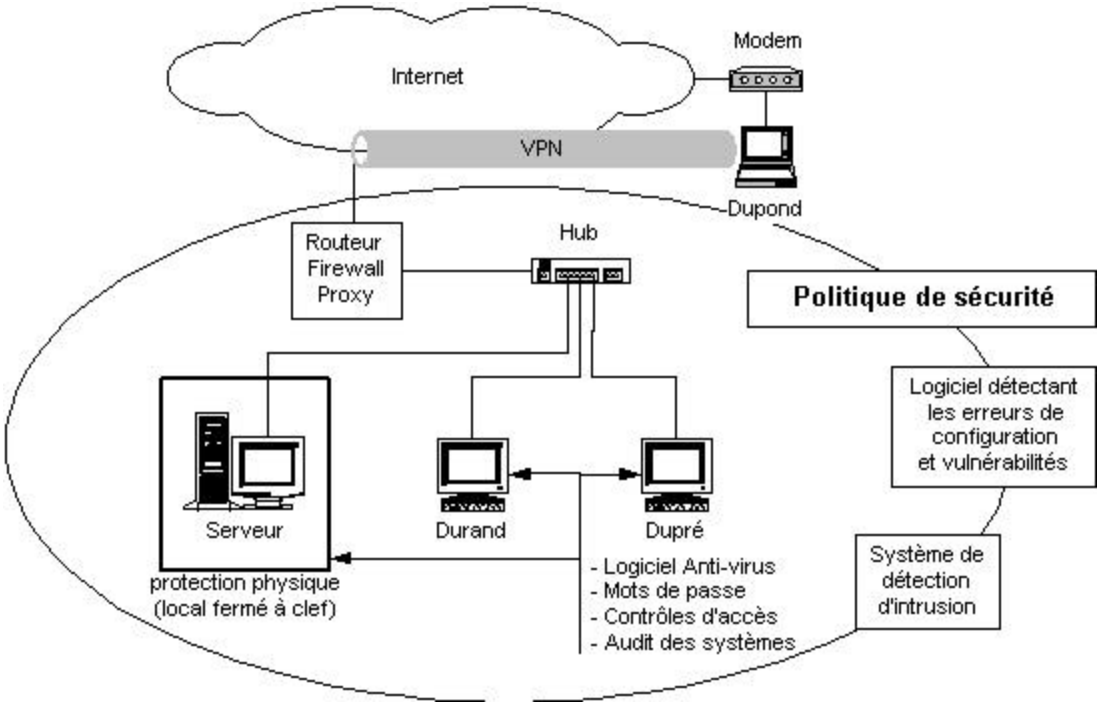
Les pirates utilisent des logiciel de test de la configuration pour repérer les failles du système qu'ils attaquent. Je ne citerai ici que Cops et Satan. Ces logiciels permettent de façon automatique de chercher les erreurs de configuration ou les vulnérabilités du système. Si vous les utilisez avant le pirate et que vous réparez ces failles, ce sera moins facile pour lui!

Système de détection d'intrusions

Enfin, une fois que tout cela est en place, si vraiment vous êtes paranoïaques, vous pouvez utiliser un logiciel de détection d'intrusions. Comme pour une alarme dans une maison, ce logiciel émet une alarme lorsqu'il détecte que quelqu'un de non-autorisé est entré sur le réseau.
A l'heure actuelle, ces logiciels sont encore remarquablement inefficace car ils passent leur temps à crier au loup alors qu'il n'y a personne dans la bergerie...

Après sécurisation

Voilà ce que ça donne, mais ne vous fiez pas aux apparences : quelqu'un qui a décidé d'entrer...



Cryptographie : chiffrement et signature

Le chiffrement

Le chiffrement des données fut inventé pour assurer la confidentialité des données. Il est assuré par un système de clé (algorithme) appliqué sur le message. Ce dernier est décryptable par une clé unique correspondant au cryptage.

Il existe à l'heure actuelle deux grands principes de cryptage : le cryptage symétrique basé sur l'utilisation d'une clé privée et le cryptage asymétrique qui, repose sur un codage à deux clés, une privée et l'autre publique.

Le cryptage symétrique

Le cryptage à clé privé ou symétrique est basé sur une clé (ou algorithme) partagée entre les deux parties communicantes. Cette même clé sert à crypter et décrypter les messages. Les algorithmes de chiffrement les plus connus sont : Kerberos, DES (Data Encryption Standard) et RSA.

Le principal problème est le partage de la clé : Comment une clé utilisée pour sécuriser peut être transmise sur un réseau insécurisé ? La difficulté engendrée par la génération, le stockage et la transmission des clés (on appelle l'ensemble de ces trois processus le management des clés : key management) limite le systèmes des clés privées surtout sur Internet.

Pour résoudre ces problèmes de transmission de clés, les mathématiciens ont inventé le cryptage asymétrique qui utilise une clé privée et une clé public.

Le cryptage asymétrique

Ce système de cryptage utilise deux clés différentes pour chaque utilisateur : une est privée et n'est connue que de l'utilisateur ; l'autre est publique et donc accessible par tout le monde.
Les clés publique et privée sont mathématiquement liées par l'algorithme de cryptage de telle manière qu'un message crypté avec une clé publique ne puisse être décrypté qu'avec la clé privée correspondante. Une clé est

donc utilisée pour le cryptage et l'autre pour le décryptage.

Ce cryptage présente l'avantage de permettre le placement de signatures numériques dans le message et ainsi permettre l'authentification de l'émetteur.

Le principal avantage du cryptage à clé publique est de résoudre le problème de l'envoi de clé privée sur un réseau non sécurisé. Bien que plus lent que la plupart des cryptage à clé privée il reste préférable pour 3 raisons :
- Plus évolutif pour les systèmes possédant des millions d'utilisateurs
- Authentification plus flexible
- Supporte les signatures numériques

Signature

Dans toute transaction professionnelle, les deux parties doivent offrir une garantie de leur identité. La signature numérique et le certificat sont des moyens d'identification de l'émetteur du message.

Signature numérique

Le principe de la signature numérique consiste à appliquer une fonction mathématique sur une portion du message. Cette fonction mathématique s'appelle fonction de hachage et le résultat de cette fonction est appelé code de hachage. Ce code fait usage d'emprunte digitale du message. Il faut noter que la fonction est choisie de telle manière qu'il soit impossible de changer le contenu du message sans altérer le code de hachage.

Ce code de hachage est ensuite crypté avec la clé privée de l'émetteur et rajouté au message. Lorsque le destinataire reçoit le message, il décrypte ce code grâce à la clé publique de la source puis il compare ce code à un autre code qu'il calcule grâce au message reçu. Si les deux correspondent, le destinataire sait que le message n'a pas été altéré et que son intégrité n'a pas été compromise. Le destinataire sait aussi que le message provient de l'émetteur puisque seul ce dernier possède la clé privée qui a crypté le code.

Ce principe de signature fût amélioré avec la mise en place de certificats permettant de garantir la validité de la clé public fourni par l'émetteur.

Les certificats

Pour assurer l'intégrité des clés publiques, les clés publiques sont publiées avec un certificat. Un certificat (ou certificat de clés publiques) est une structure de données qui est numériquement signée par une autorité certifiée (CA : Certification Authority) – une autorité en qui les utilisateurs peuvent faire confiance. Il contient une série de valeurs, comme le nom du certificat et son utilisation, des informations identifiant le propriétaire et la clé publique , la clé publique elle même , la date d'expiration et le nom de l'organisme de certificats. Le CA utilise sa clé privée pour signer le certificat et assure ainsi une sécurité supplémentaire.

Si le récepteur connaît la clé publique du CA, il peut vérifier que le certificat provient vraiment de l'autorité concernée et est assuré que le certificat contient donc des informations viables et une clé publique valide.

Commerce électronique et paiement en ligne

Le commerce électronique

Le commerce électronique, qui existait déjà avec le minitel à partir de 1980, vit avec Internet un véritable essor. Il s'agit de toutes les transmissions de données pour des activités commerciales.

Les enjeux économiques pour ce type d'opérations, et notamment la vente en ligne, sont très importants. On estime, dans le monde, qu'il y a 550 millions d'internautes pour un chiffre d'affaire lié au commerce électronique de

7 milliards de dollars. Sur 250 000 sites, 100 000 ont un but commercial !

On retrouve sur Internet, et dans la vente en ligne, les mêmes acteurs que dans la vie : le commerçant, qui veut être payé, le consommateur, qui veut payer sans crainte et simplement, et la banque, qui se veut garant de la bonne marche des opérations. Les produits qui fonctionnent le mieux (enquête de février 1997) sont les produits informatiques, les livres, CD et vidéos, et tout ce qui touche aux voyages et loisirs.

Généralement, les sites de vente mettent en ligne une description du produit et des photos (comme une vitrine), et propose une commande en ligne avec plusieurs moyens de payement… C'est justement l'aspect payement qui est le point sensible de l'échange.

Le problème du paiement sur Internet

Les paiements sont notamment limités par les lois du pays qui n'autorisent pas forcement le libre chiffrement des informations (c'est le cas en France). Les internautes sont encore très frileux pour la consommation sur Internet, car ils ne savent pas ce qu'on fait de leur numéro de carte de crédit lorsqu'ils le donnent, et ont peur que quelqu'un d'autre ne le récupère.

En règle général, les sites de vente propose soit un paiement traditionnel (par chèque), soit un paiement en ligne (par carte de crédit). Les inconvénients du paiement traditionnel est évident en terme de délais et d'échange de devises avec les pays étrangers.

Deux possibilités existent pour le paiement en ligne. La première possibilité est le porte-monnaie électronique, qui est géré par un organisme tiers et qui correspond à une carte virtuel sur laquelle on dépose de l'argent. Cette solution est généralement utilisée pour les produits de faible coût. La deuxième solution est le paiement directement avec sa carte de crédit, comme tout autre achat. C'est la que les problèmes de sécurité commence et que la peur des consommateurs se fait sentir.

La sécurité du paiement

Les risques sont multiples. Le commerçant peut modifier le montant à débiter ou vendre un produit qui n'existe pas et que le client ne recevra jamais. Le client, lui, peut utiliser une carte qui n'est pas la sienne, contester avoir passé une commande ou avoir un découvert à la banque. Enfin, une tiers personne peut récupérer les informations sur la carte de crédit et les utiliser…

Il s'agit donc de sécuriser les échanges en s'assurant qu'ils sont chiffrés (confidentialité), que ceux qui y participent sont bien ceux qu'ils disent être (authentification), que les données n'ont pas été modifiées (intégrité). Il faut également pouvoir certifier que les échanges ont bien eu lieu (non répudiation) et que le client peut payer.

Il existe plusieurs mécanismes pour assurer une certaine sécurité :
- SSL : Secure Socket Layers : c'est de loin le plus utilisé, il assure le chiffrement des échanges mais ne garantit pas que le marchand va vous livrer, ni que le client peut payer. On sait que l'échange est sécurisé car l'adresse http:// est remplacée par https:// et un cadenas apparaît en bas de votre navigateur.
- SET : Secure Electronic Transaction : chiffrement des données de la carte de crédit, signature des messages et authentification des différents acteurs de l'échange.
- C-SET : Chip Secure Electronic Transaction : C'est une extension de SET avec un lecteur de carte. Ces deux systèmes sont compatibles, mais C-SET permet de contrôler d'avantage de chose de façon physique (vérification de la carte, etc…). Ce système est aussi sûr qu'un paiement par carte bancaire dans un magasin.

D'autres mécanismes de sécurité existe mais ne devrait pas être utilisés pour le paiement.

Conclusion : Faut-il avoir peur de payer sur Internet ?

Après avoir payé des années sur le minitel, on se pose la question de la sécurité sur Internet pour le paiement en

ligne. Ce qu'il faut se dire, c'est qu'on peut sans problème se fier à une entreprise qui a pignon sur rue, comme fnac.fr, amazon.com, ou internic.net et que dans ce cas, les craintes ne sont pas justifiées. Par contre, il faut se méfier des sites tape-à-l'œil inconnus jusque là… C'est peut-être pour ça qu'il est difficile de faire sa place sur Internet !

Le principal risque, en effet, est que le commerçant en face vous ne soit pas sérieux ou que son entreprise soit fictive. Le risque de se faire voler son numéro de carte bleue n'est pas nul, mais il est improbable… Pourquoi ? Regardez le dernier ticket de paiement que vous avez reçu en utilisant votre carte de crédit : n'y voyez-vous pas le numéro de carte qui y figure ? Le commerçant garde toujours un double de ce ticket… alors pourquoi quelqu'un irait décrypter des numéros de cartes de crédit sur Internet ? Vous avez déjà donné votre numéro de carte à tous les commerçants de France et de Navarre !

Firewalls

Voici la traduction de quelques questions et réponses d'une FAQ sur les firewalls. Je me suis permis de l'adapter et d'ajouter certaines choses, ce qui n'engage que moi… Cette FAQ, en anglais, peut être retrouvée dans son intégralité à l'adresse suivante : http://www.interhack.net/pubs/fwfaq/ et http://www.clark.net/pub/mjr/pubs/fwfaq/

Qu'est-ce qu'un firewall?

Un firewall est un système ou un groupe de système qui gère les contrôles d'accès entre deux réseaux. Plusieurs méthodes sont utilisées à l'heure actuelle. Deux mécanismes sont utilisés : le premier consiste à interdire le trafic, et le deuxième à l'autoriser.

Certains firewalls mettent beaucoup d'énergie à empêcher quiconque de passer alors d'autres tendent à tout laisser passer. La chose la plus importante à comprendre est qu'il représente une politique de contrôle d'accès. Vous devez avoir une idée précise de cette politique dans son ensemble pour savoir ce que vous devez autoriser ou interdire.

De quoi protège un firewall?

Certains firewalls laissent uniquement passer le courrier électronique. De cette manière, ils interdisent toute autre attaque qu'une attaque basé sur le service de courrier. D'autres firewalls, moins strictes, bloquent uniquement les services reconnus comme étant des services dangereux.

Généralement, les firewalls sont configurés pour protéger contre les accès non authentifier du réseau externe. Ceci, plus qu'autre chose, empêche les vandales de se logger sur des machines de votre réseau interne, mais autorise les utilisateurs de communiquer librement avec l'extérieur.

Les firewalls sont également intéressants dans le sens où ils constituent un point unique où l'audit et la sécurité peuvent être imposés. Tous les échanges passeront par lui. Il pourra donner des résumés de trafic, des statistiques sur ce trafic, ou encore toutes les connexions entre les deux réseaux.

De quoi ne protège pas un firewall?

Un firewall ne protège pas des attaques qui ne passe pas par lui… Certaines entreprises achètent des firewalls à des prix incroyables alors que certains de leurs employés sont parfois connectés par modem au monde extérieur. Il est important de noter qu'un firewall doit être à la mesure de la politique de sécurité globale du réseau. Il ne sert à rien de mettre une porte blindée sur une maison en bois… Par exemple, un site contenant des documents top-secret n'a pas besoin d'un firewall : il ne devrait tout simplement pas être connecté à Internet, et devrait être

isolé du reste du réseau !

Une autre chose contre laquelle un firewall ne peut vous protéger est les traitres et les idiots qui sont à l'intérieur de l'entreprise… Si un espion industriel décide de faire sortir des données, il y arrivera, surtout sur disquette… Il vaut mieux vérifier qui a accès aux informations que de mettre un firewall dans ce cas !

Que dire des virus?

Les firewalls ne protège pas très bien des virus. Il y a trop de manières différentes de coder des fichiers pour les transférer. En d'autres termes, un firewall ne pourra pas remplacer l'attention et la conscience des utilisateurs qui doivent respecter un certain nombre de règles pour éviter les problème… La première étant bien évidemment de ne jamais ouvrir un fichier attaché à un mail sans être sûr de sa provenance.

Il faut prendre des mesures globales et importantes contre les virus. Avant de traquer les virus à l'entrée du réseau, il faut s'assurer que chaque poste de travail dispose d'un anti-virus. Les virus passe également très facilement par disquette… Les virus sur Internet son bien moins important que les virus sur disquette.

Quoiqu'il en soit, de plus en plus de vendeurs de firewalls vous offrent des firewalls qui détectent les virus. Ils permettent probablement d'arrêter les virus simples. Ne comptez pas sur leur protection !

Quelles sont les points à prendre en compte pour un firewall?

Il y a un certain nombre de règles qui doivent être prise par le chanceux qui a reçu la responsabilité de configurer et de gérer le firewall.

Le plus important est de refléter la politique de sécurité choisit par l'organisation. Entre tout interdire et tout autoriser, il y a différent degrés de paranoïa. Le choix final doit être le résultat d'une politique globale de sécurité plus que d'une décision d'un ingénieur…

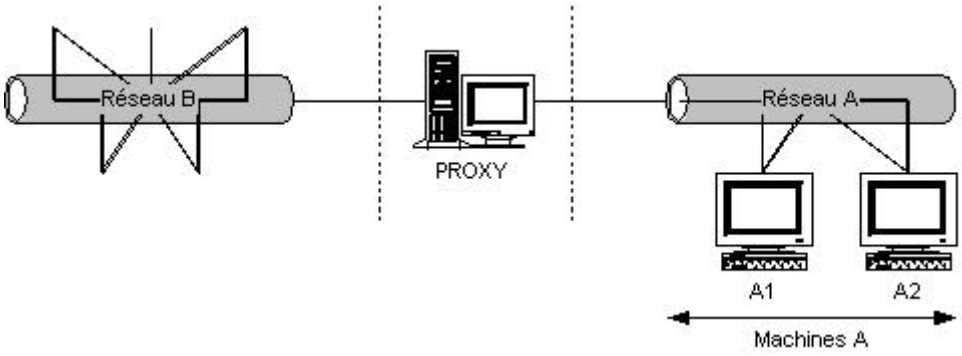
La deuxième est de savoir le degré de contrôle que vous voulez. Après avoir analysés les risques, il faut définir ce qui doit être autorisé et interdit.

Le troisième point est financier : c'est de savoir le busget que vous allouez au firewall. Un firewall complet peut être gratuit, ou coûter 100 000 dollars. La solution gratuite, comme la configuration d'un routeur, ne coûte rien sinon beaucoup de temps et de café. D'autres solutions coûteront cher au départ et peu ensuite… Il est important de considérer le prix de départ, mais aussi celui du support.

Un firewall coûte cher et prend beaucoup de temps à administrer… Vérifiez que vous avez des bijoux avant d'acheter un coffre-fort hi-tech !

Qu'est-ce qu'un proxy?

Le but d'un serveur proxy est d'isoler une ou plusieurs machines pour les protéger, comme indiqué sur le schéma :



Les machines A doivent se connecter au réseau par l'intermédiaire du serveur Proxy. Ce dernier sert de relais entre le réseau et les machines à cacher. Ainsi, les machines du réseau B auront l'impression de communiquer avec le proxy, et non les machines A.

Pour les applications du réseau B, l'adresse IP du client sera celle du serveur Proxy. Par exemple, lors d'une connexion à un serveur HTTP, le browser se connecte au serveur proxy et demande l'affichage d'une URL. C'est le serveur proxy qui gère la requête et qui renvoie le résultat à votre browser.

Ainsi, en utilisant un numéro de port différent, le proxy oblige toutes les requête à passer par lui en supprimant les trames dont le numéro de port ne lui correspond pas.

De plus, le proxy possède un avantage supplémentaire en termes de performances. Si deux utilisateurs demandent à peu de temps d'intervalle la même page, celle-ci sera mémorisée dans le proxy, et apparaîtra donc beaucoup plus rapidement par la suite.

Ce procédé est très intéressant en termes de sécurité sur Internet, les machines sont protégées. Le serveur proxy peut filtrer les requêtes, en fonctions de certaines règles.

Les VPN et le protocole PPP

Qu'est-ce qu'un VPN ?

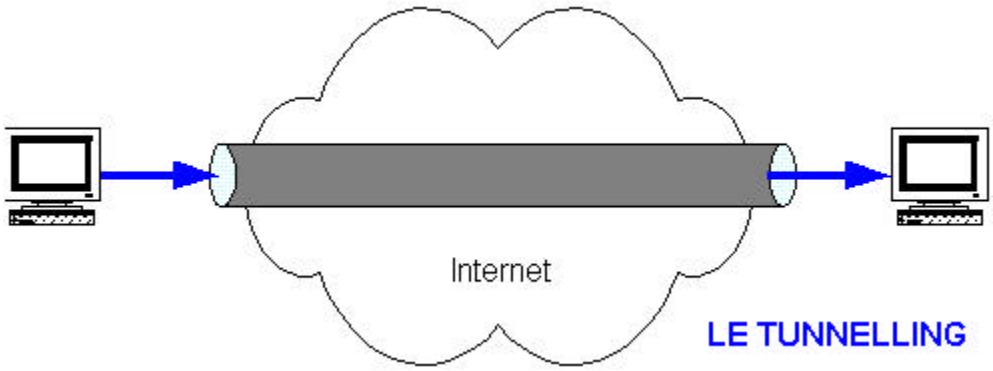
Les réseaux privés virtuels (VPN : Virtual Private Network) permettent à l'utilisateur de créer un chemin virtuel sécurisé entre une source et une destination. Avec le développement d'Internet, il est intéressant de permettre ce processus de transfert de données sécurisé et fiable. Grâce à un principe de tunnel (tunnelling) dont chaque extrémité est identifiée, les données transitent après avoir été chiffrées.

Un des grands intérêts des VPN est de réaliser des réseaux privés à moindre coût. En chiffrant les données, tout se passe exactement comme si la connexion se faisait en dehors d'Internet. Il faut par contre tenir compte de la toile, dans le sens où aucune qualité de service n'est garantie.

Comment marche un VPN ?

Le principe du VPN est basé sur la technique du tunnelling. Cela consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Ensuite la source chiffre les données et les achemine en empruntant ce chemin virtuel.

Les données à transmettre peuvent appartenir à un protocole différent d'IP. Dans ce cas le protocole de tunnelling encapsule les données en rajoutant une entête. Permettant le routage des trames dans le tunnel. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation.



A quoi sert un VPN ?

Auparavant pour interconnecter deux LANs distants, il n'y avait que deux solutions, soit les deux sites distants étaient reliés par une ligne spécialisée permettant de réaliser un WAN entre les deux sites soient les deux réseaux communiquaient par le RTC.

Une des première application des VPN est de permettre à un hôte distant d'accéder à l'intranet de son entreprise ou à celui d'un client grâce à Internet tout en garantissant la sécurité des échanges. Il utilise la connexion avec son fournisseur d'accès pour se connecter à Internet et grâce aux VPN, il crée un réseau privé virtuel entre l'appelant et le serveur de VPN de l'entreprise.

Cette solution est particulièrement intéressantes pour des commerciaux sillonnant la France : ils peuvent se connecter de façon sécurisée et d'où ils veulent aux ressources de l'entreprise. Cela dit, les VPN peuvent également être utilisé à l'intérieur même de l'entreprise, sur l'intranet, pour l'échange de données confidentielles.

Services des VPN

Ces VPN n'ont pas comme seul intérêt l'extension des WAN à moindre coût mais aussi l'utilisation de services ou fonctions spécifiques assurant la QoS et la sécurité des échanges. Les fonctionnalités de sécurité sont matures mais par contre la réservation de bandes passantes pour les tunnels est encore un service en développement limité par le concept même d'Internet.

La qualité de service (QoS) est une fonctionnalité importante des VPN n'est pas encore une technologie assez mature et les solutions proposées sur le marché à l'heure actuelle ne permettent que des garanties sur des réseaux locaux propriétaires, c'est pourquoi peu d'ISP proposent à leurs clients des solutions VPN.

La sécurité des échanges est assurée à plusieurs niveaux et par différentes fonctions comme le cryptage des données, l'authentification des deux extrémités communicantes et le contrôle d'accès des utilisateurs aux ressources.

Principaux protocoles de VPN

Il existe sur le marché trois principaux protocoles :

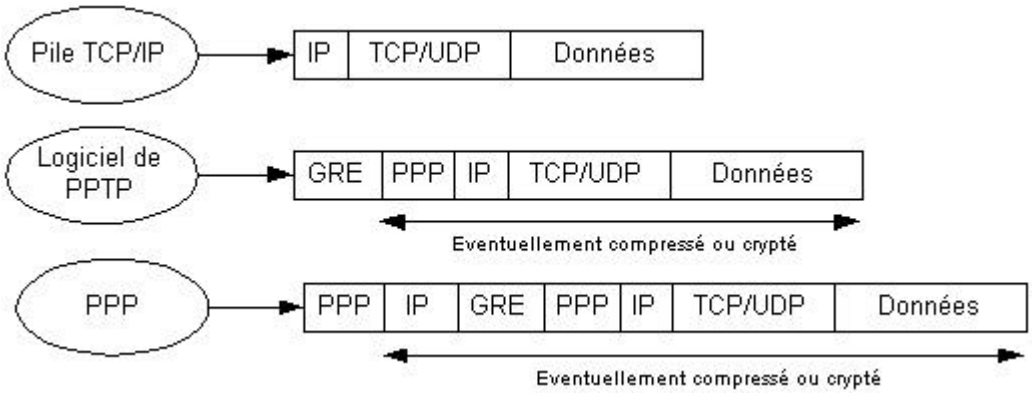
- PPTP (Point to Point Tunnelling Protocol) de Microsoft
- L2F (Layer Two Forwarding) de Cisco
- L2TP (Layer Two Tunnelling Protocol) de l'IETF

PPTP (Point to Point Tunnelling Protocol)

C'est un protocole de niveau 2 qui encapsule des trames PPP dans des datagrammes IP afin de les transférer sur

un réseau IP. PPTP permet le cryptage des données PPP encapsulées mais aussi leur compression.

Le schéma suivant montre comment un paquet PPTP est assemblé avant d'être transmis par un client distant vers un réseau cible.



L'intérêt de PPTP est de ne nécessiter aucun matériel supplémentaire car les deux logiciels d'extrémité (le client et le serveur) sont intégrés dans NT4. Par contre, il ne fonctionne que sous NT pour le moment.

L2F (Layer Two Forwarding)

L2F est un protocole de niveau 2 qui permet à un serveur d'accès distant de véhiculer le trafic sur PPP et transférer ces données jusqu'à un serveur L2F (routeur). Ce serveur L2F désencapsule les paquets et les envoie sur le réseau. Il faut noter que contrairement à PPTP et L2PT , L2F n'a pas besoin de client.

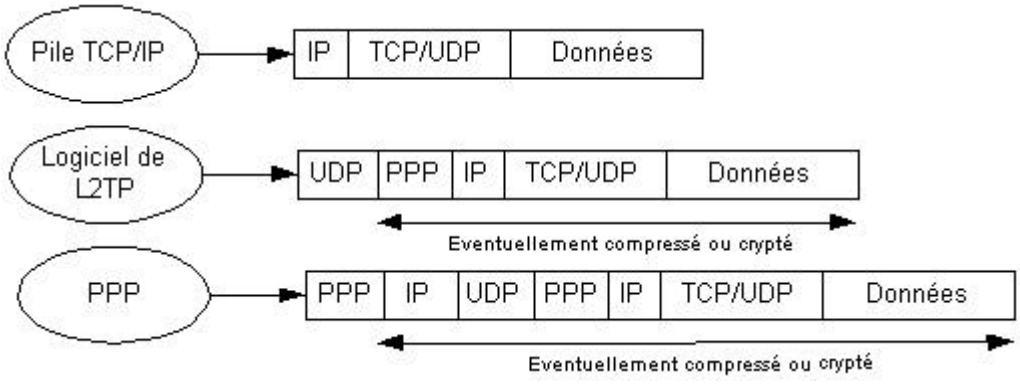
Ce protocole est progressivement remplacé par L2TP qui est plus souple.

L2TP (Layer Two Tunnelling Protocol)

Microsoft et Cisco, reconnaissant les mérites des deux protocoles L2F et PPTP , se sont associés pour créer le protocoles L2TP. Ce protocole réunit les avantages de PPTP et L2F.

L2TP est un protocole réseau qui encapsule des trames PPP pour les envoyer sur des réseaux IP, X25, relais de trames ou ATM. Lorsqu'il est configuré pour transporter les données sur IP, L2TP peut être utilisé pour faire du tunnelling sur Internet. Mais L2TP peut aussi être directement mis en œuvre sur des supports WAN (relais de trames) sans utiliser la couche de transport IP.

On utilise souvent ce protocole pour créer des VPN sur Internet. Dans ce cas, L2TP transporte des trames PPP dans des paquets IP. Il se sert d'une série de messages L2TP pour assurer la maintenance du tunnel et d'UDP pour envoyer les trames PPP dans du L2TP.



PPP : Point-to-Point Protocol

Introduction

PPP fut développé pour transférer des données sur des liens synchrones ou asynchrones entre deux points en utilisant HDLC comme base d'encapsulation et un Frame Check Sequence (FCS) HDLC pour la détection des erreurs. Cette liaison permet le full duplex et garantit l'ordre d'arrivée des paquets.

Une fonctionnalité intéressante de ce protocole est le multiplexage simultané de plusieurs protocoles de niveau 3 du modèle OSI.

Ce protocole encapsule des paquets IP,IPX et NetBEUI, … dans des trames PPP, puis transmet ces paquets PPP encapsulés à travers la liaison point à point. PPP est donc utilisé entre un client distant et un serveur d'accès distant.

Le protocole PPP est décrit dans la RFC 1331.

Format de la trame PPP

Fanion 01111110	Adresse 11111111	Contrôle 00000011	Protocole 16 bits	Données	FCS 16 bits	Fanion 01111110

Fanion : séparateur de trame. Un seul drapeau est nécessaire entre 2 trames.

Adresse : Le champ adresse correspond à une adresse HDLC, or PPP ne permet pas un adressage individuel des stations donc ce champ doit être à 0xFF (toutes les stations), toute adresse non reconnue fera que la trame sera détruite.

contrôle : Le champ contrôle doit être à 0x03, ce qui correspond à une trame HDLC non numérotée. Toute autre valeur fera que la trame sera détruite.

Protocole : La valeur contenue dans ce champ doit être impaire, l'octet de poids fort étant pair. Ce champ identifie le protocole encapsulé dans le champ informations de la trame. Les différentes valeurs utilisables sont définies dans la RFC « assign number » et représentent les différents protocoles supportés par PPP (OSI,IP,Decnet IV,IPX,…), les NCP associés ainsi que les LCP.

Informations : De longueur comprise entre 0 et 1500 octets, ce champ contient le datagramme du protocole supérieur indiqué dans le champ »protocole ». Sa longueur est détectée par le drapeau de fin de trame, moins 2 octets de contrôle

FCS (Frame Check Sequence) : Ce champ contient la valeur du checksum de la trame. PPP vérifie le contenu du FCS lorsqu'il reçoit un paquet. Le contrôle d'erreur appliqué par PPP est conforme à X25.

Le protocole LCP

Ce protocole de contrôle de liens est chargé de gérer les options et les liens créés. LCP est utilisé pour établir, maintenir, et fermer la liaison physique.

Dans l'optique d'être transportable sur un grande nombre d'environnements, PPP comprend un protocole de contrôle de liens LCP (Link Control Protocol) pour établir, configurer, tester, et terminer le lien. LCP est utilisé pour manipuler les tailles variables des paquets, en effet selon le protocole d'encapsulation sélectionné dans le champ protocole,la taille du champ options/données n'est pas la même. Ces fonctions de test permettent de détecter un lien bouclé sur lui même ou toute autre erreur classique de configuration. D'autres fonctionnalités optionnelles comme l'authentification d'identité des extrémités, et la détermination de l'état du lien peuvent s'avérer intéressantes.

L' en-tête est le suivant :

Code 1 octet	Identifiant 1 octet	Longueur 2 octets	Options

Code : Définit , sur un octet, le type de paquet LCP :
1 : Configure request - 2 : Configure Ack - 3 : Configure NAK - 4 : Configure Reject - 5 : Terminate Request - 6 : Terminate Ack - 7 : Code Reject - 8 : Protocol Reject - 9 : Echo Request - 10 : Echo Reply - 11 : Discard Request - 12 : Link quality report

Identifiant : Ce champ contient une valeur numérique qui sert à la gestion des requêtes et des réponses.

Longueur : Longueur totale du paquet LCP. Ce paquet comprend le code, l'identifiant, la longueur et les données.

Données / Options : Ce champ de taille variable peut contenir une ou plusieurs configuration d'options. Le format d'une configuration d'options LCP possède 3 champs : type, longueur et données.
- Longueur : Longueur de la configuration d'options, c'est à dire la longueur des trois champs : type, longueur et données.
- Type : Cet octet indique la configuration d'options ou de données choisie : Paquets de configurations, paquets de fin de connexion, paquets détruits ou paquets de test.

Les systèmes de détection d'intrusions

Ce rapport est une partie de ma recherche bibliographique de DEA : c'est une synthèse d'article de recherche sur la détection d'intrusions faîte en février 2000.

---

1 Introduction

1.1 Pourquoi les systèmes sont-ils vulnérables?

La sécurité est devenue un point crutial des systèmes d'informations. Cependant, les organisations sont peu ou pas protégées contre les attaques sur leur réseau ou les hôtes du réseau. Dorothy DENNING, après avoir donné des chiffres montrant l'importance du nombre d'attaques dans le monde, nous donne des raisons visant à démontrer la vulnaribilité des systèmes d'informations.

La première raison qui fait que les systèmes sont mal protégés est que la sécurité coûte chère. Les organismes n'ont pas de budget alloué à ce domaine. Elle souligne également que la sécurité ne peut être sûr à 100%, voire qu'elle est même souvent innefficace. Aurobino SUNDARAM nous en donne les raisons : les bugs dans les

programmes sont courants et seront toujours exploitables par les attaquants. De plus, même la cryptographie a ses faiblesses et les mots de passe, par exemple, peuvent être cassés. Il n'existe pas d'organisation centralisée gèrant l'ensemble des clefs et autres éléments de cryptographie. Enfin, même un système fiable peut être attaqué par des personnes abusant de leurs droits légitimes.

Dorothy DENNING ajoute d'autres raisons démontrant la vulnérabilités des systèmes : la politique de sécurité est complexe et est basée sur des jugements humains. On trouve notamment des faiblesses dues à la gestion et à la configuration des systèmes. Il y a aussi en permanence de nouvelles technologies qui émergent, et par là-même, de nouveaux points d'attaques. En dernier point, les organisations acceptent de courir ce risque, la sécurité n'étant pas leur principale priorité.

Pour exploiter ces faiblesses, les attaquants profitent de la négligence des utilisateurs vis-à-vis de leurs droits et autorisations d'accès, en se faisant passer pour un employé du service informatique dans le but d'obtenir des informations. Ils peuvent aussi casser les clefs d'une longueur insuffisante ou les mots de passe par une attaque systématique. Ils peuvent se mettre à l'écoute sur le réseau pour obtenir des informations. Ils peuvent changer leur adresse réseau pour se faire passer pour quelqu'un de confiance. Ils ont la possibilité d'injecter du code comme un virus ou un cheval de Troie sur la cible. Enfin, ils peuvent exploiter les faiblesses des applications, des protocoles ou des systèmes d'exploitation.

1.2 Introduction à la sécurité des systèmes d'informations

Etant donné le nombre de systèmes attaqués ces dernières années et les enjeux financiers qu'ils abritent, les systèmes d'informations se doivent aujourd'hui d'être protégés contre les anomalies de fonctionnement provenant soit d'une attitude intentionnellement malveillante d'un utilisateur, soit d'une faille rendant le système vulnérable.

Du fait du nombre toujours croissant de personnes ayant accès à ces systèmes par le biais d'Internet, la politique de sécurité se concentre généralement sur ce point d'entrée du réseau interne. La mise en place d'un pare-feu est devenu indispensable afin d'interdire l'accès aux paquets indésirables. On peut, de cette façon, proposer une vision restreinte du réseau interne vu de l'extérieur et filtrer les paquets en fonction de certaines caractéristiques telles qu'une adresse ou un port de communication.

Cependant, ce système de forteresse est insuffisant s'il n'est pas accompagné d'autres protections. Citons la protection physique des informations par des accès contrôlés aux locaux, la protection contre les failles de configuration par des outils d'analyse automatique des vulnérabilités du système, ou encore la protection par des systèmes d'authentification fiables pour que les droits accordés à chacun soient clairement définis et respectés, ceci afin de garantir la confidentialité et l'intégrité des données.

Faire de la sécurité sur des systèmes d'informations consiste à s'assurer que celui qui modifie ou consulte des données du système en a l'autorisation et qu'il peut le faire correctement car le service est disponible.

Même en mettant en place tous ces mécanismes, il reste encore beaucoup de moyens pour contourner ces protections. Pour les compléter, une surveillance permanente ou régulière des systèmes peut être mise en place : ce sont les systèmes de détection d'intrusions. Ils ont pour but d'analyser tout ou partie des actions effectuées sur le système afin de détecter d'éventuelles anomalies de fonctionnement.

1.3 L'audit de sécurité

L'audit de sécurité permet d'enregistrer tout ou partie des actions effectuées sur le système. L'analyse de ses informations permet de détecter d'éventuelles intrusions. Les systèmes d'exploitation disposent généralement de systèmes d'audit intégrés, certaines applications aussi. Les différents évènements du systèmes sont enregistrés dans un journal d'audit qui devra être analysé fréquemment, voire en permanence. Sur les réseaux, il est indispensable de disposer d'une base de temps commune pour estampiller les évènements.

Voici les types d'informations à collecter sur les systèmes pour permettre la détection d'intrusions. On y trouve les informations sur les accès au système (qui y a accédé, quand et comment), les informations sur l'usage fait du système (utilisation du processeur, de la mémoire ou des entrées/sorties) et les informations sur l'usage fait des fichiers. L'audit doit également permettre d'obtenir des informations relatives à chaque application (le lancement ou l'arrêt des différents modules, les variables d'entrée et de sortie et les différentes commandes exécutées). Les

informations sur les violations éventuelles de la sécurité (tentatives de commandes non autorisées) ainsi que les informations statistiques sur le système seront elles aussi nécessaires.

Notons que ces nombreuses informations occupent beaucoup de place et sont très longues à analyser. Ces informations devront être, au moins pour un temps, stockées quelque part avant d'être analysées par le système de détection d'intrusions.

2 Classification des systèmes de détection d'intrusions

Pour classer les systèmes de détection d'intrusions, on peut se baser sur plusieurs variables. La principale différence retenue est l'approche utilisée, qui peut être soit comportementale, soit par scénarios. Nous verrons ensuite d'autres paramètres permettant de classer les différents systèmes de détection d'intrusions.

2.1 Approche comportementale et approche par scénarios

Dans les traces d'audit, on peut chercher deux choses différentes. La première correspond à l'approche comportementale, c'est-à-dire qu'on va chercher à savoir si un utilisateur a eu un comportement déviant par rapport à ses habitudes. Ceci signifierait qu'il essaye d'effectuer des opérations qu'il n'a pas l'habitude de faire. On peut en déduire, soit que c'est quelqu'un d'autre qui a pris sa place, soit que lui même essaye d'attaquer le système en abusant de ses droits. Dans les deux cas, il y a intrusion.

La deuxième chose que l'on peut chercher dans les traces d'audit est une signature d'attaque. Cela correspond à l'approche par scénarios. Les attaques connues sont répertoriées et les actions indispensables de cette attaque forment sa signature. On compare ensuite les actions effectuées sur le système avec ces signatures d'attaques. Si on retrouve une signature d'attaque dans les actions d'un utilisateur, on peut en déduire qu'il tente d'attaquer le système par cette méthode.

Plusieurs méthodes différentes peuvent être mises en oeuvre pour détecter le comportement déviant d'un individu par rapport à un comportement antérieur considéré comme normal par le système. La méthode statistique se base sur un profil du comportement normal de l'utilisateur au vu de plusieurs variables aléatoires. Lors de l'analyse, on calcule un taux de déviation entre le comportement courant et le comportement passé. Si ce taux dépasse un certain seuil, le système déclare qu'il est attaqué. Les systèmes experts, eux, visent à représenter le profil d'un individu par une base de règles créée en fonction de ses précédentes activités et recherchent un comportement déviant par rapport à ces règles. Une autre méthode consiste à prédire la prochaine commande de l'utilisateur avec une certaine probabilité. Notons également l'utilisation des réseaux de neurones pour apprendre les comportements normaux des utilisateurs ou encore l'utilisation de la méthode dîte "d'immunologie" se basant sur le comportement normal du système et non des utilisateurs.

De même que pour l'approche comportementale, plusieurs méthodes peuvent être utlisées pour gérer les signatures d'attaques. Les systèmes experts les représentent sous forme de règles. La méthode dite du "Pattern Matching" (reconnaissance de forme) représente les signatures d'attaques comme des suites de lettres d'un alphabet, chaque lettre correspondant à un évènement. Les algorithmes génétiques sont également utilisés pour analyser efficacement les traces d'audit. Les signatures d'attaques peuvent être également vues comme une séquence de changements d'états du système. La simple analyse de séquences de commandes a été rapidement abandonnée car elle ne permettait pas la détection d'attaques complexes. Pour l'approche par scénarios, le poids donné à chaque entité (audit, base de signatures d'attaques et mécanisme d'analyse) et la façon dont elles sont mises en relation est décisif pour obtenir un système de détection efficace.

Chacune des deux approches a ses avantages et ses inconvénients, et les systèmes de détection d'intrusions implémentent généralement ces deux aspects. Avec l'approche comportementale, on a la possibilité de détecter une intrusion par une attaque inconnue jusqu'alors. Par contre, le choix des paramètres est délicat, ce système de mesures n'est pas prouvé exact, et on obtient beaucoup de faux positifs, c'est-à-dire que le système croit être attaqué alors qu'il ne l'est pas. Qui plus est, un utilisateur peut apprendre à la machine le comportement qu'il souhaite, notamment un comportement totalement anarchique ou encore changer lentement de comportement. Avec l'approche par scénarios, on peut prendre en compte les comportements exacts des attaquants potentiels. Les inconvénients sont dans la base de règles qui doit être bien construite et les performances qui sont limitées par l'esprit humain qui les a conçues. Notons également que l'approche par scénarios ne permet évidemment pas de détecter une attaque inconnue jusque là.

2.2 Autres méthodes de classification des systèmes de détection d'intrusions

Si la classification la plus utilisée est celle de l'approche comportementale et de l'approche par scénarios, il est possible de classer les systèmes de détection d'intrusions en fonction d'autres paramètres :

On peut classer les systèmes en fonction de la réponse qu'il apporte à l'intrusion qu'ils ont détectée. Certains systèmes se contentent d'émettre une alarme à l'administrateur (réponse passive) tandis que d'autres essayent de contrer l'attaque en cours (réponse active). Il y a pour l'instant deux principaux mécanismes de réponse implémentés : les alarmes qui permettent de prévenir rapidement l'administrateur et le filtrage des paquets venant de l'attaquant.

Les systèmes peuvent être classés en fonction de la provenance de leurs données d'audit, selon qu'elles viennent du système, des applications ou des paquets du réseau.

Certains systèmes surveillent en permanance le système d'informations tandis que d'autres se contentent d'une analyse périodique.

On peut très bien envisager de se baser sur d'autres paramètres comme le délai de détection, c'est-à-dire si le système détecte les intrusions en temps réel ou non, sa capacité de traiter les données de façon distribuée, sa capacité à répondre aux attaques sur lui-même ou encore son degré d'interopérabilité avec d'autres systèmes de détection d'intrusions.

3 Les systèmes de détection d'intrusions actuels

3.1 Modèle de base d'un systèmes de détection d'intrusions

Le premier système de détection d'intrusions a été proposé en 1980 par James ANDERSON. Il en existe maintenant beaucoup d'autres, commerciaux ou non. La majorité de ses systèmes se basent sur les deux approches, comportementale et par scénarios.

Stefan AXELSSON donne un modèle d'architecture de base pour un système de détection d'intrusions. Du système surveillé, un module s'occupe de la collecte d'informations d'audit, ces données étant stockées quelque part. Le module de traitement des données intéragit avec ces données de l'audit et les données en cours de traitement, ainsi qu'avec les données de référence (signatures, profils) et de configuration entrées par l'administrateur du système de sécurité. En cas de détection, le module de traitement remonte une alarme vers l'administrateur du système de sécurité ou vers un module. Une réponse sera ensuite apporté sur le système surveillé par l'entité alertée.

Les imperfections de ce type de systèmes monolithiques et même des systèmes de détection d'intrusions en général sont à prendre en compte. Stefano Martino souligne que si un certain nombre de techniques ont été développées jusque là pour les systèmes de détection d'intrusions, la plupart analysent des évènements au niveau local et se contentent de remonter une alarme sans agir. Ils détectent de plus les activités dangereuses d'un utilisateur sans se préoccuper du code dangereux.

3.2 Imperfections dans les implémentations actuelles

Dans la plupart des cas, les systèmes de détection d'intrusions sont faits d'un seul bloc ou module qui se charge de toute l'analyse. Ce système monolithique demande qu'on lui fournisse beaucoup de données d'audit, ce qui utilise beaucoup de ressources de la machine surveillée. L'aspect monolithique pose également des problèmes de mises à jour et constitue un point d'attaque unique pour ceux qui veulent s'introduire dans le système d'informations.

D'autres imperfections plus générales sont relevables dans les systèmes de détection d'intrusions actuels :
- Même en implémentant les deux types d'approches, certaines attaques sont indécelables et les systèmes de détection sont eux-même attaquables. Les approches comportementale et par scénarios ont elles-mêmes leurs

limites.
- Les groupes de travail sur ce sujet sont relativement fermés et il n'y a pas de méthodologie générique de construction. Aucun standard n'a pour l'instant vu le jour dans ce domaine. Des groupes y travaillent, notament au sein de la DARPA et de l'IETF.
- Les mises à jour de profils, de signatures d'attaques ou de façon de spécifier des règles sont généralement difficiles. De plus, les systèmes de détection d'intrusions demande de plus en plus de compétence à celui qui administre le système de sécurité.
- Les systèmes de détection sont généralement écrits pour un seul environnement et ne s'adapte pas au système surveillé alors que les systèmes d'informations sont, la plupart du temps, hétérogènes et utilisés de plusieurs façons différentes.
- Aucune donnée n'a été pour l'instant publiée pour quantifier la performance d'un système de détection d'intrusions. De plus, pour tester ces systèmes, les attaques sont de plus en plus difficile à simuler.

De ces imperfections, on a tenté de répondre à la question "Quelles sont les obligations d'un système de détection d'intrusions?" et on en a déduit des conditions indispensables pour un bon fonctionnement de ces systèmes.

3.3 Conditions de fonctionnement des systèmes de détection d'intrusions

Stefano MARTINO souligne qu'un système de détection d'intrusions vise à augmenter la fiabilité d'un réseau et en devient donc un composant critique. Un système de détection d'intrusions, quelque soit son architecture, doit :

- tourner en permanence sans superviseur humain.
- être tolérant aux fautes et résister aux attaques.
- utiliser un minimum de ressources du système surveillé.
- détecter les déviations par rapport à un comportement normal.
- être facilement adaptable à un réseau spécifique.
- s'adapter aux changements avec le temps.
- être difficile à tromper.

Les conditions à appliquer aux systèmes de détection d'intrusions peuvent être classées en deux parties : les conditions fonctionnelles, c'est-à-dire ce que le système de détection se doit de faire, et les conditions de performances, c'est-à-dire comment il se doit de le faire.

Un système de détection d'intrusions se doit évidemment de faire une surveillance permanente et d'émettre une alarme en cas de détection. Il doit de fournir suffisamment d'informations pour réparer le système et de déterminer l'étendu des dommages et la responsabilité de l'intrus. Il doit être modulable et configurable pour s'adapter aux plates-formes et aux architectures réseaux. Il doit pouvoir assurer sa propre défense, comme supporter que tout ou partie du système soit hors-service. La détection d'anomalies doit avoir un faible taux de faux positifs. Le système de détection doit tirer les leçons de son expérience et être fréquemment mis à jour avec de nouvelles signatures d'attaques. De plus, il doit pouvoir gérer les informations apportées par chacune des différentes machines et discuter avec chacune d'entre elles. En cas d'attaques, il doit être capable d'apporter une réponse automatique, même aux attaques coordonnées ou distribuées. Ensuite, le système de détection devra également pouvoir travailler avec d'autres outils, et notamment ceux de diagnostic de sécurité du système. Il faudra, lors d'une attaque, retrouver les premiers évènements de corruption pour réparer correctement le système d'informations. Enfin, il va de soi qu'il ne doit pas créer de vulnérabilités supplémentaires et qu'il doit aussi surveiller l'administrateur système.

Les évènements anormaux ou les brèches dans la sécurité doivent être rapportés en temps réel pour minimiser les dégâts. Le système de détection d'intrusions ne devra pas donner un lourd fardeau au matériel surveillé, ni interférer avec les opérations qu'il traite. Il doit pouvoir s'adapter à la taille du réseau qu'il surveille.

Pour pallier à un certain nombre de ses problèmes et remplir ses conditions, la technologie des agents mobiles a été appliquée aux systèmes de détection d'intrusions. Le paragraphe suivant explique le principe, les avantages et les inconvénients des agents mobiles.

4 Utilisation des agents mobiles dans les systèmes de détection d'intrusions

Une alternative à l'utilisation d'un module monolithique pour la détection d'intrusions est la mise en oeuvre de processus indépendants.

4.1 Qu'est-ce qu'un agent mobile ?

Un agent mobile est un programme autonome qui peut se déplacer de son propre chef, de machine en machine sur un réseau hétérogène dans le but de détecter et combattre les intrusions. Cet agent mobile doit être capable de s'adapter à son environnement, de communiquer avec d'autres agents, de se déplacer et de se protéger. Pour ce dernier point, une des fonctions de l'agent doit être l'identification et l'authentification pour donner l'emplacement et l'identité de celui qui l'a lancé.

Ainsi, Chaque agent est un programme léger, insuffisant pour faire un système de détection d'intrusions entier car il n'a qu'une vision restreinte du système. Si plusieurs agents coopèrent, un système de détection plus complet peut être construit, permettant l'ajout et le retrait d'agents sans reconstruire l'ensemble du système.

La première caractéristique dont ont peut tirer des avantages est la mobilité des agents. Le fait qu'il n'y ait pas de programme principal qui se sert des autres modules comme esclaves mais plutôt la présence de plusieurs entités intelligentes qui collaborent, fait que si une des entités s'arrête, le système continue de fonctionner.

4.2 Avantages et inconvénients des agents mobiles

Si les agents n'apportent pas fondamentalement de nouvelles capacités, ils apportent néanmoins des réponses aux imperfections soulignées précédemment. Stefano MARTINO fait d'ailleurs une analogie entre le système immunitaire humain et cette approche : chaque cellule ou agent doit combattre les intrus avant que ça ne deviennent une menace pour le système.

Quatre classes peuvent être faites pour caractériser ces avantages :

- La flexibilité : on a la possibilité d'adapter le nombre d'agents à la taille du système d'informations ainsi que d'avoir des agents entraînés en fonction du système surveillé.
- L'efficacité : les agents affectent moins les performances de chaque machine puisqu'ils peuvent travailler sur les ressources ayant uniquement rapport avec leur champ de vision. Le gain au niveau de l'échange d'informations, sur le réseau notamment, est loin d'être négligeable.
- La fiabilité : c'est la tolérance aux fautes. Si un agent est hors-service, il reste d'autres agents qui peuvent se reproduire. Le système de défense n'est pas annihilé par la compromission d'un seul agent, un agent corrompu ne donnnant pas une image fausse de l'ensemble du système aux autres agents.
- La portabilité : les agents supportent plus facilement les systèmes distribués, et donc à la fois l'aspect hôte et l'aspect réseau. Notons par exemple que ce système permet de détecter les attaques distribuées, c'est-à-dire dûes aux attaques simultanées de plusieurs personnes réparties sur un réseau.

En plus de ses avantages, il y en a encore un certain nombre. L'architecture par agents mobiles est naturelle et présente une plus grande résistance aux attaques puisqu'elle se base sur un système autre que hiérarchique. Qui plus est, elle est basée sur une exécution asynchrone et une certaine autonomie, ce qui fait que les agents mobiles sont désolidarisés du reste pour une plus grande tolérance aux fautes. Enfin, les agents mobiles présentent la capacité de s'adapter dynamiquement aux changements et peuvent donc réagir plus rapidement.

Si les systèmes par agents mobiles ont des avantages indéniables, ils ont également des inconvénients notables. Il est clair que le codage et le déploiement sera difficile pour assurer un code code sûr avec beaucoup de fonctionnalités.

Il y a d'autres inconvénients : quand les agents se déplacent, un noeud dépourvu d'agent est vulnérable pendant un moment. De plus, si les agents ont besoin d'un apprentissage, ce temps peut être long. Il souligne ensuite quelques unes des imperfections des systèmes de détection d'intrusions qui ne sont pas corrigées par le système

des agents mobiles. Ils peuvent être corrompus et ils imposent une utilisation des ressources et que quelque soit le système. Enfin, certains attaquants réussiront toujours à obtenir des droits pendant quelques temps avant d'être détectés.

Enfin, quelques points resteront à étudier, comme la performance, car il faut voir la rapidité avec laquelle l'agent détecte et remonte l'information d'intrusion, la taille du code, car les systèmes de détection sont complexes et les agents risquent de demander d'assez gros programmes et le temps d'adaptation des agents à un système, car il y aura un manque de connaissance de base étant donné que beaucoup de plates-formes et de configurations sont différentes.

4.3 Conclusion et perspectives pour les agents mobiles

Si les agents mobiles apportent des avantages importants, les inconvénients qu'ils engendent du même coup ne sont pas négligeable. Cependant, l'approche par agents mobiles semble pouvoir donner des résultats meilleurs que les autres technologies et la recherche va développer une nouvelle architecture pour cette technologie.

Les avantages des agents mobiles pourront être exploités de plusieurs façons : en prévoyant de la surveillance en plus de la détection, en fournissant une réponse aux attaques et en augmentant la fiabilité du système. On peut aussi tirer profit de la diversité en représentant les signatures d'attaques par une méthode différente pour chaque agent.

5 Perspectives pour la recherche

Les tendances de la recherche vont de la machine vers le réseau, d'un système centralisé vers un système distribué, vers une plus grande interopérabilité des systèmes et vers une plus grande résistance aux attaques. Les constantes de la recherche sont l'utilisation d'un système hybride (approche comportementale et par scénarios) permettant de la détection en temps réel. Beaucoup de chercheurs se penchent sur le problème de l'amélioration du nombre de faux positifs et d'attaques non détectés.

Les mécanismes idéaux de réponses aux attaques consisteraient à supprimer l'action de l'intrus dans la cible, éteindre la cible et protéger le reste du réseau. Dans le cas des attaques internes, il faudrait bloquer l'attaquant, éteindre sa machine ou être capable de remonter à l'attaquant très rapidement pour surveiller ses actions. Enfin, il faudrait que le système de détection puisse toujours modifier les tables de filtrage des routeurs et pare-feux, ce qui est déjà le cas de certains systèmes du commerce.

L'approche par agents mobiles apportent là aussi une solution puisqu'il n'est pas nécessaire d'avoir un serveur de sécurité dans le sens où les agents peuvent automatiquement se mouvoir dans le réseau et installer les composants appropriés sur les éléments qu'il faut. Ils peuvent traquer les attaquants et rassembler des preuves de façon automatique ou encore effectuer des opérations sur la machine de l'attaquant, sur la machine cible ou sur le réseau en les mettant, par exemple, en quarantaine.

Un certain nombre de questions restent ouvertes :

- Quels types d'intrusions est-on sûr de détecter ?
- De quelles données d'audit a-t-on besoin pour prendre la décision qu'il y a eu intrusion ?
- Quels sont les types d'attaques contre les systèmes de détection même ?
- Quand est-on sûr que le système de détection d'intrusions n'est pas compromis et si c'est le cas, que faire ?
- Quelle quantité minimum de ressources peut prendre un système de détection pour être efficace ?

A ces questions, on peut en ajouter une autre : Comment peut-on réduire le taux de faux positif? La réponse passera sans doute par ces deux autres questions :

- Quelles méthodes et mécanismes permettent de détecter les scénarios d'attaques complexes?
- Comment peut-on faire coopérer les différents systèmes de détection d'intrusions?

Bibliographie

- Dorothy Denning, "Protection and Defense of Intrusion", 1996
- Ludovic Mé and Cédric Michel, "La détection d'intrusions : bref aperçu et derniers développements", 1999
- Aurobindo Sundaram, "An introduction to Intrusion Detection", 1996
- L. Mé and V. Alanou, "Détection d'intrusions dans un système informatique : méthodes et outils", 1996
- Stefan Axelsson, "Research in Intrusion-Detection Systems : A Survey", 1999
- Hervé Debar, "Détection d'intrusions, une aide a la sécurité pour l'accès mobile", 1999
- Roland Buschkes, Dogan Kesdogan et Peter Reichl, "How to Increase Security in Mobile Networks by Anomaly Detection", 1998
- Stefano Martino, "A mobile agent approach to intrusion detection", 1999
- Wayne Jansen, Peter Mell, Tom Karygiannis et Don Marks, "Applying Mobile Agents to Intrusion Detection and Response", 1999
- J.P. Anderson, "Computer Security Threat Monitoring and Surveillance", 1980
- Mark Crosbie et Gene Spafford, "Active Defense of a Computer System using Autonomous Agents", 1995
- Nadia Boukhatem, "Les agents mobiles et applications", 1999
- S. Corson et J. Macker, "Request For Comments 2501", 1999

www.guill.net
Mars 2000