AGTech
Association Romande des Techniciens Genève

WWW.AGTECH.CH

Le mot du président

Ce que nous offre la presse technique et scientifique
- Serveur proxy, firewall et sécurité
- Chiffrement et cryptographie

Sorties et activités pour cette année

Pause - café …

On the web …

Mot du Président

Chers membres,

L'ARTech bouge. La semaine dernière nous sommes allés visiter l'entreprise SKYguide, visite au terme de laquelle, nous avons appris que les contrôleurs du ciel sont bigrement mis à l'épreuve dans leur travail. J'en profite pour vous dire que cette entreprise est en manque chronique d'effectifs. En ces temps plutôt moroses, cela pourrait rendre service.

Nous avons trouvé un webmaster pour une refonte complète du site. Bienvenue à Thibault (technicien en informatique) qui est un as des sites web ! Dans quelques temps, quand il aura pris connaissance des us et coutumes du comité, nous aurons droit à un magnifique site.

La cotisation à deux vitesses est un grand succès. Nos membres qui ne désirent plus faire partie de l'ASET, sans pour autant perdre les avantages de l'ARTech peuvent désormais le faire ! Lors de notre prochaine AG, nous vous présenterons le pourcentage de membres qui ont décidé de ne plus faire partie de l'ASET.

L'IFAGE à repris contact avec nous, car cette année plusieurs sessions arrivent à termes. L'électronique, le génie civil et l'informatique. Nous avons des experts dans les deux premières sessions, mais pas encore dans l'informatique. Bien que j'aie déjà proposé des noms de membres en qualité d'expert.

Je pense que vous avez tous découvert notre nouveau logo qui, je trouve, est magnifique. Merci Thibault et encore bienvenue au sein du comité !

Didier Moullet
Président ARTech

Serveur proxy, firewall et sécurité

A l'origine, le serveur proxy a été conçu pour relayer vers Internet les requêtes des navigateurs. Aujourd'hui, ce rôle ancien a disparu au profit de nouvelles fonctionnalités : cache, enregistrement, filtre, navigation anonyme et sécurité du réseau local. Pour cette dernière fonction, le serveur proxy est avantageusement remplacé par le firewall.

A l'époque héroïque du web, les réseaux locaux n'étaient pas reliés à Internet, ils n'utilisaient pas le protocole TCP/IP , et les navigateurs étaient des logiciels fort rudimentaires. On conçoit que le CERN (Centre Européen de Recherche Nucléaire, à l'origine du web) ait éprouvé le besoin de créer (en 1994) un serveur destiné à relayer vers Internet les requêtes des navigateurs. Ce dispositif fut baptisé ***serveur mandataire*** : mais c'est le terme ***serveur proxy*** qui s'est imposé dans notre langue.

Aujourd'hui, les réseaux locaux sont de plus en plus souvent reliés à Internet via une passerelle ou un routeur, et ils utilisent de plus en plus fréquemment le protocole TCP/IP ; le rôle initial de relais joué par le serveur proxy est devenu obsolète. Pour continuer à vendre des serveurs proxy, les éditeurs de logiciel les ont dotés de nouvelles fonctions (décrites ci-après). On notera que l'on peut concevoir un serveur proxy pour chacun des services utilisant le réseau Internet (web, ftp, telnet, news…), mais qu'en pratique on rencontre surtout des serveurs proxy destinés au web.

Un serveur proxy peut offrir les cinq fonctions suivantes :

- la fonction de ***cache*** (caching). Le serveur proxy conserve en mémoire toutes les pages web demandées par les clients qu'il dessert;
- la fonction d'***enregistrement*** (tracking ou logging). Le serveur proxy garde une trace détaillée de toutes les informations qui le traversent;
- la fonction de ***filtre*** (filtering). On peut configurer un serveur proxy de telle sorte qu'il examine l'information qui le traverse, et qu'il refuse de délivrer les fichiers contenant une chaîne de caractère donnée. On peut également lui demander de gérer les droits de chaque client en ce qui concerne Internet;
- la fonction d'***anonymiseur*** (anonymizing). On peut faire en sorte que les requêtes relayées par un serveur proxy ne contiennent pas l'adresse du navigateur client, de manière à protéger l'anonymat de l'internaute sur le web;
- la fonction de ***sécurité***. Le serveur proxy peut constituer une barrière entre Internet et le réseau local de l'entreprise;
- enfin un proxy peut éventuellement remplacer un ***routeur*** à translation d'adresse (NAT).

LE ROLE DE CACHE DU SERVEUR PROXY

En jargon informatique, une ***mémoire cache*** sert à conserver localement des informations qui ont une certaine probabilité de servir à nouveau à court terme. Ainsi, on trouve une mémoire cache dans les micro-processeurs, dans les contrôleurs de disque dur, dans les navigateurs, dans les serveurs web, etc… Un serveur proxy stocke provisoirement les pages web que les utilisateurs vont chercher sur Internet. Si un internaute requiert une information qui se trouve déjà dans le cache, il sera servi ***plus rapidement*** . Dans le cas contraire, il sera servi ***un peu plus lentement***, car la traversée du serveur proxy représente une étape supplémentaire dans le transport de l'information.

Le rôle de cache du serveur proxy pose en fait un double problème :

- l'internaute est-il, ***en moyenne***, servi plus lentement ou plus rapidement grâce au cache ?
- l'information qui a séjourné dans le cache est-elle ***toujours valide*** ?

Le cache accélère-t-il les consultations ? Il existe de par le monde un peu plus de **38 millions de sites web** (1) régulièrement actifs. Ils mettent à notre disposition un peu plus de deux milliards de pages web. La probabilité pour que deux internautes, dont les besoins en information sont indépendants, demandent la même page, vaut donc 5.10^{-10}. Si le proxy dessert 100 utilisateurs, et si chacun d'eux télécharge 10 pages web, il existe ***moins d'une chance sur un million*** pour que le proxy joue son rôle de cache, et ce ***pour une seule page***. Si les décideurs qui signent les bons de commande connaissaient mieux Internet et le calcul des probabilités, on ne vendrait pas beaucoup de serveurs proxy pour leur rôle de cache !

Le calcul précédent suppose que toutes les pages du web ont la même probabilité d'être consultées, et que tous les internautes ont des besoins distincts en information, ce qui est loin d'être le cas. Pour donner une chance au serveur proxy de servir à quelque chose, il faut se placer dans le cas favorable ou l'une au moins des conditions suivantes est remplie :

- le proxy dessert un ***grand nombre d'utilisateurs***;
- ces utilisateurs ont des besoins en informatique ***fortement corrélés***;
- les pages web qu'ils requièrent présentent un ***fort taux de consultation.***

1) – Le nombre d'utilisateurs.

Cette condition est difficile à remplir : si un proxy dessert 1000 utilisateurs, et si chacun d'eux décharge 100 pages, il y a moins d'une chance sur mille pour que le cache fonctionne, et ce pour une page seulement. D'où l'idée d'installer un serveur proxy-cache au point d'interconnexion entre deux dorsales Internet, ou même à l'échelle de tout un pays. Ainsi, aux Etats-Unis, dix grands **« web caches »** ont été installés, dans le cadre du projet **IRCache** (2), financé de 1995 à 2000 par le National Laboratory for Applied Network Research (**NLANR)** (3). Bien que le projet soit arrêté, les caches sont maintenus en activité, à des fins de recherche essentiellement (ces caches utilisent un logiciel gratuit appelé **Squid** (4), qui fonctionne sous Unix).

En France, le cache national du réseau Renater, mis en place en 1998 et complété par des caches régionaux, est arrêté depuis le 24 août 2000. Ces exemples montrent que les grands web-caches, qui coûtent cher en matériel et en maintenance, ne sont pas économiquement justifiés : il est moins onéreux d'augmenter la bande passante que de l'économiser à l'aide de caches. Tous les web-caches n'ont pas encore disparu, mais leurs jours sont probablement comptés. La campagne **Cache Now !** en faveur du développement des web-caches est au point mort. Seuls les Anglais gardent un moral de fer en ce qui concerne leur web-cache universitaire **Janet** (5) .

En fait, le seul système de web-cache réellement efficace est celui des **« Content Delivry Networks »** (6) ou **CDN**. Ce sont des ensembles de serveurs miroirs déployés à travers Internet, qui stockent l'information le plus près possible du client. Les CDN travaillent pour les grands sites web (quelques milliers actuellement), qui leur confient la distribution de leurs fichiers ***les plus lourds*** : images de grande taille, animations, vidéos en différé ou en streaming. Un système de répartition de charge (load balancing) détermine quel est le serveur le mieux à même de satisfaire le client. Le CDN le plus connu est ***Akamai***, mais il en existe de nombreux autres (7-8). Les CDN sont aussi utilisés pour distribuer de simples pages HTML, en cas de très grosse pointe de trafic.

Un nouveau langage de description de page, baptisé **ESI** (9) **(Edge Side Includes)**, a récemment été créé pour étendre le système CDN aux pages web dont une partie est générée de manière dynamique.

2) – Des besoins corrélés en information.

Cette condition, par contre, peut être plus facile à satisfaire. Si un proxy dessert 1000 utilisateurs déchargeant chacun 100 pages, et si 10% d'entre eux ont les mêmes besoins, le cache va resservir environ 10'000 pages. Où trouve-t-on des populations ayant des besoins communs en information ? Plutôt dans le grand public, dont les goûts ont été modelés et uniformisés par la publicité et les grands média. C'est pourquoi, les **FAI** (Fournisseurs d'Accès Internet), et plus particulièrement ceux dont la clientèle est constituée principalement de particuliers, utilisent un serveur proxy, dont le cache servira de nombreuses fois pour la météo, les nouvelles du jour, etc… . Mais comment se fait-il que, malgré la présence de ces caches, les sites serveurs de nouvelles (ex : CNN) soient débordés lorsqu'un événement très médiatique se produit ?

En s'éloignant de plus en plus du client, on peut arriver à la conclusion qu'il faut mettre un cache …

sur les serveurs web eux-mêmes. De fait, tous les logiciels de serveur web gèrent un cache en mémoire vive et, si l'on examine le fonctionnement d'un serveur à fort trafic, on s'aperçoit que son cache est effectivement très utilisé. On peut aller plus loin en installant les fichiers du site web en ***ramdisk*** (si la mémoire vive du PC est suffisante). Cette technique est efficace lorsque le temps de réponse du serveur est limité par les accès au disque, ce qui n'est pas toujours le cas. Certains sites conseillent même de coupler serveur proxy et serveur web ; pour que ce dernier ne soit pas caché aux internautes, le proxy est monté à l'envers **(*reverse proxy*)**. Pour peu que l'on s'y prenne mal, les internautes qui veulent accéder au site doivent reconfigurer leur navigateur… Une histoire de fou, quoi ?
Etant donné qu'un serveur web gère son propre cache, on ne voit pas pourquoi il faudrait lui adjoindre un système de cache externe. A moins que le serveur ne soit protégé par un ***firewall***, et que le système de cache ne soit installé ***devant*** le firewall – une solution qui existe, mais dont on parle peu.

3) – Des pages web à forte consultation.

Lorsque l'on examine les fichiers « log » d'un serveur proxy, on y trouve toujours le même type d'information. Elle est constituée *des pages d'accueil des sites les plus fréquentés du web* : moteurs de recherche réputés, portails renommés, sites météo, journaux et sites de nouvelles, agences de voyage, horaires des moyens de transport, jeux en ligne… Nombreux sont ceux qui vantent les mérites du cache des serveurs proxy, mais rares sont ceux qui ont l'honnêteté de publier le fichier journal correspondant.

Prenons l'exemple d'un internaute qui pose une question à un moteur de recherche. Seule la page d'accueil dudit moteur sera mise en cache, car les autres pages sont spécifiques (elles sont générées par un script côté serveur, repérables par un point d'interrogation dans leur URL, et ne sont en principe jamais cachées par les serveurs proxy). Certes, l'internaute obtiendra la première page plus vite, mais on lui servira les autres ***plus lentement***, car il faut le temps de traverser le proxy. Prétendre que, dans ces conditions, le serveur proxy accélère globalement la fourniture des pages demande une belle dose d'optimisme… ou de mauvaise foi. Le même raisonnement peut s'appliquer aux autres cas précités, car plus l'internaute s'enfonce dans un site, plus sa navigation devient spécifique, et la probabilité de trouver la même page en cache devient alors négligeable.

L'information cachée est-elle périmée ? En fait, tout dépend de la manière dont est configuré le serveur proxy. Plusieurs points doivent être respectés lors de la configuration d'un tel dispositif :

- le serveur doit lire l'en-tête du paquet pour décider si ce dernier doit être mis en cache ou non. Par ex : on ne doit pas stocker un paquet dont la durée de validité est nulle;
- on ne doit pas stocker des paquets dont le contenu est très spécifique. Par ex : une page générée par un script côté serveur en réponse à la question précise d'un client;
- on ne doit pas stocker des paquets qui ne contiennent pas d'information tangible. Par ex : ceux qui ne contiennent qu'un code HTTP particulier (un code d'erreur, …);
- le proxy ne doit pas mettre en cache les paquets authentifiés ou sécurisés, sauf indication contraire dans l'en-tête du paquet;
- le proxy doit appliquer des règles claires pour déterminer si l'information contenue dans un paquet caché est encore valide (***fresh***) ou si elle est périmée (***out of date, stale***) et
- en cas de doute, le proxy doit interroger le serveur web qui a fourni le paquet pour savoir si l'information a changé.

Ceci dit, les caches de serveurs proxy ne sont pas toujours configurés correctement. Un serveur proxy est souvent réglé de telle sorte qu'il ne vérifie pas ailleurs que dans son cache si la copie qu'il possède est suffisamment récente **(*TTL = Time To Live*, temps que l'on peut fixer de manière arbitraire)**. Il est donc conseillé aux utilisateurs du web d'utiliser la fonction ***actualiser*** de leur navigateur chaque fois qu'ils ont le moindre doute de la validité de la page affichée. Le problème peut également venir du cache du navigateur lui-même, cache qu'il ne faut pas hésiter à purger.

LE RÔLE D'ENRENGISTREMENT DU SERVEUR PROXY

Comme tout serveur qui se respecte, un proxy génère un fichier journal ***(log file)***. On y trouve la trace de toutes les requêtes effectuées par tous les postes clients dépendant du serveur en question.

Contrairement à ce qui se passe pour les serveurs web, il n'existe pas de format normalisé pour le fichier journal des serveurs proxy. Cependant, quelle que soit sa présentation, ce fichier journal contient pratiquement toujours :

- la date et l'heure ;
- l'identification du client, sous une forme qui dépend de la manière dont est géré le réseau local. Il peut s'agir d'un numéro ou d'un nom de machine, d'un nom d'utilisateur, etc … Les personnes qui utilisent un ordinateur portable (lequel reçoit un numéro IP à la volée lorsqu'on le branche) peuvent être difficiles à identifier ;
- l'URL de la ressource demandée ;
- la taille de la ressource ;
- le temps de téléchargement ;
- le résultat de l'opération, etc …

On conçoit qu'un chef d'entreprise veille à ce qu'aucun employé n'abuse de la bande passante en écoutant la radio sur Internet, en jouant en ligne, ou en téléchargeant interminablement des fichiers MP3. On conçoit également qu'il ne veuille pas que ses employés utilisent Internet à titre privé pendant les heures de travail. Mais le personnel doit être averti de l'existence du proxy et de l'exploitation de son fichier journal. Les règles d'utilisation d'Internet doivent être clairement définies, de même que les sanctions en cas de manquement. Malheureusement on croit souvent bon, lors de l'installation d'un proxy dans l'entreprise, de mettre en avant des raisons de ***sécurité informatique***, alors que le véritable motif est le plus souvent ***la surveillance du personnel*** qui utilise le web. L'hypocrisie d'un tel comportement ne peut être cachée longtemps, et elle risque de créer dans l'entreprise un climat empoisonné de suspicion et d'autocensure. L'un des logiciels dédiés à l'analyse des fichiers ***.log*** du serveur proxy commercialisé par Microsoft ne s'appelle-t-il pas **Webspy** [(10)] ?

Tous les fournisseurs d'accès à Internet (FAI), ou presque, utilisent un serveur proxy, ce qui les met dans une situation juridique quelque peu contradictoire. D'une part, un FAI doit garder la trace de ce que font ses clients, de manière à pouvoir réagir au cas où l'un de ces derniers contreviendrait à la loi (***spamming, hacking, pédophilie, racisme, appel à la violence, terrorisme …***) et à fournir tous les éléments nécessaires à la justice en cas d'enquête. D'autre part, l'enregistrement détaillé de ce font les clients peut être considéré comme une atteinte à la vie privée, d'autant que certains FAI utilisent les fichiers *log* de leur proxy pour créer des listes de prospects à des fins de commercialisation. La déontologie des FAI n'est pas encore tout à fait au point, de même que la jurisprudence.

LE RÔLE DE FILTRE DU SERVEUR PROXY

On peut configurer un serveur proxy de telle sorte qu'il examine le contenu des paquets qu'il reçoit pour le compte des clients, et qu'il refuse de transmettre ceux qui ne répondent pas à certains critères.

Le problème du filtrage a été particulièrement débattu aux Etats-Unis, parce que de nombreuses bibliothèques et écoles mettent le web à la disposition de leur public, et qu'il faut éviter que les enfants accèdent à des contenus dont seuls les adultes doivent avoir connaissance. Mais le problème est insoluble, parce qu'un bon filtrage requiert de l'intelligence, et que les ordinateurs n'en ont pas. Filtrer sur des mots détachés de leur contexte – et c'est bien ainsi que fonctionnent les filtres – conduit aux pires sottises. De plus les ordinateurs ne savent pas analyser les images, et on ne peut pas leur demander de faire la différence entre un nu académique, un nu érotique et un nu pornographique – à titre d'exemple. Le serveur proxy, comme tout autre système de filtre, est un censeur désastreux.

Bien que, dans l'entreprise, il n'y ait pas d'enfant à protéger, l'idée qu'il existe des sites « **répréhensibles** » et qu'il faut bloquer les informations « **inappropriées** » a fait son chemin. Cela signifie que l'on soulève un ***problème de gestion***, et qu'on prétend le résoudre avec des ***moyens techniques***. Une telle tentative est en grande partie vouée à l'échec, car ceux qui veulent contourner le filtre y arriveront toujours peu ou prou. D'ailleurs, fouille-t-on la serviette des employés qui arrivent le matin au travail, pour voir si elle contient des informations « inappropriées » ?
On ne peut pas s'empêcher de sourire en pensant que, pendant que l'on dépense de l'argent et de l'énergie pour mettre en œuvre un filtre, un ***hacker*** doué est peut-être en train de s'introduire dans le système informatique de l'entreprise et d'y faire des dégâts.

Le serveur proxy peut également être utilisé pour définir les droits de chaque client en ce qui concerne le web : personnes autorisées, heures permises, sites

accessibles ou défendus, etc… Les gestionnaires de système informatique adorent ce genre de chose, et nul doute qu'un proxy bien doté en matière de gestion des droits leur plaise particulièrement.

LE RÔLE D'ANONYMISEUR

Il existe sur Internet des sites web « ***bidons*** » montés dans seul but de savoir qui s'intéresse à un sujet donné. Cela va du sondage d'opinion à l'espionnage industriel. Bien sûr, une adresse Internet n'est pas liée à un nom de personne, mais elle est liée à un nom d'organisme. Quand vous parcourez le web, les serveurs des sites que vous visitez ont connaissance du numéro IP de votre machine (ex : 195.220.30.95). A l'aide d'un annuaire DNS inverse (ex : **RIPE**) [(11)], les administrateurs de ces serveurs peuvent savoir à quel serveur votre machine est connectée.

Pour cette raison ou pour une autre (respect de la vie privée, par ex.), il peut être intéressant de rechercher de l'information sur le web de manière ***anonyme***. Pour ce faire, on peut utiliser un poste client qui ne possède pas d'adresse Internet « ***en dur*** » , mais qui reçoit une adresse à la volée du DHCP d'un fournisseur d'accès.

Exemple : Si vous parcourez le web via AOL, l'administrateur de serveur qui relève votre numéro IP et l'introduit dans un DNS inverse apprend que ce numéro appartient à AOL, et rien de plus (en fait, il n'a même pas besoin d'utiliser cette procédure, car le nom d'AOL s'inscrit dans le fichier journal du serveur). Remarque : pour plus de sûreté, il faut aussi configurer son navigateur de telle sorte qu'il n'accepte pas les cookies.

Une autre solution consiste à utiliser un serveur proxy public dénommé « ***anonymizer*** ». Un tel serveur doit remplir les 3 conditions suivantes :

- ne pas retransmettre l'adresse IP du client ;
- supprimer tous les cookies ;
- ne pas enregistrer de fichier journal, ou le détruire dans les délais légaux sans l'avoir utilisé.

Les anonymiseurs ne sont pas sans défaut :

- il faut reconfigurer son navigateur pour se connecter au web via un proxy public ;
- le risque existe qu'un anonymiseur ne soit pas de bonne foi, et plus particulièrement lorsque le service est gratuit, la seule source de financement provenant alors de la publicité ;
- le passage par l'anonymiseur ralentit beaucoup l'accès au web ;
- les sites qui requièrent l'usage des cookies ne peuvent pas être atteints ;
- les anonymiseurs gratuits n'assurent pas les liaisons sécurisées par le protocol SSL.

Pour toutes les questions relatives aux anonymiseurs, on peut consulter la FAQ mise en ligne par **iNetPrivacy Software** . Certains sites entretiennent des listes de serveurs proxy publics : **AltaVista** , **Rosinstrument** [(12)] , **Samair** [(13)] , etc… .

SÉCURITÉ ET FIREWALL

Comme déjà signalé plus haut, la sécurité du réseau local constitue souvent l'argument massue de ceux qui installent un proxy dans une entreprise. Il est vrai que certains logiciels de serveur proxy incorporent des fonctions de sécurité. Mais comme dit le proverbe : ***qui trop embrasse mal étreint*** . Pour une vraie sécurité, rien ne vaut un ***dispositif dédié***, lequel s'appelle un ***coupe-feu*** (firewall).

En fait, l'entreprise doit d'abord **définir une politique de sécurité** avant d'envisager le type de matériel qu'elle envisage d'acheter. Une telle politique doit résulter d'un ***compromis*** entre les desiderata du service informatique (qui veut réaliser un système très sûr, donc très restrictif), et les besoins des utilisateurs (qui désirent un système aussi permissif que possible, de manière à rester créatifs et à pouvoir travailler). C'est seulement lorsque la politique de sécurité est définie que l'on peut choisir les matériels qui permettront sa mise en œuvre.

Une politique de sécurité complète doit tenir compte des agressions provenant de l'extérieur – dont on parle beaucoup – et de celles provenant de l'intérieur – dont on parle fort peu, bien qu'elles représentent la majorité des cas. Bien entendu, proxy ou firewall ne sont utiles que vis à vis des attaques extérieures. Pour parer aux attaques internes à l'entreprise, il faut utiliser un **système de détection d'intrusion** (Intrusion Detection System). Ce dernier surveille le système informatique, et signale tout événement sortant de l'ordinaire. Nombre de ces événements,

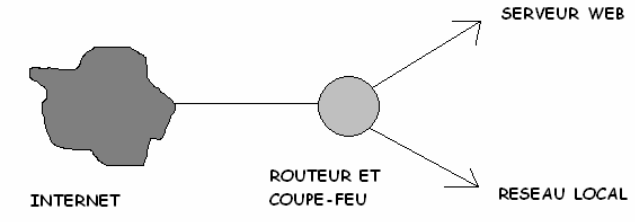
bien sûr, constituent de fausses alertes, si bien que la détection d'intrusion n'est pas chose facile.

Le coupe-feu est un système informatique (ordinateur + logiciel), que l'on intercale entre le réseau local de l'entreprise et le réseau mondial Internet, et qui surveille les échanges d'information, dans les deux sens, entre ces deux réseaux. On peut même être plus général, et définir le firewall comme l'interface entre deux réseaux, ou entre deux parties d'un même réseau. Le pare-feu examine chaque paquet d'information qui le traverse et décide, en application des règles définies lors de sa configuration, de le laisser passer ou de le détruire. La notion de coupe-feu est apparue pour la première fois en 1987, et la première réalisation pratique date de 1994. Depuis les problèmes de sécurité n'ont fait que croître et embellir sur Internet, si bien que le coupe-feu fait une carrière commerciale plus qu'honorable.

Dans la ***taxonomie des firewalls*** (14) , les puristes en distinguent plusieurs types (de deux à quatre), suivant le niveau dans lequel le dispositif doit fonctionner. Les firewalls commercialement disponibles fonctionnent souvent sur plusieurs niveaux à la fois. Pour simplifier, on peut distinguer deux cas extrêmes :

- le pare-feu qui n'examine que l'en-tête des paquets. C'est souvent ainsi que fonctionne le pare-feu destiné à protéger un réseau local ;
- le pare-feu qui n'examine que l'information utile contenue dans les paquets. C'est souvent le cas du pare-feu destiné à protéger un serveur web.

Le schéma classique de protection centralisée d'un réseau local comportant un serveur web est représenté sur la figure ci-après :



L'entreprise est reliée à Internet via un routeur, derrière lequel on place un coupe-feu. Ce dernier possède une entrée (vers le routeur), et deux sorties (l'une vers le réseau local, l'autre vers le serveur web). On configure **de manière distincte** les trois canaux de communication ainsi créés : entre Internet et le serveur web (tâche la plus difficile), entre Internet et le réseau local, entre le serveur web et le réseau local. Pour encore plus de sécurité, on peut transformer le routeur en « ***bastion*** », c'est à dire que l'on durcit ses protections au maximum (utilisation d'un système d'exploitation dédié, suppression de toutes les fonctions inutiles, application immédiate des patchs,etc…).

La protection peut également être décentralisée : un coupe-feu personnel peut être installé sur chaque ordinateur de l'entreprise (distibuted firewall). De nombreux logiciels coupe-feu existent sur le marché, et Windows XP Pro en comporte un en standard. Cette solution décentralisée présente plusieurs inconvénients :

- elle complique la tâche de l'administrateur du réseau ;
- elle ne permet pas de partager des fichiers ou des périphériques (ex : imprimante) ;
- elle est incompatible avec l'usage d'un serveur web personnel (Personnal Web Server).

Le coupe-feu personnel devrait donc être réservé aux ordinateurs des particuliers qui ont une liaison permanente avec internet (via le câble ou l'ADSL), mais qui ne sont pas reliés à un réseau local.

La protection d'un serveur web public est également possible mais elle est nettement plus difficile à assurer que celle d'un réseau local, et le firewall ne constitue pas la panacée universelle. De nombreux coupe-feu ont été traversés par les ***vers CodeRed*** et ***Nimda*** au cours de l'année 2001, si bien que certains webmasters préfèrent transformer leur serveur web en bastion, plutôt que de faire confiance à un firewall quel qu'il soit. On notera qu'un serveur web fonctionnant en simple serveur de fichiers est plus facile à protéger qu'une machine fonctionnant aussi en serveur d'applications. On notera également qu'il est extrêmement difficile de se protéger contre une attaque de type ***DoS*** (***Deny of Service***) bien conduite.

CONCLUSIONS

L'installation d'un serveur proxy ne se justifie que dans la mesure où l'on veut **enregistrer** (ou plus encore, **réglementer**) l'accès d'une communauté d'internautes au web. Les autres arguments généralement invoqués – l'accélération des accès grâce au cache, la sécurité – ne sont le plus souvent que de faux-semblants. Il faut reconnaître que l'intérêt du proxy provient de son fichier journal, dans lequel sont enregistrées toutes les opérations effectuées par les internautes.

Si le cache joue effectivement un rôle positif, que l'on rende donc l'usage du proxy ***facultatif***. Ainsi, les internautes pourront faire leur propre expérience, et juger par eux-mêmes des avantages et des inconvénients du serveur proxy. En fait, il est rarissime que le service informatique d'une entreprise agisse de la sorte. Autoritarisme ou crainte du résultat ?

Le rôle de sécurité du proxy est un leurre. Mieux vaut utiliser un firewall **correctement configuré** – ce qui n'est pas une mince affaire. On a dit et répété que 300 000 serveurs avaient été compromis par le ver Nimda au cours de ces six derniers mois, mais on oublie d'ajouter que bon nombre d'entre eux étaient **« protégés »** par un firewall. Car les hackers savent eux aussi comment on configure un coupe-feu, et l'attaquant a toujours une longueur d'avance sur le défenseur. En matière de sécurité informatique, il n'y a ni recette miracle, ni solution définitive.

(Source : Web) C.B.

Références Web :

(1) www.netcraft.com/survey/
(2) www.ircache.net/
(3) www.nlanr.net/
(4) www.squid-cache.org
(5) wwwcache.ja.net
(6) www.informationweek.com/815/cdvendors.htm
(7) www.web-caching.com/cdns.html
(8) www.webreference.com/internet/software/site_management/cdns.html
(9) www.esi.org
(10) www.webspy.com/microsoft/index.asp
(11) www.ripe.net/perl/whois
(12) tools.rosinstrument.com/proxy/
(13) www.samair.ru/xwww/proxy.htm
(14) rr.sans.org/signup/login.php ?9e098a7c1d1a2e413f88466a1f23fede

Chiffrement et cryptographie

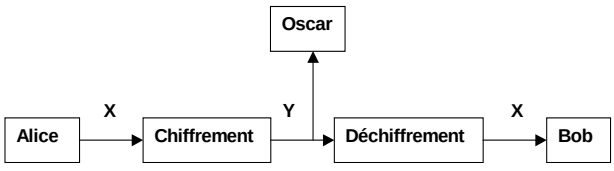
L'explosion des réseaux que nous connaissons actuellement remet au devant de l'affiche des problèmes de sécurité dans les transmissions de données. Ces problèmes ne sont pas nouveaux car ils sont apparus à la fin des années 1970 avec l'émergence des réseaux de communication internes aux entreprises. Les protocoles cryptographiques ont été inventés pour établir une connexion confidentielle entre deux interlocuteurs d'un réseau. En Europe, on trouve assez peu d'ouvrages techniques ou de sites Internet concernant le chiffrement alors qu'au contraire aux Etats-Unis c'est un sujet très populaire.

Il ne faut pas penser comme beaucoup de gens le croient encore aujourd'hui, que l'utilisation de moyens de chiffrement est récente. En effet, la cryptographie est vieille de plus de 2000 ans puisque des études menées par Jean-François Champolion en 1932 ont montré que ce n'est pas 1 mais 3 modes de chiffrement qui furent utilisés par les Egyptiens dans leur écriture hiéroglyphique. Des civilisations anciennes telles que l'Egypte, la Grèce ont utilisé très tôt des techniques pour rendre leurs communications secrètes, et ce sont eux les précurseurs de la science du chiffrement. Cette science a beaucoup évolué depuis ses origines, surtout depuis l'apparition des traitements automatisés de l'information, mais les principes anciens restent encore d'actualité aujourd'hui.

DÉFINITIONS

Le chiffrement est la transformation d'une information intelligible (ex: un texte de départ) en une information qui ne pourra pas être comprise par des personnes qui ne seraient pas autorisées à lire cette information. C'est l'idée de base à toujours garder en tête. Aussi l'objectif fondamental de la cryptographie est de permettre à deux personnes, appelées traditionnellement Alice et Bob, de communiquer par l'intermédiaire d'un canal de transmission ***public*** (ligne de téléphone, réseau …) sans qu'un espion éventuel appelé Oscar en comprenne le sens. Le message de départ qu'Alice envoie à Bob noté X , peut être un simple texte dans une langue naturelle, une image, une musique, ou tout autre forme de données numériques. Alice transforme le message de départ X par un procédé de chiffrement (ou ***codage***) noté K en un message Y , et l'envoie alors à Bob. Oscar qui espionne le canal de transmission ne peut pas comprendre le message car il ne connaît pas la façon de procéder pour le déchiffrer (ou ***décoder***). Ce n'est pas le cas de Bob, qui peut appliquer le procédé inverse à celui d'Alice, et transformer le message chiffré Y pour qu'il soit identique au message X d'origine.

Le message est couramment appelé ***texte en clair***. Le processus de transformation d'un message, de telle manière à le rendre incompréhensible, est appelé ***chiffrement*** (ou ***encryption***). Le résultat de ce processus de chiffrement est appelé ***texte chiffré*** (ou ***cryptogramme***). Le processus de reconstruction du texte en clair à partir du texte chiffré est appelé ***déchiffrement*** (ou ***décryptage***).



L'art et la science de garder le secret des messages est appelé ***cryptographie*** et elle est pratiquée par les ***cryptographes***. Les ***cryptanalystes*** quant à eux pratiquent la ***cryptanalyse*** qui est l'art de décrypter des messages chiffrés. La branche des mathématiques qui traite de la cryptographie et de la cryptanalyse s'appelle la ***cryptologie*** et ses pratiquants sont appelés ***crpytologues***. De nos jours, presque tous les cryptologues sont des mathématiciens théoriciens par la force des choses.

POURQUOI CHIFFRER ?

Avant l'utilisation massive des ordinateurs, les principaux utilisateurs de moyens de chiffrement furent les gouvernements et les militaires. Pour ces utilisateurs, le besoin de ***conserver le secret*** de leurs communications était primordial. Ce n'est seulement qu'après les années 60, que la cryptographie a commencé à être utilisée à des fins non plus strictement gouvernementales, mais également privées. Ceci s'explique par le développement de l'informatique, des télécommunications, et des réseaux (Internet) qui ont augmenté considérablement le nombre d'informations échangées dans le monde. Aujourd'hui, le chiffrement est toujours une ***arme*** très importante pour les militaires, mais elle est également très utilisée par les banques et les institutions financières (cartes de crédit, …) et par les entreprises. On peut constater également que depuis ces dix dernières années, elle entre dans nos vies de tous les jours par l'intermédiaire du courrier électronique (protection des informations personnelles) et de l'Internet en général (commerce électronique, jeux, …).

Le chiffrement à deux problèmes majeurs à résoudre. Le premier est la ***protection*** des données enregistrées sur des supports de masse (CD-ROM,…) ou échangées sur le réseau contre des destructions ou des modifications non voulues. C'est ce que l'on nomme le problème de la ***confidentialité***. Protéger les informations importantes d'une entreprise devient de plus en plus essentiel pour maintenir un niveau de compétitivité suffisant. Le vol ou la destruction (ou endommagement) de données confidentielles ou importantes (***hacking, espionnage industriel***) entraîne pour une entreprise des dommages financiers très coûteux. C'est pourquoi elles se doivent de se protéger en utilisant des méthodes de chiffrement efficaces qui ne pourront pas être trop facilement brisés par des esprits malveillants.

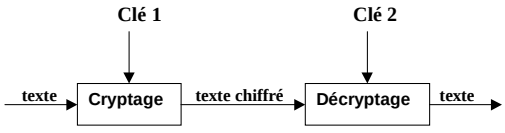
Le chiffrement permet souvent l'***authentification***, c'est à dire de s'assurer de l'identité d'une personne; que celle-ci est bien celle à qui l'on s'adresse sans aucun doute possible. Dans le même ordre d'idées, elle permet un filtrage d'accès, c'est-à-dire, de limiter et de contrôler l'ensemble des personnes ayant un droit d'accès sur des informations de diverses natures. Enfin, la cryptographie peut garantir l'envoi d'une information et sa réception sans que l'émetteur, ni le récepteur puissent nier la transaction ainsi que son contenu (très important pour le commerce électronique). On parle alors en droit de ***non-répudiation***.

PRINCIPALES MÉTHODES EXISTANTES

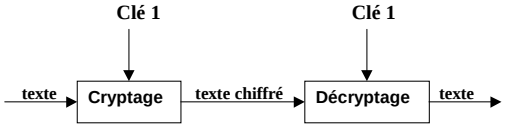
Les méthodes utilisées par la cryptographie moderne ne peuvent être employées par l'être humain. Des algorithmes complexes ont été conçus et sont exécutés sur des ordinateurs ou des dispositifs matériels spécialisés. Dans la plupart des applications, le chiffrement est opéré par des moyens logiciels, et de nombreux kits de logiciels de chiffrement/déchiffrement sont disponibles.

Avant l'apparition des ordinateurs, la sécurité du chiffrement reposait sur le secret des opérations réalisées (***méthodes de substitution ou de transposition***) et il suffisait de connaître la façon de coder, pour pouvoir décoder très facilement (chiffrement ***restreint***). Actuellement, ces méthodes n'ont plus aucun intérêt car dans la pratique, elles sont très vite cassées par les cryptanalystes et les pirates. Les nouveaux algorithmes de chiffrement utilisés sont publics, et leur sécurité repose sur le concept des clés.

On distingue deux classes d'algorithmes à base de clés: les premiers sont dits ***symétriques***, et les seconds ***asymétriques*** (voir. Figure ci-dessous). La différence est que les algorithmes symétriques utilisent la même clé pour chiffrer et déchiffrer, alors que les seconds utilisent une clé de déchiffrement différente de la clé de chiffrement.



Chiffrement Asymétrique



Chiffrement Symétrique

Dans le cas des algorithmes asymétriques, la clé de chiffrement est souvent appelée ***clé publique*** et la clé de déchiffrement ***clé privée*** .

La cryptographie est une science en perpétuelle évolution, et de nombreuses recherches en la matière sont réalisées dans des laboratoires du monde entier. Le but de ces recherches est de rendre les méthodes de chiffrement de plus en plus sûrs. Le futur reste cependant toujours incertain, puisqu'on a du mal à imaginer quelle sera la puissance réelle des ordinateurs de demain. Cependant depuis quelques années, tous les regards sont tournés vers les progrès réalisés en matière de ***physique quantique*** qui pourraient être spectaculaires et très prometteurs s'ils sont appliqués à la cryptographie. Apporteront-ils la sécurité infaillible que l'on recherche depuis toujours ? Est-ce que les algorithmes à base de clés seront un jour dépassés et ne pourront plus subvenir aux besoins en matière de sécurité et de fiabilité ?

De nombreux algorithmes de chiffrement sont disponibles sur Internet (mais c'est encore illégal d'en importer un certain nombre d'entre eux !). Le ***DES*** et l'***IDEA*** sont les exemples les plus fameux des algorithmes symétriques. ***RSA*** , quant à lui, est l'application la plus répandue en matière de chiffrement asymétrique. Un premier algorithme quantique est déjà disponible, mais il n'en est encore qu'au stade de démonstration.

ASPECT TECHNIQUES DU CHIFFREMENT

Il y a trois grandes classes dans les systèmes de chiffrement :

- classiques (substitutions, transpositions)
- modernes (clé publique, clé privée)
- futures (quantique, …)

La cryptographie classique décrit la période avant les ordinateurs. Elle traite des systèmes reposant sur les lettres et les caractères d'une langue naturelle (allemand, anglais, français,…). Les principaux outils utilisés remplacent des caractères par des autres et les transposent dans des ordres différents. Les meilleurs systèmes (de cette classe d'algorithmes) répètent ces deux opérations de base plusieurs fois. Cela suppose que les procédures (chiffrement et déchiffrement) soient gardées ***secrètes*** ; et sans cela, le système est complètement inefficace. On appelle cette classe de méthodes : le chiffrement à ***usage restreint***.

Les méthodes utilisées de nos jours sont plus complexes, cependant la philosophie reste la même. La différence fondamentale est que les méthodes modernes (les algorithmes, puisque l'on utilise maintenant des ordinateurs) manipulent directement des bits (liés à l'implantation sur les machines) contrairement aux anciennes méthodes qui opéraient sur des caractères alphabétiques. Ce n'est donc qu'un changement de taille (ou de représentation), puisque l'on utilise plus que deux éléments au lieu des 26 lettres de l'alphabet. La plupart des bons systèmes de cette catégorie combinent toujours des substitutions et des transpositions, et les règles sont connues de tous, c'est pourquoi on appelle cette classe : le chiffrement à ***usage général*** . La sécurité de ces méthodes repose maintenant sur un nouveau concept : ***les clés*** .

CHIFFREMENT CLASSIQUE

Il existe des centaines de façon de chiffrer des données représentées par l'alphabet classique, tout en gardant les opérations réalisées secrètes.

1) - Substitution

La substitution consiste à effectuer des dérivations pour que chaque caractère du message chiffré soit différent des caractères du message en clair. Le destinataire légitime du message applique la dérivée inverse au texte chiffré pour recouvrer le message initial. La complexité des systèmes à substitutions dépend de trois facteurs :

- la composition spécifique de l'alphabet utilisé pour chiffrer ou pour communiquer ;
- le nombre d'alphabets utilisés dans le cryptogramme;
- la manière spécifique dont ils sont utilisés.

a) *substitution simple ou monoalphabétique*

Chaque caractère du texte en clair est remplacé par un caractère correspondant dans le texte chiffré. Les exemples les plus célèbres sont les algorithmes de ***César*** , ***Rot13*** et bien évidemment le code morse. Ils sont encore utilisés aujourd'hui pour cacher le sens de certains messages (ex: solution de certains jeux dans les journaux), mais ils sont très peu sûrs. En effet avec ce principe, les lettres les plus fréquentes dans le texte en clair restent les plus fréquentes dans le texte chiffré, il ne cache donc pas les fréquences

d'apparition des caractères. C'est une faiblesse importante puisque des techniques statistiques peuvent être utilisées pour associer aux lettres les plus fréquentes, une lettre probable et, en appliquant une technique sémantique récursive, les algorithmes à base de substitutions monoalphabétiques sont facilement cassés par les spécialistes.

Ex: texte en clair = " Non je ne suis pas fou "
texte chiffré (5 divisions) = "abawr arfhv fcnfs bh"

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

N O P Q R S T U V W X Y Z A B C D E F G H I J K L M

Dictionnaire ROT13

b) *substitution homophonique*

Comme pour le principe précédent sauf qu'à un caractère du texte en clair on fait correspondre plusieurs caractères dans le texte chiffré. Par exemple, "A" peut correspondre à 15, 13, 25 ou 56 ; "B" à 7, 19, 31, ou 42 ; … .Ce procédé est plus sûr, mais également craqué par les spécialistes expérimentés.

Ex: texte en clair = " changeons les mentalités suisses "
texte chiffré = " 3811475151419 383119
13311420138946545 1947945193145 "

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
---
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
27 28 29 30 31 32 33 34 35 36 37 …

c) *substitution polyalphabétique*

Le principe consiste à remplacer chaque lettre du message en clair par une nouvelle lettre prise dans un ou plusieurs alphabets aléatoires associés. Par exemple, on pourra utiliser "n" substitutions monoalphabétiques ; celle qui est utilisée dépend de la position du caractère à chiffrer dans le texte en clair. On choisit une clé qui sert d'entrée dans la grille polyalphabétique incluant autant de symboles qu'il y a de lettres différentes à chiffrer. Chaque caractère de la clé désigne une lettre particulière dans la grille de codage. Pour coder un caractère, on doit lire le caractère correspondant du texte en clair en utilisant la grille polyalphabétique et le mot clé associé dans l'ordre séquentiel (on répète la clé si la longueur de celle-ci est inférieure à celle du texte de départ). Les exemples les plus célèbres sont les algorithmes de ***Vigenère*** et de ***Beaufort***. L'illustration la plus simple qui corresponde à ce principe est l'utilisation d'une fonction "**à base de**" ou "**exclusif**" (XOR).

Ex: texte en clair = " ABCBACCBA ACBB "
clé = " **DBBCBAACD** "

	ABCD
A	*CBDA*
B	*DCAB*
C	*CABD*
D	*BDAC*

Grille polyalphabétique

texte chiffré = " BCAAD DDABB ACA "

d) *substitution par polygramme*

Les caractères du texte en clair sont chiffrés par blocs. Par exemple, "ABA" peut être chiffré par "RTQ" tandis que "ABB" est chiffré par "SLL". Les exemples les plus célèbres sont les algorithmes de ***Playfair*** et de ***Hill*** inventés en 1854 et utilisés pendant la première guerre mondiale par les Anglais.

Ex: texte en clair = " pour la *léga*lisation de la crypto "
texte chiffré = " cesl as *ococ*rocoquip ik as lekuss "

2) - Transposition

Avec le principe de la transposition toutes les lettres du message sont présentes, mais dans un ordre différent. Il utilise le principe mathématique des ***permutations***. Plusieurs types différents de transpositions existent.

a) *transposition simple par colonnes*

On écrit le message horizontalement dans une matrice prédéfinie, et on trouve le texte à chiffrer en lisant la grille verticalement (voir ex. ci-après). Le destinataire légal pour décrypter le message réalise le

procédé inverse. L'algorithme allemand ADFGFX est fondé sur ce principe et fut utilisé pendant la première guerre mondiale.

Ex: texte en clair = " I love my english teacher "

utilisation d'une matrice [6;4]

I	L	O	V
E	M	Y	E
N	G	L	I
S	H	T	E
A	C	H	E
R			

texte chiffré = " iensa rlmgh coylt hveie e "

b) *transposition complexe par colonnes*

Un mot clé secret (avec uniquement des caractères différents) est utilisé pour dériver une séquence de chiffres commençant à 1 et finissant au nombre de lettres composant le mot clé. Cette séquence est obtenue en numérotant les lettres du mot clé en partant de la gauche vers la droite et en donnant l'ordre d'apparition dans l'alphabet. Une fois que la séquence de transposition est obtenue, on chiffre en écrivant d'abord le message par lignes dans un rectangle, puis on lit le texte par colonnes en suivant l'ordre déterminé par la séquence.

Ex: texte en clair = " I love my english teacher "
mot clé = " **SERGIO** "

S	**E**	**R**	**G**	**I**	**O**
6	*1*	*5*	*2*	*3*	*4*
I	**L**	**O**	**V**	**E**	**M**
Y	**E**	**N**	**G**	**L**	**I**
S	**H**	**T**	**E**	**A**	**C**
H	**E**	**R**			

texte chiffré = " lehev geela micon triys h "

c) *transposition par carré polybique*

Un mot clé secret est utilisé pour construire un alphabet dans un tableau. Les coordonnées des lignes et des colonnes correspondant aux lettres du texte à chiffrer sont utilisées pour transcrire le message en chiffres. Avec ce procédé chaque lettre du texte en clair est représenté par deux chiffres écrit verticalement. Ces deux coordonnées sont ensuite transposées en les recombinant par deux sur la ligne ainsi obtenue.

Ex: texte en clair = " Cryptology is a passionate topic "

	1	*2*	*3*	*4*	*5*	*6*
1	**S**	**E**	**R**	**G**	**I**	**O**
2	**A**	**F**	**T**	**P**	**K**	**M**
3	**L**	**N**	**Z**	**Y**	**U**	**X**
4	**W**	**Q**	**B**	**V**	**C**	**H**
5	**J**	**D**	**&**	**'**	**#**	**}**
6	**%**	**$**	**£**	*****	**°**	**§**

texte en clair (coordonnées) :

" ***41***32***21***311311222111132121214 "
" 534436164451242115623236455 "

texte fractionné, groupé par 2 et recombiné en coordonnées :

"***41***32***21***31***13***11***22***21***11***11***32***12***12***14***53***44***36***16***44***51***24***21***15***62***32***36***45***5"
" ***G*** T ***E*** R ***L*** S ***F*** E ***S*** S ***T*** A ***A*** W ***U*** V ***£*** % ***V*** I ***Q*** E ***J*** M ***T*** £ ' 5 "

texte chiffré avec divisions des mots :

" gterl sfess taawu v£%vi qejmt £'5 "

Il est important de remarquer que les transpositions sont plus contraignantes que les substitutions, car elles ont besoin de plus de mémoire et ne fonctionnent que sur des messages à chiffrer d'une longueur limitée ; c'est pourquoi elles sont moins utilisées dans les algorithmes même si elles sont plus sûres que les substitutions.

CHIFFREMENT MODERNE

Les algorithmes de chiffrement contemporains sont peu sûrs en général ; le cassage du programme ***Fantasia*** pendant la deuxième guerre mondiale reposant à la fois sur des transpositions et des substitutions combinées atteste de la vulnérabilité de ces techniques.

Le chiffrement moderne utilise la puissance des ordinateurs modernes. Comme les données traitées par les ordinateurs sont uniquement sous forme numérique (bits), les procédés de substitutions et de transpositions sont toujours utilisées mais maintenant seulement sur deux éléments primaires (0 et 1).

Ce changement de dimension rend plus sûr les techniques de chiffrement actuelles. Certains sont incassables, ou du moins prendraient des millions d'années avec la puissance actuelle de nos meilleurs super-calculateurs. D'autre part, les algorithmes actuels ne sont plus cachés mais au contraire sont connus de tous. Les clés sont leur sécurité.

1) - Chiffrement symétrique

Les systèmes symétriques sont synonymes de systèmes à clés secrètes. Une même clé est utilisée pour le chiffrement et le déchiffrement, d'où l'obligation que celle-ci reste confidentielle, sous peine de rendre le système inéfficient.

a) *théorie*

L'émetteur (Alice) et le destinataire (Bob) doivent se mettre d'accord préalablement sur la clé (k) à utiliser. Pour ceci ils ne doivent pas utiliser le réseau de communication standard qui est susceptible d'être espionné par Oscar. Chaque fois qu'Alice veux transmettre un message (m) à Bob, elle utilise sa clé secrète pour chiffrer, et elle envoie le résultat de ce chiffrement par l'intermédiaire du même canal. Bob utilise à son tour la même clé secrète et le même algorithme public pour déchiffrer le message codé qu'il a reçu.

Les problèmes de cette technologie sont :

- si la clé secrète est compromise (volée, extorquée, piratée, …) par un opposant, alors ce dernier pourra déchiffrer tous les messages encodés avec celle-ci. Oscar peut même se faire passer pour Alice ou Bob ;
- les clés doivent être distribuées secrètement: c'est très difficile à l'échelle planétaire;
- si une clé différente est utilisée pour chaque paire différentes d'utilisateurs du réseau, le nombre total des clés augmente très rapidement en fonction du nombre total d'utilisateurs.

b) *The Data Encryption Standard*

Le ***D.E.S.*** est un standard mondial depuis plus de 15 ans. Il a été développé en 1976 par IBM pour le N.B.S. (National Bureau of Standards) avec pour objectif de fournir un nouveau standard pour limiter la prolifération d'algorithmes différents qui ne pouvaient pas communiquer entre eux. Bien qu'il montre des signes de vieillesse, il a remarquablement bien résisté à des années de cryptanalyse et il est toujours sûr contre tous les adversaires excepté peut-être les plus puissants. Il est devenu le système de chiffrement le plus utilisé dans le monde. Depuis son adoption, le D.E.S. a été réévalué environ tous les 5 ans et sa plus récente version date de 1998.

C'est un algorithme à clé secrète, il chiffre un bloc de texte clair de 64 bits en utilisant une clé de 56 bits, pour obtenir un bloc de texte chiffré de 64 bits. Il utilise les deux grandes lois de ***Shannon*** : diffusion (en utilisant des permutations) et confusion (en utilisant des substitutions) de bits pour casser la fréquence d'apparition des lettres dans le texte en clair, et compliquer le lien entre le fichier encodé et la clé secrète utilisée. Il repose sur 16 itérations imbriquées, et avec une clé suffisamment longue et pas trop simple, sa résistance aux différentes attaques possibles est bonne.

Il reste très utilisé dans le domaine commercial et les banques. Il est implanté dans de nombreuses cartes de crédits. Son principal avantage est d'offrir une vitesse de chiffrement et déchiffrement assez élevée.

2) - Chiffrement asymétrique

Ces algorithmes sont aussi synonymes d'algorithmes à clés publiques. Une clé différente est utilisée à la fois pour chiffrer et déchiffrer et il est impossible de générer une clé à partir de l'autre. Il a été inventé en 1975 par deux ingénieurs en électronique : Whitfield Diffe et Matin Hellman de l'Université de Stanford.

a) *théorie*

Une des difficultés principales de cette méthode est que chaque couple potentiel d'utilisateurs doit posséder sa propre clé secrète et se l'échanger par un moyen sécurisé avant leur premier échange d'informations, ce qui peut s'avérer difficile à réaliser dans la pratique. Le but d'un système à clé publique

est de résoudre ce problème. La clé publique est généralement publiée dans un répertoire. L'avantage est donc qu'Alice peut envoyer un message à Bob sans communication privée préalable (elle choisit sa clé privée et la clé publique de Bob). Bob est la seule personne à pouvoir déchiffrer le message en appliquant sa clé secrète et personnelle, et la clé publique d'Alice. On dit généralement que chaque clé déverrouille le code produit par l'autre. Avec ce système même Alice, qui a chiffré un message pour Bob, ne pourra déchiffrer le message ainsi codé. C'est un des systèmes les plus évolués que l'on peut actuellement trouver.

La première application de ce principe fut le chiffrement ***R.S.A.*** . Depuis, plusieurs systèmes ont été proposés. Leur sécurité repose sur divers problèmes calculatoires, et notamment la théorie des grands nombres.

b) *R.S.A.*

Cet algorithme a été inventé par ***Rivest R. , Shamir A. et Adlemann L.*** du M.I.T. (Massachussets Institute of Technology). C'est l'algorithme à clé publique le plus commode qui existe. Comme pour le D.E.S. sa sécurité repose sur l'utilisation de clés suffisamment longue (512 bits n'est pas assez, 768 est modérément sûr, et 1024 bits est une bonne clé). C'est la difficulté que l'on a à factoriser les entiers premiers (le problème des logarithmes discrets est souvent considéré comme insurmontable) qui font que l'on ne peut que difficilement casser cet algorithme. Cependant, de larges avancées en matière de factorisation des entiers larges, ou une augmentation considérable de la puissance de nos super-calculateurs rendront R.S.A. très vulnérable.

R.S.A. est aujourd'hui utilisé dans une large variété de produits (téléphones, réseaux Ethernet, …), de logiciels de différentes marques (Microsoft, Apple, Novell, Sunn) et dans des industries.

3) - Chiffrement mixte et authentification

Les algorithmes à clé publique sont assez lents. La méthode généralement utilisée pour envoyer un message, est de tirer au hasard une clé secrète, chiffrer le message avec un algorithme à clé privée en utilisant cette clé, puis chiffrer cette clé aléatoire elle-même avec la clé privée. Il existe un logiciel qui effectue toutes ces opérations et de manière transparente, et qui de plus, est gratuit et téléchargeable à partir de dizaines de sites dans le monde : le célèbre ***PGP*** de ***Phil Zimmermann***.

Correctement utilisé, il est sûr, même contre les meilleures cryptanalystes du monde.

L'authentification permet de prouver son identité à travers le réseau. Il utilise généralement la technique des signatures électroniques. L'envoyeur joint une signature électronique à son message.

CHIFFREMENT DU FUTUR

Tous les systèmes étudiés précédemment prenaient pour acquis que les communications numériques pouvaient être toujours espionnées d'une façon passive (c'est à dire sans détecter une modification éventuelle de l'intégrité des données échangées) ou enregistrées par un tiers pour un usage futur, même si ce dernier ne peut en comprendre le sens.

La cryptographie quantique est née au début des années 70. Elle repose sur ***le principe d'incertitude d'Heisenberg***, selon lequel la mesure d'un système quantique perturbe ce système. Une oreille indiscrète sur un canal de transmissions quantique engendre des perturbations inévitables qui alertent les utilisateurs légitimes. Ainsi, il est possible de distribuer une clé secrète aléatoire à deux utilisateurs qui ne partagent initialement aucun secret, de façon sécurisée contre des espions même de puissance de calcul infinie. Une fois cette clé secrète établie, elle peut être utilisée avec un système cryptographique classique. On obtient ainsi des preuves de sécurité reposant uniquement sur la correction des principes quantiques.

Les systèmes quantiques sont toujours à un stade expérimental, cependant depuis 1992, ils ont quitté le stade de la Science-Fiction depuis que ***Benett*** et ***Brassard***, deux chercheurs américains ont construit un prototype fonctionnant sur une courte distance (env. 1 Km). Cette approche souffre aujourd'hui du désavantage que les transmissions quantiques sont très faibles et sont difficilement amplifiables par la route, et que la polarisation des photons posent encore des problèmes en raison de l'imperfection de l'appareil lui-même.

Seul le futur nous dira si cette nouvelle approche, un peu plus compliquée puisque reposant directement sur la physique quantique, remplacera les systèmes utilisés actuellement. Cependant, pour l'instant les réponses aux problèmes posés restent incertaines, ce

qui permet encore de beaux jours aux D.E.S. , R.S.A. et autres standards du chiffrement moderne.

CONCLUSION

Le chiffrement est un sujet très intéressant du point vue technique. Ses enjeux sont également très importants et il faut en avoir conscience dès aujourd'hui. Il est à parier que le chiffrement jouera un rôle encore plus important au XXI e siècle dans une société totalement mondialisée et c'est nous qui en serons alors les principaux utilisateurs et bénéficiaires. D'ailleurs le phénomène est déjà en marche avec le développement du commerce électronique, assez significatif ces derniers temps…

(Source : Web) C.B.

Sorties et activités

Au vu du succès remporté par la visite de Skyguide du 10 octobre dernier, visite qui nous a expliqué le fonctionnement de l'entreprise Skyguide ainsi que le métier des aiguilleurs du ciel, nous serons en pleine forme pour organiser l'année prochaine de nouvelles sorties et visites.

Contrairement à ce qui était encore prévu pour cette année, la sortie karting aura lieu aux alentours du mois de février 2003 . Un courrier sera envoyé.

Pour le reste du programme, il faudra patienter jusqu'en avril 2003, en lisant le prochain journal de l'ARTech.

Amicalement

M. Berchten

Convocation à l'assemblée générale

le mercredi 4 décembre 2002 à 18h30

au Cercle des Vieux-Grenadiers
Rue de Carouge 92
1205 Genève

Cher(e) membre,

Comme chaque année, il est temps de se retrouver. Des décisions importantes concernant l'association seront prises, alors si vous voulez y participer n'hésitez pas à venir (re)découvrir vos collègues et amis.

Un travail « considérable » a été accompli par le comité. De nouvelles perspectives sont annoncées pour l'association.

Ordre du jour

- Ouverture
- Approbation du PV de l'assemblée générale 2001
- Approbation du PV de l'assemblée générale extraordinaire du 19 mars 2002
- Compte rendu de l'année écoulée
- Rapport du trésorier et des vérificateurs
- Approbation des comptes
- Election du président
- Election du trésorier
- Election du nouveau comité
- Election des vérificateurs des comptes pour le nouvel exercice
- Election de membres d'honneur
- Désignation des experts et des observateurs pour les défenses de diplômes
- Distribution des nouveaux statuts
- Projets pour la nouvelle année
- Propositions individuelles et diverses
- Clôture

Au plaisir de vous rencontrer lors de cette assemblée, je vous présente, cher(e) membre, mes plus amicales salutations.

Didier Moullet
Président

PAUSE – CAFÉ

1– Shake hands

Dans une soirée, le nombre de personnes ayant serré un nombre pair de mains est impair .

Et le nombre de personnes ayant serré un nombre impair de mains, est-il pair ou impair ??

2- Somme digitale

On écrit tous les nombres entiers de 1 à 2002, puis on remplace chacun d'entre eux par la somme des ses chiffres.
On recommence à remplacer chaque nombre par la somme de ses chiffres jusqu'à ne plus avoir que 2002 nombres à un seul chiffre.

Y'a-t-il alors plus de chiffres pairs ou de chiffres impairs ?? Ou autant ??

3- Différences

On écrit encore tous les entiers de 1 à 2002. Cette fois, on remplace deux d'entres eux par leur différence. Puis on prend à nouveau deux des 2001 nombres restants et on les remplace par leur différence.
Au bout de 2001 opérations, il ne reste plus qu'un seul nombre.

Est-il pair ou impair ??

4- Produit

On écrit dans un ordre quelconque tous les nombres de 1001 à 2001 . On enlève alors 1 au premier, 2 au deuxième, 3 au troisième … 1001 au dernier.
On fait alors le produit des 1001 nombres ainsi écrits.

Quelle est la probabilité qu'il s'agisse d'un nombre impair ??

5- Les 2002 points

2002 points sont répartis dans le plan de façon que quatre d'entre eux ne soient jamais alignés. Le nombre de triplets de points alignés est pair.

Le nombre de droites obtenues en joignant ces points de toutes les façons possibles est-il pair ou impair ??

6- Solutions

Shake hands

En totalisant les mains serrées par chaque personne, on trouve deux fois le nombre de poignées de mains, soit un nombre pair. Pour y parvenir, le nombre de personnes ayant serré un nombre impair de mains doit être pair.

Somme digitale

Chacun des nombres non multiples de 9 est remplacé par un nombre compris entre 1 et 8 qui est égal au reste de sa division par 9.
Ces restes étant alternativement pairs et impairs, il y a autant de nombres pairs que de nombres impairs. Tous les multiples de 9 sont remplacés par 9, ce qui donne une majorité confortable aux nombres impairs.

Différences

La différence de deux nombres a même parité que leur somme. L'algorithme revient donc, pour ce qui concerne la parité, à remplacer les 2002 nombres par leur somme. Or la somme des 2002 premiers entiers vaut 1001 X 2003 . C'est un nombre impair. Le dernier nombre sera donc impair.

Les 2002 points

Le nombre de façons de joindre 2002 points 2 à 2 est 1001 X 2001 , soit un nombre impair.
Mais certaines de ces droites contiennent trois points. Elles sont donc comptées trois fois, donc deux de trop (si une droite contient A, B et C, elle est comptée AB, BC et CA). La parité ne change donc pas, et le nombre de droites différentes reste impair.

Impressum	
Editeur :	comité ARTech
Rédaction :	Christophe Battagliero Marc Berchten Didier Moullet
Mise en pages :	Ch. Battagliero
Correspondance :	AGT Case postale 5490 1211 Genève 11 Stand
e-mail :	contact@agtech.ch
Le bulletin de l'AGT :	parait 2x par an
Tirage :	100 exemplaires

ON THE WEB…

Images spatiales

L'agence spatiale canadienne met à disposition une banque d'images et de vidéos sur les astronautes, navettes spatiales et autres satellites. La recherche des documents, plus de 700 disponibles, s'effectue par mots clés, sujet ou catégorie. A voir notamment le survol de la Station spatiale internationale (ISS), ou encore *Soyouz* s'arrimant à cette même station .

www. Space.gc.ca/asc/search_f.asp

Le monde des microbes

Bienvenue au « Microbe Zoo » ! Et attention où vous mettez les pieds… Ce parc d'attractions virtuel du centre de microbiologie de l'université du Michigan est en effet dédié aux microbes de toutes sortes. A DirtLand, un monde jonché de détritus, on apprendra qu'une simple poignée de terre peut contenir plusieurs millions de microbes et des milliers d'espèces. Quelques mètres plus loin, le pavillon des animaux réunit bactéries et autres micro-organismes intimement liés à la vie des mammifères. Une pause au Snack Bar et l'on retrouve *Saccharomyces Cerevisiae*, la fameuse levure de bière, et les non moins célèbres bactéries lactiques. Y'a-t-il des micro-organismes dans l'espace ? L'attraction « Space Adventure » hasarde quelques réponses. « Microbe Zoo » propose ainsi un panorama ludique du monde microbien. Une base de données apporte également les compléments scientifiques et illustrations nécessaires.

commtechlab.msu.edu/sites/dlc-me/zoo/index.html

Tout savoir sur les polymères

Molécules constituées d'un enchaînement répété de petites molécules, les polymères sont partout. Le plastique, le nylon ou bien encore le kevlar… « Macrogalleria » explique de manière détaillée leurs constitutions et met en relief leurs utilisations. Au-delà des polymères synthétiques, on apprendra dans le « Polyquarium » que les dauphins fabriquent un polymère naturel. Ce mucus leur permettrait d'augmenter leur vitesse de nage en diminuant les turbulences induites au voisinage de leur peau. Une dizaine de thèmes sont déclinés. On trouvera démonstrations et expériences, ainsi qu'une bibliothèque complète pour en savoir plus.

www.psrc.usm.edu/macrog/new.htm

C.B.