40 NOV./DÉC. 2008

France Métro : 8 € / DOM : 8,80 € / TOM Surface : 990 XPF / TOM Avion : 1300 XPF / CH : 15,50 CHF BEL, LUX, PORT.CONT : 9 Eur / CAN : 15 $CAD

MISC

Multi-System & Internet Security Cookbook

100 % SÉCURITÉ INFORMATIQUE

INFOWAR

La guerre de l'information dans le conflit russo-géorgien

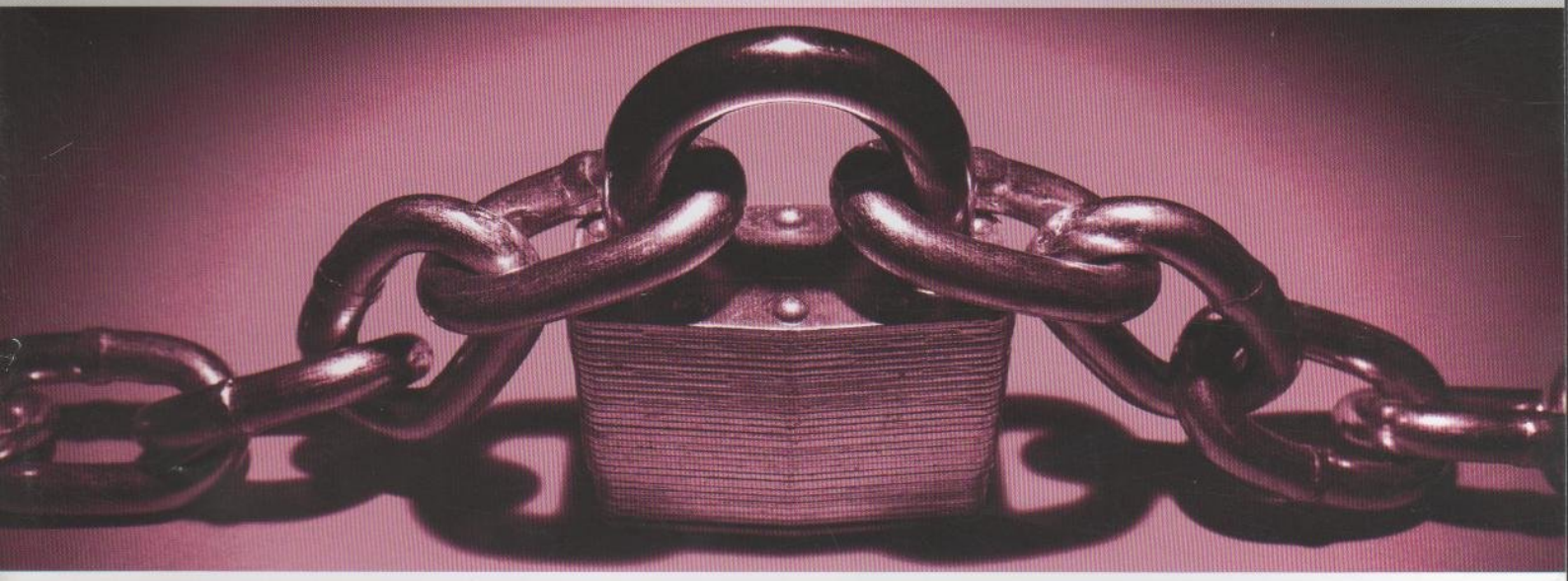
Information, désinformation, infowar, cyber-attaques, brouillard informationnel... Quand le conflit devient cyber-conflit ! (p. 4)

DOSSIER

SÉCURITÉ DES RÉSEAUX

LES NOUVEAUX ENJEUX

- Évolutions technologiques
- Contrôle de la sécurité
- Tests : émuler et éprouver ses architectures



SCIENCE

La biométrie en question : solution ou illusion ? (p. 70)

SYSTÈME

Comprendre les rôles et la technologie RBAC, Role-Based Access Control, de Solaris™ et d'OpenSolaris. (p. 60)

CRYPTOGRAPHIE

Le Match On Card (MOC) ou comment une carte à puce peut identifier son porteur. (p. 14)

L 19018 - 40 - F: 8,00 € - RD

ÉDITO ▶ Jeunesse, lève-toi !

J'ai l'étrange impression que nous vivons un changement assez radical sans pour autant bien en saisir encore les implications. Certes, le monde a évolué et, si ma grand-mère, dans son infinie sagesse, a vu naître l'informatique pendant la 2ème Guerre Mondiale, mes neveux, dans leur quête de la plus grosse bêtise, sont nés avec un téléphone portable, le WiFi et Laurence Ferrari au 20h de TF1.

Une des moultes questions qui hantent les méandres de mes synapses, c'est comment mes neveux arriveront à acquérir puis dépasser la sagesse de ma grand-mère (qui se trouve également être leur arrière-grand-mère... si vous êtes déjà largués, reposez tout de suite ce magazine et soufflez dans l'alcootest). Ça va être difficile, mais ils vont s'accrocher, ils sont *petits mais costauds*.

Je me trouvais à Limoges, inestimable capitale de la région limousine, connue et appréciée pour ses vaches, ses assiettes en porcelaine et Cédric B., auteur du *Worldwide security conferences happy guide* **[1]**. On notera d'ailleurs qu'on retrouve dans ce dernier (Cédric, pas le guide) l'allure charnue des premières et la rondeur des deuxièmes. Mais, je m'égare. Tellement il voyage, le Sid, qu'il fait à lui tout seul du *ciel le plus bel endroit de la Terre*.

J'étais donc à la fac pour signer des autographes, me faire harceler par des groupies et, accessoirement, dispenser mon savoir. Je profitais de discuter avec une fan de la promo précédente pour la pousser à écrire dans ces pages. Réponse laconique : « oualala, mais j'ai pas le niveau » ! Texto (pas sms, ça veut dire « littéralement ») ! Fausse idée numéro 1. *N'imitez pas, innovez* !

Un peu plus tard, en discutant avec quelques étudiants, l'un d'entre eux me demande si on peut avoir une vie en dehors de la sécurité, conserver sa copine ou même aller au cinéma. Des trucs de dingues quoi ! Un autre m'avait posé une question semblable quelques mois plus tôt. Fausse idée numéro 2. *On a tous besoin d'une pause lotus*.

Je ne sais pas quelle perception les petits ont du monde de la sécurité, mais ce n'est pas tout à fait ça.

Certes, c'est une discipline difficile et exigeante, on est souvent confronté à l'échec et on devient parano si on ne l'était pas. Mais c'est pareil pour tout le monde et, à un moment, il faut se lancer. Allez hop, jeunesse, lève-toi, comme qui dirait. Quid de l'insouciance, de l'astuce, de l'espièglerie ? Secouez-vous, *vous le valez bien* !

Que ce soit dans cette revue ou à SSTIC, on a toujours essayé d'encourager les vocations. Le but n'est pas de s'entendre dire ensuite que c'est trop balaise : *au loto, 100% des gagnants ont tenté leur chance*.

Alors, certes, je suis fier que ce journal et cette conférence pour lesquels je me suis beaucoup dépensé (et beaucoup d'autres aussi) soient maintenant reconnus. Mais, les considérer comme inaccessibles, ça m'énerve. *Ils sont assurément humains*.

Quant à la vie en dehors de la sécurité, il est nécessaire de beaucoup bosser au début, c'est vrai, pour acquérir des connaissances variées. Mais, pour autant, chaque jour, c'est du bonheur à tartiner. De plus, le néo-sportif que je suis vous dira que ça fait du bien de s'aérer : l'esprit aussi a besoin de repos, c'est indispensable *pour faire durer le plaisir*.

De plus en plus de personnes compétentes sortent des nombreuses formations liées à la sécurité. Malheureusement, quand elles se retrouvent confrontées à la vie en entreprise, avec une hiérarchie qui ne comprend pas forcément grand-chose et une inertie pesante, forcément, ça décourage. À côté de ça, les 2 initiatives qui ont généré le plus de mouvements ces dernières années (selon une source à la fiabilité douteuse : moi), le challenge SecuriTech et SSTIC, sont nées de l'effort de quelques-uns, en dehors de tout cadre. Faut-il en conclure que les structures (entreprises ou autres) ne servent à rien ? Certainement pas : elles permettent de pérenniser et valoriser les initiatives. Mais pour cela, encore faut-il des choses à pérenniser et valoriser : lancez donc des initiatives *conçues pour faire la différence* !!!

Bref, je me demande vraiment d'où viennent ces fausses idées. Mais une chose est sûre : c'est un domaine passionnant en pleine mutation. Du « piratage » du compte en banque de notre président à la lutte informatique offensive, de nombreuses initiatives sont à lancer. N'oubliez pas, *l'ingrédient le plus actif, c'est vous*.

Alors, envoyez-moi vos articles, soumettez à SSTIC **[2]** et, plus généralement, bougez-vous et *vous ne viendrez plus chez nous par hasard*. Osez !!!

Bonne lecture,

Fred Raynal

P. S. 1 : Merci à Cédric Llorens pour s'être occupé du dossier pendant ses vacances.

P. S. 2 : Désolé pour la fausse surprise annoncée dans le précédent édito pour le 3 octobre. Devant la profusion d'articles sur la carte à puce, nous avons finalement opté pour faire 2 hors-série, l'un orienté utilisation (*HS Linux Mag* 39), l'autre sécurité (*HS MISC* 2).

[1] http://sid.rstack.org/blog

[2] http://sstic.org

SOMMAIRE ▼

MISC
est édité par **Diamond Editions**
B.P. 20142 - 67603 Sélestat Cedex

Tél. : 03 88 58 02 08
Fax : 03 88 58 02 09
E-mail : cial@ed-diamond.com
Service commercial : abo@ed-diamond.com
Sites : www.ed-diamond.com

www.miscmag.com

LES ÉDITIONS DIAMOND

Printed in Germany / Imprimé en Allemagne
Dépôt légal : à parution
N° ISSN : 1631-9036
Commission Paritaire : 02 09 K80 190
Périodicité : Bimestrielle
Prix de vente : 8 Euros

Directeur de publication : Arnaud Metzler
Chef des rédactions : Denis Bodor
Rédacteur en chef : Frédéric Raynal
Relecture : Dominique Grosse
Secrétaire de rédaction: Véronique Wilhelm
Conception graphique : Kathrin Troeger
Responsable publicité : Tél. : 03 88 58 02 08
Service abonnement : Tél. : 03 88 58 02 08
Impression : Druckhaus Kaufmann (Lahr/Allemagne)
Distribution France :
(uniquement pour les dépositaires de presse)
MLP Réassort :
Plate-forme de Saint-Barthélemy-d'Anjou.
Tél. : 02 41 27 53 12
Plate-forme de Saint-Quentin-Fallavier.
Tél. : 04 74 82 63 04
Service des ventes : Distri-médias :
Tél. : 05 61 72 76 24

Charte du magazine : MISC est un magazine consacré à la sécurité informatique sous tous ses aspects (comme le système, le réseau ou encore la programmation) et où les perspectives techniques et scientifiques occupent une place prépondérante. Toutefois, les questions connexes (modalités juridiques, menaces informationnelles) sont également considérées, ce qui fait de MISC une revue capable d'appréhender la complexité croissante des systèmes d'information, et les problèmes de sécurité qui l'accompagnent.
MISC vise un large public de personnes souhaitant élargir ses connaissances en se tenant informées des dernières techniques et des outils utilisés afin de mettre en place une défense adéquate.
MISC propose des articles complets et pédagogiques afin d'anticiper au mieux les risques liés au piratage et les solutions pour y remédier, présentant pour cela des techniques offensives autant que défensives, leurs avantages et leurs limites, des facettes indissociables pour considérer tous les enjeux de la sécurité informatique.

Daniel Ventre – CNRS/CESDIP – daniel.ventre@gern-cnrs.com

CONFLIT RUSSO-GÉORGIEN ET GUERRE DE L'INFORMATION

mots clés : *conflit / Russie / Géorgie / cyber-attaques / guerre de l'information*

« Ghost Recon commence en 2008 avec des troubles civils en Russie. Des ultra-nationalistes ont pris le pouvoir à Moscou et veulent remettre en vigueur le Rideau de fer. Leur première action est de soutenir clandestinement des factions rebelles en Géorgie et dans les pays baltes... Durant les premières missions du jeu, les Ghosts doivent combattre les forces rebelles d'Ossétie du Sud, du Nord de la Géorgie, qui sont en train de harceler le gouvernement légitime et ses alliés ». Tel est relaté sur Wikipédia **[1]** le scénario du jeu vidéo Ghost Recon **[2]**, distribué en 2001. En 2008, la réalité a partiellement rejoint la fiction. La compréhension et l'analyse aussi objective que possible de ce conflit armé qui a éclaté entre la Russie et la Géorgie, aux enjeux géopolitiques et stratégiques internationaux complexes, sont rendues d'autant plus difficiles qu'un fort brouillard d'information voile le paysage. D'information, de désinformation et même de guerre de l'information il a été fortement question lors de ce conflit. Il y a eu la guerre des communiqués, la propagande, les opérations d'influence : l'information dans la guerre a toujours joué un rôle crucial. Il y a eu aussi des cyber-attaques dont furent victimes les deux belligérants (§1). La cyber-guerre se serait invitée au conflit, dénoncée par le discours politique officiel (§2). Il convient alors d'analyser ces cyber-attaques (§3), opérations civiles ou militaires (§4), et de s'interroger sur leur nature, leur origine et leur place dans le conflit (§5).

1. Opérations dans les cyberespaces russe et géorgien

À compter du 8 août 2008, date que, par simplification, nous retiendrons comme celle du début des hostilités militaires, de nombreux sites internet géorgiens ont été paralysés, leurs serveurs pliant sous le choc d'attaques DDoS, ou bien ont été défigurés. Parmi les sites touchés à compter de cette date et au cours de la semaine qui a suivi, on compte ainsi **[3]** :

- celui du Président Mikhail Saakashvili **[4]** ;
- celui du ministère des Affaires Étrangères **[5]** ;
- celui du Parlement **[6]** ;
- celui du ministère de la Défense **[7]** ;
- celui de la banque nationale de Géorgie **[8]** ;
- celui de la chaîne de télévision Rustavi2 **[9]** ;
- **sosgeorgia.org** (qui fait depuis défiler sur son site un bandeau pour informer les internautes qu'il fait l'objet d'attaques massives de la part des hackers russes) **[10]**.

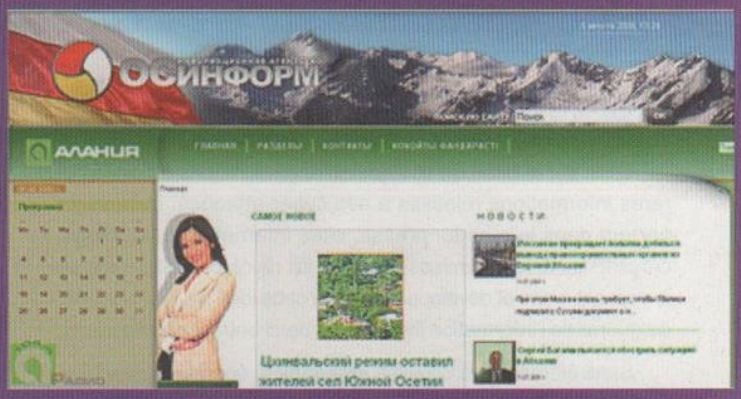
La Géorgie ne fut cependant pas seule touchée par ces opérations de hacking de sites. Ont ainsi été piratés **[11]** :

- le site d'information **skandaly.ru** ;
- le site de l'agence de presse russe RIA-Novosti **[12]** ;

- le site d'information de Russia Today [13] [14] ;
- les sites d'information d'Ossétie du Sud, **osinform.ru** et **osradio.ru**, dont les pages furent remplacées par celles de l'agence d'information géorgienne Alania TV ;
- le site **stopgeorgia.ru** [15] ;
- le site du gouvernement d'Abkhazie [16].

Les ISP géorgiens (Caucasus On-Line et GRENA [17]) ont pour leur part procédé au filtrage de l'internet (sur ordre du gouvernement ?) pour bloquer les sites russes, en guise de mesure défensive, dans la logique de l'Etat d'urgence décrété par le gouvernement.

Nous ne proposons ici aucun tableau chronologique des attaques, car celui-ci n'aurait de valeur qu'en présence d'une liste exhaustive des faits. Une connaissance partielle ne saurait autoriser qu'une représentation erronée du tempo des agressions et des classes de cibles, données essentielles à la recherche d'une éventuelle relation de type attaque/contre-attaque. D'autre part, une telle représentation chronologique ne saurait se satisfaire d'une analyse des faits survenus uniquement au cours des quelques jours du conflit armé. Les attaques enregistrées contre le site du Président géorgien dès le 20 juillet 2008, contre les sites **osinform.ru**, **osradio.ru** le 5 août, sont-elles par exemple des signes avant-coureur [18] ?



Capture d'écran du site osinform.ru dont la page d'accueil a été remplacée par celle d'Alania TV
Capture d'écran publiée le 5 août 2008 sur le site http://www.civil.ge/eng/article.php?id=18896&search=hack

2. Introduction des expressions « cyber-guerre » et « guerre de l'information » dans le conflit

Le ministère des Affaires Étrangères géorgien publie sur son blog de substitution [19] quelques lignes sans équivoque, indiquant qu'« *une campagne de cyber-guerre organisée par la Russie perturbe sérieusement de nombreux sites géorgiens, dont celui du ministère des Affaires Étrangères. Si vous ne pouvez pas accéder aux sites officiels du gouvernement géorgien, consultez les sites suivants, qui vous donneront les dernières informations officielles du gouvernement de la Géorgie :* **http://georgiamfa.blogspot.com**, *le site du Président de la République de Pologne, Lech Kaczynski* **www.president.pl** *(en vous rendant sur le lien d'informations sur les derniers développements en Géorgie)* » [20]. Le post est titré « Des cyber-attaques paralysent les sites internet géorgiens ».

> *...Cyber-guerre et guerre de l'information se sont immiscées dans le discours politique officiel...*

Le site du président polonais affirme par ailleurs que « *parallèlement à l'agression militaire, la Fédération de Russie bloque les portails internet géorgiens* ». C'est pour venir en aide à la Géorgie, par solidarité, et à la demande de M. Saakashvili, que le Président de la République de Pologne [21] a accepté de mettre à disposition son propre site internet pour la dissémination de l'information du gouvernement géorgien [22].

La thèse d'attaques massives et coordonnées par la Russie contre les systèmes d'informations géorgiens est relayée et appuyée par les déclarations de Thomas R. Burling, responsable de l'hébergeur américain Tulip System (petite entreprise dont la PDG, Nino Doijashvili, est une géorgienne expatriée) : « *Nous avons accepté d'héberger le site du Président parce que des hackers russes ont paralysé tout l'internet géorgien* » [23]. La société héberge d'autres sites géorgiens, dont celui de la télévision Rustavi2 [24].

La « guerre de l'information » est la raison d'être du très médiatisé site de hackers pro-russe, **stopgeorgia.ru**. Le site, ouvert le 9 août, dénonce les opérations de guerre de l'information menées par la Géorgie. Il est essentiellement dédié à la conduite d'opérations contre le cyberespace adverse, proposant entre autres une liste des sites internet géorgiens qui doivent constituer des cibles d'attaques [25].

Cyber-guerre et guerre de l'information se sont immiscées dans le discours politique officiel et dans la dialectique de temps de guerre.

3. Commentaires sur les « cyber-attaques »

3.1 L'emballement médiatique

C'est sur la base de ces quelques déclarations officielles et rares informations relatives à des cyber-attaques, qu'aussitôt partout dans le monde, presse, sites internet, forums, blogs, croyant voir là les prémisses d'un conflit révolutionnaire dans sa forme, ont repris et développé à satiété cette idée de cyber-guerre, de guerre de l'information livrée sans merci entre les belligérants.

Sans éléments de preuves irréfutables, écoutant davantage leurs opinions, concédant à la facilité, succombant à leurs phantasmes, recopiant ce que d'autres avaient probablement déjà recopié par ailleurs, relayant le discours officiel du gouvernement, ils sont ainsi des centaines de par le web à avoir publié leurs « analyses » du cyberconflit russo-géorgien, proposant une vision de la réalité conforme à leurs convictions, dénonçant qui la Russie (les militaires, le gouvernement, les services de renseignement, le crime organisé – dont le fameux réseau cybercriminel RBN [26]), qui la Géorgie, les États-Unis, Israël, la Turquie, l'OTAN, les vrais hackers, les apprentis hackers, les hacktivistes, etc. Les mêmes informations ont pendant plusieurs semaines tourné en boucle, sans que ne semble pouvoir être formulée une analyse convaincante tant la situation semblait confuse.

La surenchère médiatique n'est pas sans rappeler celle qui s'est nourrie tout au long de l'année 2007 des désormais célèbres « cyber-attaques russes contre l'Estonie ».

3.2 L'impact des cyber-attaques

Les atteintes aux systèmes (systèmes de télécommunication, réseaux, internet…) qui permettent de délivrer de l'information officielle sont intervenues au plus mauvais moment pour la Géorgie, au plus fort de l'engagement. Elles ont d'autre part touché les sites les plus symboliques : on touche au pouvoir quand on attaque le site d'un président, d'un parlement, d'un ministère, d'une banque nationale, et on touche à la liberté d'expression, voire aux relais du pouvoir, quand on attaque les sites de certains médias. Priver un État de ces ressources, c'est limiter ses capacités de communication, l'isoler, lui interdire de voir et d'être vu. Mais tel ne fut pas tout à fait le cas. La Géorgie a trouvé des relais, des alliés, des solutions alternatives, son espace informationnel n'a pas été coupé du reste du monde : outre l'hébergement des sites du gouvernement géorgien aux États-Unis et en Pologne, l'Estonie a offert d'héberger les sites du ministère des Affaires Étrangères, de la Banque nationale et du portail Civil Georgia [27].

...Les atteintes aux systèmes ont touché les sites les plus symboliques...

Mais, au-delà de l'aspect purement symbolique des cibles concernées, les attaques ont-elles une utilité réelle, le cyber-agresseur un pouvoir de nuisance significatif ? Des attaques similaires ont été enregistrées en Russie et en Géorgie avant le conflit et le seront de toute évidence après. Quelle a donc été alors la valeur ajoutée de ces opérations en temps de guerre ? Les textes affichés sur les sites défigurés ne font passer aucun message sur le conflit inter-étatique, sur les évènements, sur les rapports de force, ni sur la manière dont l'action vise à avoir une influence sur le cours de la guerre : ils sont de la non-information. Le cyber-agresseur qui se cache derrière ces attaques DDoS et défigurations ne dit rien de lui-même, ni sur la forme de menace qu'il entend faire peser sur l'un ou l'autre des belligérants.

Les atteintes aux systèmes d'information ont probablement eu un impact très limité sur les capacités de la Géorgie, en raison de sa relativement faible dépendance aux systèmes d'information. En effet ; les infrastructures réseaux/télécommunications de la Géorgie ne sont pas parmi les plus développées, les infrastructures nationales ne sont pas encore aussi connectées qu'elles le sont dans les pays industrialisés les plus avancés, la population est peu connectée. Même s'ils sont toujours discutables (quelle a été la méthode utilisée, comment les mesures ont-elles été définies, etc.), la majorité des indices et classements internationaux mesurant le degré de développement des nations en matière de réseaux, télécommunications, internet, s'accordent pour placer la Géorgie parmi les plus mauvais élèves du monde. Avec une population de 4.6 millions d'habitants [28], dont seulement 7.49% d'internautes (statistiques 2006) [29], le pays est classé en 93ème position sur 122 du Network Readiness Index [30], derrière la Mongolie, la Tanzanie, la Moldavie. L'Estonie est en 20e position de l'indice, et la France en 23e position. Si l'on s'en réfère à la série d'indices publiés sur le site de l'INSEAD [31], la Géorgie est loin d'être de ces pays modèles en termes de développement des infrastructures et services de l'information et de la communication : elle est en 100ème position de l'indice E-Participation [32] qui mesure la qualité et l'effort d'information réalisé sur les sites gouvernementaux et l'offre de services et outils en ligne pour les citoyens. La Géorgie est ainsi au même rang que la Syrie, la Namibie, le Burundi… pas particulièrement connus pour leur niveau de développement en matière de TIC. Le classement « *ICT Use and Government Efficiency* » [33], qui mesure le niveau d'utilisation des TIC par les gouvernements pour faciliter l'interaction avec les citoyens, positionne la Géorgie en 96ème position, la Russie est classée 95ème, l'Estonie est en 2nde position. Le classement « Accessibilité des services publics en ligne » [34], place l'Estonie en première position, la Russie en 92ème, la Géorgie en 112ème. Le classement proposé par l'ITU basé sur la mesure de la bande passante pour 10 000 habitants, classe la Russie en 73ème position et la Géorgie en 105ème position sur 127 [35].

La Russie, même si elle n'est classée qu'en 70ème position du Network Readiness Index [36], en 82e position de l'Indice E-Participation (à rang égal avec le Lesotho, le Mali ou le Kazakhstan !) compte tout de même 18% d'internautes sur une population de 140 millions d'habitants [37], possède une armée surdimensionnée au regard des seules capacités de la Géorgie, et de moyens de guerre de l'information évidemment supérieurs.

L'impact d'une atteinte aux systèmes d'information sur une population et l'organisation des services de l'État est donc a priori moins immédiat et profond pour la Géorgie qu'il ne le serait dans le cas d'une attaque contre un pays très connecté.

D'autre part, si impact il y a eu sur les sites, il peut être positif : la « publicité » faite autour de ces attaques a également permis aux sites de sortir au moins temporairement de la confidentialité relative dans laquelle ils étaient plongés, pour acquérir une audience bien plus large. Qui, avant ces attaques, avait eu la curiosité de surfer sur le site du président géorgien ?

Mais, la défiguration de quelques sites, pour officiels qu'ils soient, ne peut évidemment pas décider d'une victoire ou d'une défaite. Ces atteintes n'auraient-elles pas plutôt joué en faveur de la Géorgie sur la scène internationale, y renforçant son image de victime ?

3.3 Cyber-attaques avant et après le conflit

Les atteintes aux systèmes d'information ne sont pas concentrées sur la seule période du conflit. Elles ont précédé le conflit : au cours des semaines antérieures, le site du président géorgien avait déjà été pris pour cible, apparemment vers le 20 juillet 2008 [38]. Les tensions entre les deux pays s'inscrivent dans la durée, et le conflit n'est qu'une tentative par la violence de résolution du problème existant. De fait, comme dans toute situation de crise, il y a donc eu des manifestations de la crise dans le cyberespace au cours des mois et années passés.

Les cyber-attaques se sont ensuite inscrites dans le temps du conflit, l'ont « accompagné », diraient certains. Quelques semaines après le conflit militaire, les annonces de cyber-attaques se font rares. Il n'y a toutefois aucune raison pour que ces attaques ne surviennent pas de nouveau : aucune réelle issue n'a été trouvée, aucun accord définitif entre la Russie et l'OTAN arrêté. Toutes les conditions sont réunies pour que l'expression de l'affrontement dans le cyberespace se prolonge. Mais, il semble que les velléités des hackers se soient faites moins vives passé le 15 août. Quoi qu'il en soit, si les cyber-attaques persistent, il ne se trouve plus grand monde pour s'en faire l'écho, comme si toutes les cartouches médiatiques avaient été tirées lors de la semaine du 8 août. D'autres CNA [39] devraient selon toute probabilité avoir lieu dans cette phase de crise et de tension post-conflictuelle. Quelles que soient les raisons de cette diminution apparente des cyber-attaques, il sera intéressant de prendre du recul pour observer les volumes d'attaques pré et post conflit armé.

> *...Il n'y a toutefois aucune raison pour que ces attaques ne surviennent pas de nouveau. Toutes les conditions sont réunies pour que l'expression de l'affrontement dans le cyberespace se prolonge...*

3.4 Effet de surprise impossible

On recense des actions similaires (attaques DDoS, défigurations) depuis plusieurs années, dans tous les pays de la région, comme partout dans le monde, et surtout là où se développent les crises, les conflits : entre la Chine et les États-Unis, le Japon et la Chine, la Russie et la Tchétchénie, la Malaisie et l'Indonésie, Israël et la Palestine, etc. Récemment (juin-juillet 2008), 300 sites lituaniens ont été défigurés (slogans anti-lituaniens, drapeaux soviétiques) suite à l'adoption d'une loi interdisant l'affichage public de symboles datant de l'ère soviétique et de jouer l'hymne national soviétique [40]. Les pages défigurées affichent le drapeau soviétique et des slogans anti-lituaniens [41]. En avril 2008, des groupes diffusant de la propagande pro-Kosovo ont défiguré des sites albanais, et diffusé des listes de sites internet albanais à prendre pour cibles. La récurrence du phénomène est telle que les autorités géorgiennes ou russes ne peuvent pas invoquer l'effet de surprise dans un contexte de tensions extrêmes entre les deux pays. Similitudes dans les procédés, dans les techniques utilisées, dans la logique (contexte de crise, conflit), mais aussi dans la nature des cibles : le site du président géorgien est touché en juillet et août 2008, en octobre 2007 le site du président ukrainien [42] faisait également l'objet d'attaques DDoS [43], aux Etats-Unis, le Pentagone est en permanence l'une des cibles majeures de tous les hackers de la planète. Les sites à valeur politique, symboliques du pouvoir, sont bien évidemment des cibles de choix.

D'autre part, les affrontements dans l'espace informationnel ne sont pas ponctuels, limités au seul temps de guerre. Les attaques dans le domaine de l'information [44], font ainsi l'objet de querelles depuis plusieurs années entre l'Ossétie du Sud et la Géorgie. Un article publié sur le site **www.Civil.ge** le 14 janvier 2006 titrait « *S. Ossetia calls Tbilisi to Stop 'Information War'* » [45], dénonçant les campagnes d'information visant à dénigrer le président de l'Ossétie du Sud. La dimension « guerre de l'information », quelles que soient les composantes mises en œuvre, fait partie du paysage des relations internationales. L'effet de surprise ne peut donc pas être invoqué dans cette situation de guerre. Ce qui peut être souligné par contre reste l'état d'impuissance face à de telles opérations, et peu importe d'ailleurs qui en est l'auteur.

Comment et pourquoi les systèmes de sécurité d'un État se laissent-ils encore déborder par des cyber-agressions fortement prévisibles ?

La conscience des nouvelles donnes en matière de sécurité de l'information et des systèmes d'information existe en Géorgie, puisqu'elle est formulée dans des textes officiels, notamment dans le « *National Security Concept of Georgia* » **[46]**, publié sur les pages du site du ministère de la Défense, qui traite spécifiquement de la question de la sécurité de l'information en ses points 4.10 et 5.10 **[47]** :

> *« 4.10 – Challenges liés à l'information : la sécurité nationale géorgienne peut être menacée en raison de l'absence de politique nationale de l'information cohésive, de la faiblesse de l'infrastructure implémentant une telle politique [...]. De plus, l'existence d'un système insatisfaisant de protection de l'information classifiée, la possibilité d'accès illégal aux systèmes d'information de l'État dans le but d'acquérir et détruire l'information, et la probabilité de voir menées depuis des pays étrangers des attaques informationnelles de grande ampleur contre la Géorgie, représentent de sérieux challenges à la sécurité nationale ».*
>
> *« 5.10 - Politique de sécurité de l'information. [...] La Géorgie accorde une très grande importance à la protection de l'information classifiée, à la régulation de la sécurité des technologies de l'information, et à la protection des systèmes d'information critiques de l'État. [...] le gouvernement géorgien développe les bases législatives et l'infrastructure nécessaire au développement des technologies de l'information et au flux sécurisé de l'information. Une Agence Spécialisée des Communications et de l'Information, placée sous la tutelle du Conseil National de la Sécurité a été créée. L'établissement d'un centre de gestion de crise est en cours, au Conseil National de la Sécurité, pour faciliter le libre flux de l'information en période de crises, la coordination inter agences et la gestion coordonnée des situations de crises ou d'état d'urgence ».*

La conscience de l'importance du rôle de l'espace informationnel sur la sécurité et la défense nationale exprimée dans ces quelques lignes ne va toutefois pas jusqu'à la définition d'une véritable doctrine de guerre de l'information, ni même à l'ébauche des grandes lignes d'une stratégie sécuritaire.

On relève seulement dans ce texte :

- l'affirmation d'une attitude défensive, rien n'évoquant le besoin ni la volonté de mettre en œuvre des processus et structures à vocation explicitement agressive ;
- la conscience de la menace que peut représenter la supériorité informationnelle d'adversaires potentiels ;
- l'identification des menaces de guerre de l'information : CNA (« intrusions », « attaques à grandes échelle »...), ISR (« information classifiée », « accès illégal »...), etc.
- une démarche qui donne l'initiative à l'État en matière de sécurité et défense, mais qui ne semble pas se tourner vers un partenariat avec le secteur privé (le texte est sans doute trop court pour proposer cette orientation).

3.5 Des auteurs non identifiés

Bien que les atteintes aux systèmes d'information géorgiens et russes s'inscrivent dans le cadre d'un conflit, l'identité des auteurs (coupables) des actes reste toujours difficile à avancer avec certitude. Certes, il peut paraître juste, comme le fait d'ailleurs le gouvernement géorgien, d'accuser l'adversaire direct. La réalité est peut-être plus complexe, mais l'accusateur n'a finalement pas à se préoccuper du bien-fondé de ses propos, ni de vérifier les faits : l'accusation doit servir des intérêts politiques, idéologiques, partisans.

Les serveurs impliqués se trouvent en Russie, en Turquie, aux États-Unis... Outre les militaires et les gouvernements, on pourrait raisonnablement penser que des hackers mus par un sentiment patriotique (hacktivistes) se soient impliqués :

- Qui est le fameux « *South Ossetia Hack Crew* » qui revendique la défiguration du site du Parlement géorgien, mais dont personne n'a jamais entendu parler ? Qui est derrière la signature « *FeDeRer & Terrorists* » revendiquant le 5 août 2008 la défiguration du site du ministère des Affaires Intérieures **police.ge** **[48]**? Qui est « P47RICK » signant la défiguration du site **http://saagento.security.gov.ge** ? Ou bien encore qui est SinqRonize, l'auteur revendiquant d'un simple « *NO WAR ! Fuck Russia :) For Türkiye...* » la défiguration de **kavkazblog.com** ? Même « signées », ces actions restent anonymes, car les signatures ne valent rien. Elles peuvent cacher un individu ou un groupe, plusieurs signatures peuvent cacher un seul individu, etc.
- Doit-on parler d'actions russes ou géorgiennes ? Quel est alors le sens que l'on donne à l'adjectif ?
- Quelle représentation peut-on se faire de l'ennemi désigné ?

2 *Capture d'écran publiée sur le site Zataz le 12 août 2008, http://www.zataz.com/news/17599/guerre--russe--georgie-balkan-pays-est-pirate-informatique.html. Montage associant des portraits du Président M. Saakashvili et d'A. Hitler.*

3.6 Le recours à l'image du nazisme

Les défigurations ont essentiellement consisté à remplacer les pages officielles par des photomontages associant l'image du président géorgien à celles de Hitler. De telles images se retrouvent sur le site **Flickr.com** [49] et de nombreux forums dans lesquels il n'y a pas réellement débat, mais davantage échanges virulents d'insultes. Le site **war.georgia.su**, qui dénonce la désinformation géorgienne, vidéos à l'appui, présente le président géorgien comme un nazi : Saakashvili utiliserait les mêmes méthodes que les nazis, utiliserait les mêmes vêtements, etc. Le site diabolise l'adversaire : « Ils n'ont eu aucune pitié pour personne, tuant femmes, enfants et personnes âgées ... les blessés étaient frappés à coups de baïonnettes... certains ont été brûlés vifs dans leurs maisons... ». Un « génocide », un « holocauste » a été commis, 3% de la population a été décimée en une seule nuit, etc. Les troupes russes sont qualifiées de forces de la paix, les opérations géorgiennes de crime de guerre. Cette diabolisation a plusieurs effets : jeter un adversaire en pâture à l'opinion internationale pour l'affaiblir, ternir son image, mais bien sûr aussi justifier ses propres actions. Face à des ennemis sans foi ni loi, sans morale, tout n'est-il pas permis ? Les opérations des hackers n'en apparaissent alors que plus légitimes, sans que doive même se poser la question de la moralité et de la légalité de leur action.

> *...les cyberattaques ne sont plus un phénomène nouveau dans le cadre de crises et de conflits internationaux...*

Associer l'image de dirigeants à celle des dictateurs du 20° siècle n'est bien sûr pas propre au conflit russo-géorgien : association de l'image de G. Bush à celles de Hitler et Mussolini [50], celle de Poutine à celle de Hitler [51], etc. L'Arménie (pro-russe) utilise cette comparaison quand elle parle de l'Azerbaïdjan. Selon un article publié par le site arménien **www.novarak.am** [52], les azéris auraient recours à des méthodes qui étaient celles d'Hitler, de Gebels : mentir ou dire la vérité importe peu, l'important étant de le dire le premier, savoir manipuler l'opinion publique [53] nationale et internationale, être présent dans les organisations internationales sous couvert de démocratie, appuyer l'information par des références à des individus faisant autorité, qu'ils existent ou non, institutionnaliser le mensonge, changer l'image de l'adversaire aux yeux de l'opinion publique, etc. Les agences de presse azeris Day.az, ANS, APA seraient les acteurs de cette désinformation institutionnalisée. On enregistre des échanges entre hackers arméniens et azéris depuis plusieurs années déjà. En 2000, on recensait l'attaque de dizaines de sites arméniens localisés en Arménie et aux États-Unis, par des groupes azéris aux noms de « *Green Revenge* », « *Team of hijackers-187* », etc. autour de la question du Nagorno-Karabakh. Des groupes arméniens sont également actifs comme « Liazor ». Ce sont des conflits pour la souveraineté de territoires qui entraînent ces manifestations [54].

3.7 Le thème des « cyber-attaques », de la « cyberguerre », comme outil de communication

Le gouvernement géorgien a choisi de communiquer sur cet aspect du conflit (les cyber-attaques), de se servir de ces agressions contre son cyberespace, pour dénoncer les opérations adverses, accuser la Russie, renforçant ainsi l'image de victime (justifiant la légitime défense) qu'elle a véhiculée dans sa campagne de communication à destination de l'opinion publique nationale et internationale. Si les cyber-attaques ne sont plus un phénomène nouveau dans le cadre de crises et de conflits internationaux, c'est la dénonciation de ces opérations et leur utilisation à des fins de communication qui est notable. Cette démarche avait été celle de l'Estonie en 2007, qui avait communiqué largement sur les cyber-attaques subies, accusant la Russie, attirant l'attention de la communauté internationale sur son statut de victime, sans toutefois fournir de détail précis sur la nature des attaques subies et les cibles réellement touchées.

Les phrases des textes courts publiés sur les sites du gouvernement (voir §2), sont construites sur un schéma identique à celui proposé sur **Georgiamfa.blogspot.com** par le ministère des Affaires Étrangères géorgien : « Des attaques de cyberguerre menées par la Russie perturbent les sites web géorgiens : le gouvernement de Géorgie a mis en œuvre des sites de remplacement ». Nous retrouvons dans la structure de cette phrase et dans les autres, les éléments d'information suivants :

- action (l'attaque de cyberguerre) ;
- auteur (coupable : la Russie) ;
- accusation : la Russie ;
- impact de l'attaque : sites hors service ;
- victime : la Géorgie ;
- sujet de la nouvelle action – réaction : le gouvernement géorgien ;
- action-réaction : solutions de substitution, pallier les dégâts (réaction à l'impact), accusation verbale (réaction à l'attaque) et publication en ligne de cette courte phrase (action, à l'intention de l'opinion publique nationale et surtout internationale).

Les phrases portent toute accusation. L'adversaire est présenté comme le premier agresseur. La Géorgie ne fait que réagir, de manière défensive. La cyberguerre n'est pas une menace théorique, elle est réalité. Avec des mots à peine différents et dans un ordre à peine modifié, les textes publiés par le gouvernement, mais aussi les déclarations de l'hébergeur Tulip System (§2), émettent le même message et contribuent à la construction de l'image de l'État victime, démocratie attaquée.

3.8 Quand la cybercriminalité tire profit du contexte

En marge du conflit lui-même, comme de tout évènement extraordinaire, spectaculaire, l'information est reprise par les cybercriminels, détournée, utilisée comme leurre : le *spamming* qui utilise une information connue pour leurrer l'utilisateur n'est pas un fait nouveau, mais il est déjà relevé par Symantec [55] :

- « L'information du conflit russo-géorgien utilisée pour dissimuler des codes malicieux dans du spam » [56]. Symantec a identifié un spam viral qui se déguise en article d'information portant sur le conflit russo-géorgien. Le sujet des messages est « *Journalists Shot in Georgia* ». Le message contient un attachement avec un mot de passe et les instructions pour télécharger un fichier. L'utilisateur est en fait redirigé vers un *payload* qui est identifié comme étant le troyen `Trojan.Popwin`. Il s'agit là de l'utilisation de fausse information pour attirer l'utilisateur dans une opération qui lui sera néfaste. La protection contre ces spammings viraux est la bonne utilisation des anti-virus et le bon sens.
- Autre exemple relevé par l'université de Birmingham (Alabama – USA) [57], celui de spam viral renvoyant, via un lien, sur une fausse information de la BBC selon laquelle le président géorgien serait homosexuel (19 août 2008). Les serveurs de spams se trouveraient sur le territoire russe, l'une des machines se trouvant même au sein de l'Agence Fédérale de l'Éducation. Selon l'article publié dans vnunet, le virus ajouterait les machines victimes aux *botnets* sous contrôle de pro-russes et contribuerait aussi à la propagande anti-géorgienne [58].

4. Cyber-attaques isolées ou opérations de guerre de l'information ?

Né aux États-Unis à la fin des années 1980, le concept a fait son apparition sur la scène internationale avec la première guerre du Golfe, démontrant alors l'importance de la maîtrise de l'espace informationnel dans un conflit moderne dominé par les nouvelles technologies.

La guerre de l'information est définie comme l'utilisation agressive/défensive des composantes de l'espace informationnel (information, systèmes d'information), pour atteindre/protéger les intérêts souverains d'un État en temps de paix, de crise ou de conflit [59]. Ce concept englobe ainsi toutes les formes d'utilisation, à des fins agressives et défensives, des technologies de l'information et de la communication, qui peuvent être à la fois les armes et les cibles des agressions : guerre de commandement et de contrôle, ISR, guerre électronique, Psyops, attaques par réseaux d'ordinateurs.

> *...Ces sites et les individus qui se cachent derrière eux contribuent à la fois à la guerre des informations et à la guerre de l'information...*

Les opérations de guerre de l'information peuvent être réalisées, selon qu'elles sont menées par des acteurs militaires ou civils, par un éventail impressionnant d'acteurs aux potentiels les plus disparates : États, militaires, groupes structurés (terrorisme, dissidence, activisme...), individus isolés, simples « pirates » informatiques. Leurs motivations peuvent être multiples : politiques, économiques, idéologiques...

4.1 Opérations civiles ?

Les actions qui ont été qualifiées de cyber-attaques, ont-elles uniquement été le fait d'hacktivistes ? Les hacktivistes sont-ils toujours des civils ?

Le site **stopgeorgia.ru** appelle à mener des actions dans le cyberespace pour la défense des intérêts russes : « *Nous – représentants du monde des hackers russes underground – ne tolèrerons pas de provocation géorgienne sous quelque forme que ce soit. Nous voulons vivre dans un monde libre et sans agressions [...] Nous n'avons pas besoin d'être guidés par les autorités ni par qui que ce soit, mais agissons selon nos convictions fondées sur le patriotisme, la conscience et la confiance en la vertu de la justice. Vous pouvez nous traiter de criminels et de cyber-terroristes [...] mais nous nous battrons dans le cyberespace contre l'agression inacceptable de la Russie. Nous demandons l'arrêt des attaques contre l'information et les ressources du gouvernement, et appelons tous les médias et journalistes à couvrir les évènements de manière objective. Jusqu'à ce que la situation change, nous empêcherons la dissémination de fausse information [...] Nous n'avons pas lancé cette guerre de l'information, nous ne sommes pas responsables de ses conséquences. Nous appelons à venir nous assister tous ceux qui s'inquiètent des mensonges des sites du gouvernement géorgien...* » [60]. Le site propose une liste des principales ressources officielles géorgiennes [61] sans toutefois mettre à disposition en ligne des outils de hacking. Mais, en désignant les cibles, l'objectif est de faciliter la tâche des hackers. La page d'accueil propose des liens vers des sites (**war.georgia.su** et **www.stop-war.us**) partageant le même souci de dénonciation de la désinformation géorgienne. La rubrique « media-lies » du site **war.georgia.su** dénonce la manipulation médiatique, les photos truquées de l'agence Reuters, la diffusion

par une agence de presse de fausse information et la reprise par les médias internationaux de la même fausse information.

Ces sites et les individus qui se cachent derrière eux contribuent ainsi à la fois à la guerre des informations (donner leur interprétation de la réalité [62], de la vérité ou alimenter la confusion), et à la guerre de l'information dans sa dimension CNA. Ils revendiquent leur autonomie, leur liberté d'action et de pensée. Mais toutes les hypothèses restent envisageables quant à leur vraie nature : ils ne sont peut-être pas aussi autonomes qu'ils le prétendent.

4.2 Opérations militaires ?

Les actions qui ont été qualifiées de cyber-attaques, ont-elles été le fait des militaires ? Y a-t-il eu à leur niveau, recours aux méthodes de guerre de l'information pour préparer les affrontements, couper les réseaux adverses, aveugler l'ennemi, couvrir les missions sur le terrain par des frappes informatiques préalables ? Quel usage militaire a réellement été fait de la guerre de l'information dans cette guerre éclair ? Les gouvernements russes et géorgiens, au-delà de l'ordinaire affrontement psychologique (information, désinformation) ont-ils utilisé des méthodes de type attaques par les réseaux, interception de communications, attaques physiques contre des infrastructures de communication, pour s'assurer la maîtrise de l'espace informationnel ?

Le conflit russo-géorgien a très probablement offert aux belligérants un champ d'utilisation de leurs capacités de guerre de l'information. Mais, l'absence d'information en provenance des opérations militaires russes et géorgiennes interdit toute conclusion définitive et toute analyse plus méthodique. Rien ne permet d'affirmer que les attaques contre les systèmes d'information géorgiens ont été une action coordonnée par les militaires russes en vue de couper les systèmes de communication du pays et faciliter la progression des opérations militaires. Rien ne permet de l'infirmer non plus. Ces quelques temporaires défigurations de sites et saturations de serveurs, auxquelles des solutions de remplacement rapides ont été trouvées (sites miroirs, hébergements des pages dans des pays alliés...) ne résument quoi qu'il en soit pas à elles seules le concept de guerre de l'information.

5. Formuler les bonnes questions

Sans doute est-il trop tôt aujourd'hui pour reconstruire le scénario de ce qui s'est réellement passé dans l'espace informationnel des belligérants et en tirer les conclusions.

Du temps sera nécessaire pour une enquête et une analyse méthodique, qui évitera de tomber dans le piège des raccourcis pris lors de l'emballement médiatique, en s'attachant à répondre aux questions suivantes spécifiques à ce conflit, puis plus générales et conceptuelles :

- Les opérations menées :
  - Cette « guerre de l'information », puisque telle fut l'expression utilisée, se résumerait-elle à quelques défigurations et mises hors service de sites internet officiels ?
  - Quelles actions dans le cyberespace doivent donc être définies comme des actes de guerre, lesquelles relèvent uniquement des actes de délinquance ?
  - Les affrontements révèlent-ils l'existence d'un arsenal de cyberguerre ?
  - Est-il possible de reconstituer le tempo des opérations agressives et défensives de part et d'autre et d'en tirer des conclusions générales sur le rôle joué par la 4°dimension du combat dans un conflit éclair ? Ce rôle peut-il être marginal ou bien doit-il au contraire être central ?
- Les acteurs des opérations :
  - Quelles actions ont été menées sous la direction de l'armée et du gouvernement ?
  - L'armée s'est-elle réellement emparée de l'espace informationnel, du cyberespace, pour mener cette guerre éclair ? Quelles opérations de type guerre de l'information les armées ont-elles réellement menées ? Qu'y a-t-il de nouveau dans la façon de mener cette guerre ?
  - Des citoyens (russes, pro-russes, géorgiens, pro-géorgiens) se sont-ils impliqués au cyberconflit ? Le concept de « guerre du peuple » cher à la Chine gagnerait-il le monde ? Verrait-on poindre à l'horizon une nouvelle forme de citoyen du monde cyber-combattant ? Rien n'est moins discutable. Les hacktivistes s'invitent dans toutes les crises et conflits sans que jusqu'ici leurs actions n'aient eu une influence prouvée sur le déroulement des évènements. Les masses de défigurations sont souvent l'œuvre de quelques rares hackers, qui ne peuvent à eux seuls autoriser l'utilisation d'expressions telles que « guerre du peuple », supposant l'investissement de volumes d'individus significatifs.
  - La participation des civils aux conflits serait-elle un atout ou contribuerait-elle à accroître le brouillard informationnel ? Si cette participation s'avérait néfaste au succès, serait-il possible de la contenir ? La participation des civils peut-elle influer sur les rapports de force stratégiques internationaux ?
  - Quelles sont les relations, si elles existent, entre crime organisé et effort de guerre, dans le cyberespace ? L'implication du RBN dans les cyber-attaques contre la Géorgie est-elle avérée ?

- Quelles peuvent être dans la 4° dimension du combat que constitue l'espace informationnel et particulièrement le cyberespace, les relations entre les mondes civil et militaire ? Les États pourraient-ils envisager de recourir à des Sociétés Militaires Privées (SMP) pour investir le champ du cyberespace ? L'expérience acquise par des groupes cybercriminels pourrait-elle leur permettre une reconversion temporaire en SMP du cyberespace ? L'extension du recours à des SMP ne serait alors que le prolongement dans l'espace informationnel de la privatisation de la violence. La réflexion portera alors sur le rôle que les SMP pourraient tenir dans la guerre de l'information, mais aussi sur les risques que ferait encourir aux États le recours mal maîtrisé à de tels acteurs, et sur les limites acceptables de la remise en cause du monopole et de la maîtrise de la violence par l'État Nation (l'ordre westphalien).
- Une dimension « ludique » n'apparaît-elle pas dans la guerre quand de simples hackers peuvent profiter d'un contexte de désordre pour s'immiscer, augmenter la confusion par leurs actions, faire croire à des actes de guerre, revêtir les habits des grandes puissances ? Ou quand des acteurs officiels de la guerre (militaires, gouvernements) peuvent faire croire à l'action de hackers à l'esprit ludique pour masquer leurs opérations ?
- Dès lors que les piratages de serveurs et sites ne perturbent pas de manière significative le fonctionnement des troupes armées, ne pénètrent pas et ne perturbent pas les systèmes de communication des C4ISR, ne portent pas atteinte aux systèmes assurant le fonctionnement des infrastructures sensibles, et ne mettent pas en péril les systèmes de communication assurant la gestion des situations de crise et d'urgence, faut-il s'inquiéter des opérations des hackers/hacktivistes qui défigurent ou mettent hors service des sites d'information générale voire officielle ? Dans ce conflit, le hacking de quelques sites a pris une importance médiatique hors proportions raisonnables, sans rapport avec les conséquences réelles des faits. Qui a réellement tiré profit de la caisse de résonance médiatique ?

⇨ L'impact des opérations :

- Quel aura été l'impact des défigurations et mises hors service des sites officiels ?
- L'avantage pris par l'offensive en matière de cyber-agression est-il imparable ?
- Faut-il accorder une importante stratégique, politique, aux opérations non revendiquées ?
- Quelles dimensions de la guerre de l'information sont-elles un réel facteur multiplicateur de force ? La guerre de l'information confère-t-elle un avantage menant au succès ?
- La maîtrise de l'espace informationnel n'est-elle pas une utopie ?
- Une guerre moderne, éclair ou sur le long terme, peut-elle être gagnée sans recours à la guerre de l'information ?
- À quoi la Russie doit-elle d'avoir gagné la guerre ? À ses actions cinétiques létales ou bien à un avantage sur le champ de la guerre de l'information ?
- Plusieurs catégories de sites ont été touchées : gouvernementaux, mais aussi de hackers, commerciaux, de médias, etc. L'impact sur le conflit est-il différent en fonction de la nature de la cible visée ?
- Faut-il savoir entretenir le hacking en temps de paix pour le mobiliser en temps venu par des sentiments nationalistes ? Le hacker et l'hacktiviste sont-ils manipulables ?
- Quelles alternatives existent-elles en matière de cyber-guerre et guerre de l'information aux solutions américaines coûteuses : une cyber-guerre à moindres frais, loin des coûts faramineux qu'implique la programmation, la planification, la mise en œuvre des programmes de cyber-guerre pharaoniques américains, est-elle possible ?

⇨ Conclusion

La Géorgie est une nation bien trop peu investie dans le cyberespace pour que les quelques agressions dont ce dernier a fait l'objet, se résumant à quelques attaques de serveurs et sites internet, apparaissent comme des opérations massives de guerre de l'information. Dans cette période brève de guerre dissymétrique, la Russie a remporté une victoire, mais l'on ne sait pas encore, par manque d'information, l'importance réelle qu'ont eu les opérations d'information, et si même la lutte pour la maîtrise de l'espace informationnel a été prédominante. Bien entendu, au sens traditionnel du terme, il y a eu guerre de l'information, puisque d'information de guerre et d'information dans la guerre il fut question, c'est-à-dire d'utilisation de l'information pour relater des évènements (des « histoires » **[63]** ?), pour jouer avec l'opinion, influencer, rallier à sa cause une partie du reste du monde, dénoncer, c'est-à-dire mener des opérations psychologiques. Mais en ce qui concerne les cyber-attaques au sein du conflit russo-géorgien, nous serions tenté de conclure qu'elles constituent simplement un non-évènement.

Notes et références

[1] **http://fr.wikipedia.org/wiki/Tom_Clancy's_Ghost_Recon**. Video Trailer : **http://www.youtube.com/watch?v=7FTzbT99-KI**

[2] Développé par la société *Red Storm Entertainment*

[3] Liste non exhaustive

[4] **www.president.gov.ge**

[5] **http://www.mfa.gov.ge/**

[6] **http://www.parliament.ge/**

[7] **http://www.mod.gov.ge**

[8] **http://www.nbg.gov.ge**

[9] **http://www.rustavi2.com.ge/**

[10] Le 12 septembre 2008, le texte relevé disait « Au cours des trois derniers jours, nous avons fait face à des attaques DDoS massives. Le degré de ces assauts de cyber-guerre est sans précédent et il est probable qu'ils se poursuivront et peut-être s'intensifieront [...] il ne s'agit pas uniquement d'une attaque contre notre site, mais d'une guerre à tous ceux qui parlent du Kremlin [...] ».

[11] Liste non exhaustive

[12] **http://en.rian.ru/russia/20080810/115936419-print.html**

[13] **www.russiatoday.com**

[14] **http://www.russiatoday.com/news/news/28835**

[15] **http://stopgeorgia.ru** à ne pas confondre avec le site **stoprussia.org**, pro-géorgien, qui propose de signer une pétition en ligne contre les actions de la Russie.

[16] **http://abkhazia.gov.ge**

[17] *Georgian Academic and Research Network*

[18] Les attaques DDoS ont visé le serveur **Web.Caucasus.net** (62.168.168.9) qui hébergeait le site du Président, mais aussi d'autres sites géorgiens comme celui de la Social Assistance and Employment State Agency (**www.saesagov.ge**). Il est impossible d'affirmer que le site du Président géorgien était spécifiquement visé. L'attaque serait venue du (ou passée par le) serveur 79.135.167.22 localisé en Turquie, ayant également servi à attaquer le site du Parlement géorgien.

[19] **http://georgiamfa.blogspot.com/2008/08/cyber-attacks-disable-georgian-websites.html**

[20] Texte du 11 août 2008

[21] Rappelons que le président Kaczynski avait été l'un des acteurs de la libération de la Pologne du joug soviétique : cet hébergement doit être perçu comme une expression, parmi d'autres, de la solidarité de la Pologne à l'égard de la Géorgie. Le combat des deux pays est similaire : celui de la liberté, de la démocratie. Voir à ce sujet l'article **http://www.latimes.com/news/nationworld/world/la-fg-media20-2008aug20,0,693386.story**.

[22] **http://www.president.pl/x.node?id=479**

[23] **http://www.theregister.co.uk/2008/08/14/russia_georgia_cyberwar_latest/**

[24] **http://www.ajc.com/business/content/printedition/2008/08/17/tulip.html**

[25] **http://stopgeorgia.ru/?pg=tar**

[26] Russian Business Network. Voir **http://www.zataz.com/news/17611/russe--georgie--conflit--geogia--russian--cyber-blocking.html**

[27] « *Estonia hosts Georgian Websites after cyber attacks* », 27 août 2008, **http://www.russiatoday.com/news/news/29544**

[28] Juillet 2008, estimation, **https://www.cia.gov/library/publications/the-world-factbook/geos/gg.html**

[29] **http://www.insead.edu/v1/gitr/wef/main/analysis/showcountrydetails.cfm**

[30] Proposé par le Forum Économique Mondial 2006-2007, **http://www.weforum.org/pdf/gitr/rankings2007.pdf**

[31] **http://www.insead.edu**

[32] *Global Information Technology Report 2007-2008*, **http://www.insead.edu/v1/gitr/wef/main/analysis/showdatatable.cfm?vno=9.13&countryid=340**

[33] **http://www.insead.edu/v1/gitr/wef/main/analysis/showdatatable.cfm?vno=9.11&countryid=340**

[34] **http://www.insead.edu/v1/gitr/wef/main/analysis/showdatatable.cfm?vno=9.1&countryid=340**

[35] **http://www.insead.edu/v1/gitr/wef/main/analysis/showdatatable.cfm?vno=7.2&countryid=340**

[36] Proposé par le Forum Économique Mondial 2006-2007, **http://www.weforum.org/pdf/gitr/rankings2007.pdf**

[37] **https://www.cia.gov/library/publications/the-world-factbook/geos/rs.html**, juillet 2008 – estimation.

[38] **http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080720** et **http://mypetjawa.mu.nu/archives/193591.php**

[39] *Computer Network Attacks* : attaques par réseaux d'ordinateurs

[40] La Lituanie a rejoint l'OTAN et l'UE en 2004

[41] « *Pro-russian cyber-attack hits Lithuania* », 30 juin 2008. **http://www.mywire.com/pubs/AFP/2008/06/30/6809382**

[42] **http://www.ukrainianjournal.com/index.php?w=article&id=5483** octobre 2007

[43] « *Russian hackers cripple Yushchenko website* », 30 octobre 2007. **http://www.ukrainianjournal.com/index.php?w=article&id=5483**

[44] Pas obligatoirement dans le seul « cyberspace », mais dans l'espace de l'information, dans sa globalité.

[45] **http://www.civil.ge/eng/article.php?id=11511**

[46] **http://www.mod.gov.ge/i.php?l=E&m=3&sm=1**

[47] Traduction en français : D. Ventre

[48] Voir **http://i27.tinypic.com/29pq8j.jpg et http://i28.tinypic.com/ephh84.jpg**

[49] **http://flickr.com/photos/27074615@N06/2755219768/** et **http://flickr.com/photos/75255787@N00/2753053679/**

[50] Sur **http://www.thepeoplesvoice.org/cgi-bin/blogs/voices.php/2008/08/**, voir l'image postée le 3 août 2008.

[51] **http://www.flickr.com/photos/teonna/2756230123/** ou **http://www.rgnpress.ro/Politic/Putin-=-Hitler.html**

[52] **www.novarank.am/en/?page=print&nid=1203**

[53] Définir ce qu'est « l'opinion publique » est une tâche fort difficile. Rappelons juste que pour Pierre Bourdieu « L'opinion publique n'existe pas », *Temps Modernes*, 29 (318), janvier 1973, pp. 1292-1309. Texte disponible à l'adresse : **http://www.homme-moderne.org/societe/socio/bourdieu/questions/opinionpub.html**

[54] **www.infowar-monitor.net/modules.php?op=modload&name=News&file=article&sid=141** « **Back Files : Computer Specialists Urge End to Armenian-Azeri Hack Attacks** », 18 février 2000.

[55] **http://www.symantec.com**

[56] **https://forums.symantec.com/syment/blog/article?blog.id=spam&message.id=111#M111**, 21 août 2008, « *Russia/Georgia Conflict news Used t Hide Malicious Code in Spam* ».

[57] Rapporté dans **http://www.crime-research.org/news/19.08.2008/3521/**

[58] **http://www.crime-research.org/news/19.08.2008/3521/**

[59] Définition proposée par Daniel Ventre, CNRS. Voir également du même auteur l'ouvrage *La Guerre de l'information*, éditions Lavoisier, novembre 2007.

[60] Texte disponible sur la page d'accueil du site **stopgeorgia.ru**. Traduction : D. Ventre

[61] **http://stopgeorgia.ru/?pg=tar**

[62] Sur le concept de « réalité », rappelons l'ouvrage de Paul Watzlawick, *La Réalité de la Réalité*. Confusion, désinformation, communication, Éditions du Seuil, ISBN2.02.006804.4.

[63] SALMON (Christian), *Storytelling, la machine à fabriquer des histoires et à formater les esprits*, La Découverte, ISBN 978-2-7071-4955-8.

Hervé Chabanne (Sagem Sécurité) & Didier Chaudun (Sagem Orga)

MOC OU LA BIOMÉTRIE DANS UNE CARTE À PUCE

mots clés : *empreinte digitale / carte à puce / authentification*

Nous présentons la technologie Match On Card (MOC) où une empreinte digitale est comparée dans une carte à puce à une empreinte de référence. Dans un premier temps, nous décrivons les aspects techniques du MOC et ses performances. Dans un second temps, nous considérons son déploiement dans différents domaines d'application.

Le *Match On Card* (MOC) permet une approche différente de la biométrie. Aux grandes bases de données permettant l'identification d'un individu parmi une large population, le MOC peut être vu en opposition, permettant plutôt une simple authentification locale sous le contrôle du porteur de la carte. Les prouesses algorithmiques permettent aujourd'hui un MOC fiable et rapide s'exécutant sur une CPU de carte à puce avec des ressources réduites.

1. Comment cela marche-t-il pour les empreintes digitales ?

1.1 Introduction à la reconnaissance biométrique

Le principe de la reconnaissance biométrique est très simple. Lors d'une première étape, une donnée biométrique de référence est acquise, pour laquelle des points caractéristiques sont extraits afin de constituer ce qui est appelée un *template*, conservé **dans la carte**. Ensuite, l'authentification est possible via l'acquisition d'une donnée biométrique « fraîche » et sa comparaison par rapport au template stocké.

La reconnaissance biométrique ne nécessite pas que les données biométriques soient considérées comme secrètes pour fonctionner (contrairement à un code porteur). En revanche, le système doit fournir l'assurance qu'il s'agit bien de la donnée acquise sur l'individu se présentant qui est utilisée pour la comparaison et non pas une donnée rejouée, artificielle ou appartenant à quelqu'un d'autre. Les moyens employés pour détecter **le fait** que la donnée saisie provient effectivement d'une « vraie » personne vivante peuvent varier. Par exemple, il est possible de vérifier l'activité sanguine du doigt. Plus de détails sur le sujet de la détection du vivant peuvent être trouvés pour la biométrie de l'empreinte digitale dans [1].

1.2 Les différentes informations contenues dans une empreinte digitale

Une empreinte digitale est formée par un certain nombre de reliefs de la peau, appelés des « lignes de crêtes », qui permettent de différencier efficacement les individus. Une empreinte digitale

1 *Tourbillon dans l'image de gauche*

2

comporte plusieurs niveaux de détails. Le premier niveau est global et porte sur la topographie générale des lignes de crêtes. Par exemple, la forme générale peut ressembler à une boucle à droite, à une boucle à gauche (cf. Figure 1), à une arche ou à un tourbillon (cf. Figure 1). Des formes plus composites sont aussi possibles.

Le deuxième niveau d'information est local et correspond à des points caractéristiques de l'empreinte digitale, appelés minuties (cf. Figure 2). Ces points ont été introduits en premier lieu par Galton au début du XXe siècle. Ce sont des événements de discontinuité sur les lignes de crêtes : fins de lignes, bifurcations, points isolés. En plus de la position, la direction locale de la ligne de crête associée, c'est-à-dire la tangente à la ligne de crête en ce point, est conservée.

1.3 Captures, extractions et matching d'empreintes digitales

Une fois l'image d'une empreinte digitale acquise via un capteur, de nombreux traitements d'image (amélioration du contraste, de la luminosité, élimination du bruit,...) sont effectués afin d'améliorer la qualité en pré-traitement, avant de procéder à l'extraction des points caractéristiques. Ensuite, les bruits de l'empreinte digitale elle-même sont éliminés. Par exemple, les cicatrices et coupures ne doivent pas mener à des minuties supplémentaires si elles sont considérées comme des fins de lignes de crêtes. Au final, les minuties sont détectées et la tangente en chaque minutie est également calculée. En moyenne, quelques dizaines de minuties sont observées sur une empreinte digitale. Cette capture et cette extraction des minuties ne sont pas aujourd'hui réalisées par la carte à puce.

Le principe de la comparaison – appelé *matching* – de minuties est de chercher une association entre les minuties qui viennent d'être acquises et celles de référence du template. Ce matching peut être décomposé en deux phases : une première phase pour trouver le recalage global entre les deux ensembles de minuties et une seconde phase pour compenser des distorsions locales.

L'algorithme de matching tente dans un premier temps de positionner les points caractéristiques provenant du doigt vivant de la même manière que ceux issus du template. En effet, lors de la capture, la position du doigt a pu varier. Par conséquent, sont recherchées les translations et rotations permettant de rapprocher au mieux les minuties de chaque empreinte digitale.

Ensuite, dans un second temps, l'algorithme de matching va tenter de s'affranchir des distorsions locales. À cause de facteurs extérieurs liés à l'environnement de l'acquisition et au comportement de l'utilisateur (par exemple, une pression différente exercée sur le capteur), l'empreinte digitale peut subir des déformations qui éloignent plus ou moins les minuties d'une prise à une autre.

Finalement, le matching doit être suffisamment souple pour pouvoir fonctionner tout en tenant compte de l'apparition et de la disparition de minuties entre deux captures.

L'algorithme de matching calcule un score en fonction du nombre de minuties qui se correspondent. Ce score est comparé à un seuil pour donner le résultat de l'authentification.

1.4 Le Match On Card

Le MOC (Match On Card) consiste à faire exécuter l'algorithme de matching sur une carte à puce. Les minuties, c'est-à-dire leur position et la tangente associée, sont quantifiées pour pouvoir être traitées par une CPU sans arithmétique flottante et le template de référence est conservé directement dans la carte. Différents algorithmes de matching MOC existent aujourd'hui et certains sont protégés par des brevets. Les algorithmes actuels [2] sont à la fois rapides (une comparaison est effectuée typiquement en une ½ seconde) et précis (pour une acceptation à tort de 0,1 % correspond un rejet à tort d'1 %).

La commande APDU VERIFY (ISO/IEC 7816-4) peut être utilisée pour envoyer les minuties à comparer à **celles de** la carte. En outre, depuis leur version 2.2.2, les spécifications de la Javacard comprennent une API dédiée à la biométrie où une interface BioTemplate est prévue avec les méthodes permettant de mettre en œuvre le matching MOC et une sous-interface OwnerBioTemplate dédiée au stockage du template de référence [3].

Après une authentification MOC réussie, la carte peut exécuter une authentification cryptographique simple pour signifier la levée de droits lors d'un contrôle d'accès dans un système. Des protocoles d'authentification plus sophistiqués peuvent également être employés pour un meilleur respect de la vie privée [4].

2. Applications

2.1 Authentification d'un individu au sein de la société

Le Match On Card apporte la possibilité d'authentifier le titulaire de la carte, sans avoir recours à une base de données, ni stocker les minuties ailleurs que dans la carte qui appartient à son titulaire. La carte à puce étant un coffre-fort de données personnelles, les minuties peuvent y être stockées de manière parfaitement sécurisée. L'exécution du matching dans la carte permet de n'en jamais faire sortir les minuties. Le MOC permet donc d'utiliser la biométrie pour l'authentification de personnes, sans mettre en danger le respect de la vie privée.

Parmi les applications du MOC, il y a bien sûr les applications gouvernementales :

- La vérification de l'identité : le MOC permet de vérifier l'identité d'une personne avec un terminal portable, sans le besoin de connexion à un système.
- L'authentification de la personne étant particulièrement importante lorsqu'il s'agit de lutter contre la fraude, le recours au MOC est particulièrement intéressant pour les applications d'assurances sociales et d'aide aux plus démunis.

Par exemple, en Europe, la carte d'identité espagnole est équipée d'un MOC.

2.2 De nouvelles applications

D'autres applications non gouvernementales vont faire appel à la biométrie grâce au MOC : les paiements par carte bancaire et le retrait d'argent aux distributeurs de billets. Dans ce cas, le terminal de paiement dispose d'un capteur de saisie d'empreinte digitale ; le porteur ne saisit pas de code PIN, mais appose juste son doigt sur le capteur ; la carte contrôle l'empreinte acquise et traitée par le capteur. Le code PIN étant une information qu'il est aisé de voler par simple surveillance de l'utilisation des moyens de paiement, l'apport en sécurité du MOC est extrêmement important dans ces transactions.

Le MOC permettant d'authentifier le titulaire de la carte, on peut envisager son utilisation pour l'accès à des e-services ou à des serveurs informatiques d'entreprise. Il se pose alors le problème du terminal, qui doit pouvoir être à la fois suffisamment bon marché, sans être un maillon faible dans la chaîne de sécurité. Cet usage du MOC est tout à fait intéressant dans un cadre professionnel, comme cela se fait dans le programme PIV (*Personal Identity Verification*) [5] de l'administration américaine. L'usage par un particulier pourra être envisagé, à son domicile, avec des lecteurs adaptés.

Conclusion

Le MOC tel qu'il a été présenté ici pour les empreintes digitales peut être conçu pour d'autres biométries. L'algorithme du matching de l'iris étant très simple (un simple calcul de distance de Hamming normalisée **[6]**), il ne nécessitera pas beaucoup de ressources CPU et pourra être mis en œuvre facilement dans une carte à puce. La biométrie de visage est, elle aussi, envisageable pour le MOC. Finalement, la combinaison au sein d'une même carte de plusieurs MOC pour différentes biométries (plusieurs empreintes ou empreinte + iris par exemple) permettrait d'accroître la sécurité du système.

Références

[1] SANDSTRÖM (Marie), *Liveness Detection in Fingerprint Recognition Systems, PhD thesis, University of Linköping*, 2004.

[2] **http://fingerprint.nist.gov/minexII/minex_report.pdf**

[3] *Biometric Application Programming Interface (API) for Java Card*, **http://www.javacardforum.org/03_documents/00_documents/fileload_06.pdf**

[4] BRINGER (Julien), CHABANNE (Hervé), POINTCHEVAL (David), ZIMMER (Sébastien), *An Application of the Boneh and Shacham Group Signature Scheme to Biometric Authentication*, IWSEC 2008.

[5] **http://csrc.nist.gov/groups/SNS/piv/index.html**

[6] DAUGMAN (John), *The importance of being random: statistical principles of iris recognition. Pattern Recognition*, 36(2):279_291, 2003.

Cédric Llorens & Denis Valois
cedric.llorens@wanadoo.fr, denis.valois@laposte.net

SÉCURITÉ DES RÉSEAUX : LES NOUVEAUX ENJEUX

Ce dossier présente quelques évolutions liées à la sécurité réseau qui reste en mutation permanente à cause des nouvelles architectures réseau, mais aussi en raison des nouveaux services offerts. Il est structuré par thèmes couvrant volontairement des domaines différents du monde du réseau.

- **Évolution technologique face à la sécurité** : La sécurité n'est pas statique et doit prendre en compte toutes les évolutions d'architecture ou purement technologiques. Deux points épineux y sont présentés. Comment réaliser une cohabitation « orthogonale » entre IPv4 et IPv6 avec la migration IPv6 qui s'annonce ? Comment adapter sa sécurité (supervision, analyse, etc.) avec les très hauts débits qui seront bientôt offerts à tous ?
  - « Sécurité pour l'introduction de l'IPv6 dans les cœurs de réseau » (S. Nataf), p. 19.
  - « Le très haut débit, un challenge pour la sécurité » (F. Ropert), p. 29.
- **Le contrôle de la sécurité** : L'évolution des services offerts repose soit sur de nouveaux protocoles, soit sur des extensions de protocoles existants. Quel que soit ce protocole, un contrôle dynamique des échanges doit être mis en place ainsi qu'un contrôle des configurations implémentant les règles de sécurité liées à ce service. Nous couvrons ces deux besoins en présentant tout d'abord les nouvelles sondes permettant de réaliser un contrôle sur les échanges, mais aussi en détaillant une nouvelle approche pour réaliser des audits de conformité des configurations.
  - « Les nouvelles sondes de sécurité dans les cœurs de réseaux » (C. Llorens & D. Valois), p. 38.
  - « Une nouvelle approche dans l'analyse des configurations » : HAWK (D . Valois & C. Llorens), p. 47.
- **Tester une architecture réseau et sa sécurité** : Monter un laboratoire et acheter des équipements réseau à des fins de tests et de sécurité est nécessaire, mais très coûteux. Ce dernier article du dossier illustre comment émuler un tel environnement en limitant les coûts associés.
  - « Émulation d'architectures réseau » (C. Foll), p. 53.

Compte tenu de l'ensemble des évolutions technologiques dans le domaine réseau, le dossier ne couvre évidemment pas l'ensemble des initiatives sécurité. De plus, il ne détaille pas les nouvelles attaques réseau, telles que celle découverte récemment sur le protocole de routage BGP (**http://blog.wired.com/27bstroke6/2008/08/revealed-the-in.html** : une variante d'attaque exploitant une faiblesse protocolaire bien connue), qui peuvent d'ailleurs faire l'objet d'un dossier dédié. Cependant, l'ensemble des articles illustrent la dynamique « sécurité » liée au domaine du réseau.

Enfin, nous tenons à remercier l'équipe virtuelle qui a travaillé pendant les grandes vacances pour monter ce dossier.

Bonne lecture,

Cédric Llorens & Denis Valois

Sarah Nataf – sarah.nataf@orange-ftgroup.com

SÉCURITÉ POUR L'INTRODUCTION DE L'IPv6 DANS LES CŒURS DE RÉSEAU

mots clés : *réseaux / IPv6 / MPLS / ACL*

IPv6 n'est qu'une nouvelle version du protocole IP. IPv6 respecte donc les principes fondamentaux que l'on connaît de nos jours avec IPv4. Les protocoles de routage eux-mêmes seront des évolutions des protocoles actuels pour supporter ce nouveau format de paquets. Le déploiement d'un nouveau protocole dans un réseau implique l'apparition de nouveaux risques : pour que l'introduction d'IPv6 ne rime pas avec l'introduction de nouvelles failles de sécurité dans le cœur de réseau, il faut étudier de près ces nouveaux risques et comment s'en protéger.

1. Introduction d'IPv6 dans les réseaux actuels

1.1 Rappels sur IPv6

IPv6 n'est en effet qu'une nouvelle version du protocole IP. L'information est donc toujours acheminée sous forme de paquets, dont l'en-tête contient une adresse source et une adresse destination. Les protocoles de transports sont conservés, à savoir TCP et UDP, ainsi que les couches supérieures jusqu'aux applications (http, DNS, SMTP, etc.) **[MISC1]**. Les couches inférieures sont également conservées, à quelques détails près comme certains mécanismes de niveau 2 intimement liés au niveau 3 tel que l'ARP (*Address Resolution Protocol*) pour Ethernet, mais le principe générique de fonctionnement est conservé. De même, le protocole d'échange des routes sur Internet reste BGP, les protocoles de routage internes (IGP, à savoir RIP, EIGRP, OSPF, IS-IS) sont préservés et peu modifiés, et l'architecture DNS est également identique.

Si la littérature affirme que le protocole IPv6 apporte plus de sécurité qu'IPv4, il faut donc se faire une raison : ceci est faux ou tout du moins vrai pour des aspects très limités. Certes, toute pile IPv6 doit implémenter nativement IPsec puisque l'activation de ce mécanisme est optionnelle, les en-têtes IPv6 pouvant comporter des champs assurant une intégrité et une authentification des données (AH, *Authentication Header*) et/ou la confidentialité des données échangées (ESP, *Encapsulating Security Payload*). Encore faut-il que ces options soient activées lors des communications **[1]** et, de plus, si IPsec protège certains échanges, ce mécanisme ne protège pas contre les attaques de type DoS, virus ou encore tentatives d'intrusions.

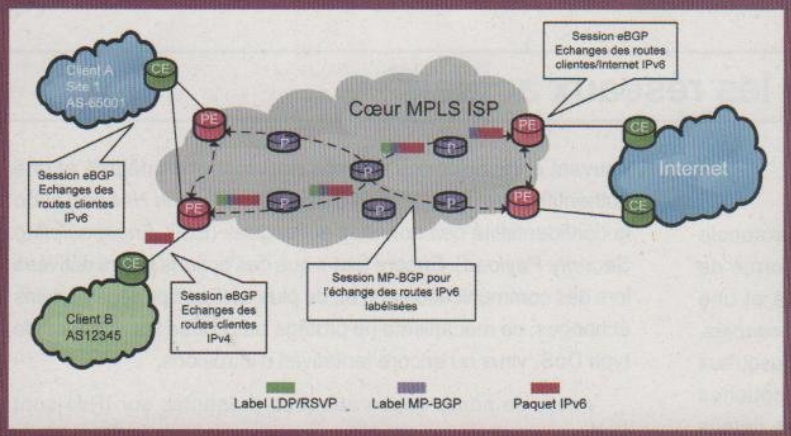
Ainsi, de nombreuses attaques présentes sur IPv4 sont toujours possibles sur IPv6. Les attaques de type MITM (*Man In The Middle*) auront la même probabilité de se produire qu'en IPv4 si IPsec n'est pas activé. Concernant les scans, les standards imposent d'adresser les liens avec des préfixes de longueur /64 (2^64 bits restant pour identifier une interface). Les sites clients (entreprises ne disposant pas de ses propres adresses IP, clients xDSL, set-top-box) se verront allouer des préfixes de taille minimale de 64 bits également. Il est donc souvent affirmé, à juste titre, que la phase de scan de réseau et de découverte des hôtes est plus longue avec IPv6. Or, l'écoute de trafic est tout autant possible en v4 qu'en v6 ; et si IPsec (ESP) assure la confidentialité des données, l'écoute permet tout de même de découvrir les adresses de victimes potentielles (hôtes, serveurs,

etc.). Enfin, comme détaillé dans **[MISC2]**, des techniques existent pour réduire les durées des scans.

1.2 Les mécanismes de transition

Pourquoi introduire une nouvelle version d'IP ? Tout simplement pour continuer à assurer une connectivité sur les réseaux IP lorsqu'il n'y aura plus d'adresses IPv4 disponibles. Avec le NAT, il est possible d'économiser les adresses IPv4, mais cela rompt le principe de communication de bout en bout. Des systèmes de double-NAT sont désormais déployés sur certains réseaux d'opérateurs pour faire communiquer les clients entre eux. Malgré cela, les dernières projections sur la vitesse de consommation des dernières plages IPv4 disponibles montrent l'épuisement du stock d'adresses IPv4 entre 2010 et 2011 **[GH1]**. Il faut donc se préparer à la migration ou, tout au moins, à l'introduction d'IPv6, et ce, en particulier sur les réseaux cœur.

L'article **[MISC3]** détaille les nombreux « mécanismes de transition » vers IPv6 qui ont été proposés jusqu'à présent. Notre article se focalise sur les mécanismes offerts pour les cœurs de réseau MPLS à la mode 6PE/6VPE, dont les points forts sont d'offrir la possibilité d'écouler du trafic IPv6 entre des îlots v6 donnés tout en conservant un cœur de réseau v4 uniquement. Nous traiterons en particulier les impacts de ces architectures sur la sécurité à l'accès et sur le cœur de réseau qui supporte la signalisation et le nouveau trafic.



Architecture de 6PE

1.3 6 PE et VPNv6 sur les cœurs de réseaux

L'article **[MISC4]** décrit en détail les solutions 6PE et VPNv6 (ou 6VPE). En quelques mots, ces solutions conservent le cœur IP/MPLS tel quel : protocole de routage IGP (OSPF ou IS-IS) inchangé, adressage IPv4, signalisation de labels MPLS inchangée (LDP ou RSVP-TE) sur IPv4, commutation de trafic labélisé **[2]**. Seuls les routeurs de bord PE nécessitent des modifications : les interfaces vers les routeurs clients (CE) sont *dual-stack* (supportent une double-pile IPv4/IPv6). Ils reçoivent sur ces interfaces du trafic IPv6 natif et activent un protocole de routage IPv6 pour obtenir les routes du CE.

En 6PE **[RFC4798]**, les PE montent des sessions MP-BGP sur des adresses IPv4 entre eux à travers le cœur pour échanger des routes IPv6 labélisées, le tout pour obtenir les routes Internet et s'échanger du trafic Internet.

En bref, dans le cas du VPNv6 **[RFC4659]**, on a les mêmes propriétés de trafic (IPv6 natif à l'*edge*, encapsulé dans deux labels sur le cœur), le même cœur IPv4, simplement les CE sont reliés aux PE sur des VRF (*Virtual Routing & Forwarding*, instances de routage et transfert dédiées) pour que chacun soit connecté à son propre VPN. Dans le cœur, les sessions MP-BGP échangent cette fois-ci des routes VPN IPv6, le trafic est du trafic client VPN et chaque CE ne voit les routes que de son propre VPN.

Dans les solutions 6PE et VPNv6, la phase d'introduction d'IPv6 dans les réseaux existants n'a pas de fortes incidences sur la politique de sécurité IPv4 sur le cœur, qui reste donc inchangée et doit être maintenue. En revanche, la politique de sécurité doit être déclinée pour IPv6 et mise en place dès le déploiement de ces nouvelles fonctionnalités, en particulier à l'accès sur toutes les zones dual-stack, sur les équipements de périphérie pour renforcer le filtrage à la fois de trafic et de routage, et sur la signalisation dans le cœur. Il faut de plus pour chaque fonction valider le niveau de sécurité avec au minimum les mêmes exigences en v6 qu'en v4.

2. Impact de l'adressage sur la sécurité

Quel que soit le mode d'introduction d'IPv6 choisi (méthode de tunnels, double pile, migration directe vers IPv6), une grande attention doit être portée au plan d'adressage du fait de sa haute influence sur l'implémentation de la sécurité et notamment du filtrage.

Le déploiement d'IPv6 représente une occasion en or pour l'architecte réseau et les ingénieurs sécurité de remettre à plat l'ensemble d'un plan d'adressage, chose qui est rarement possible sur un réseau en production, pour construire un plan efficace à la

fois au niveau du routage mais également en termes de sécurité. Plus les blocs d'adresses sont agrégés, plus la traduction de la politique de sécurité en filtres ACL de taille limitée sera simple à déployer. Notons que sur les routeurs de cœur, la taille des ACL n'a pas forcément d'impact sur les performances des routeurs, puisque, sur les équipements récents, les ACL – construites par exemple sur les adresses source et destination IPv6 – sont appliquées en hardware pour traiter le trafic ; en revanche, la diminution du nombre de lignes de configuration en facilite la gestion.

2.1 Portée des adresses

Tout d'abord, sur un réseau d'opérateur, les adresses IP sont utilisées pour répondre à plusieurs besoins : adressage du cœur en lui-même (interfaces), des liens vers les autres ISP, des clients et du management des équipements. Les différents blocs d'adresses utilisés en fonction des usages respectifs doivent être dimensionnés au mieux pour obtenir une agrégation d'adresses efficace.

De plus, plusieurs types d'adresses sont définis en IPv6 : les adresses de type *multicast*, *anycast* et *unicast* **[MISC1]**. En IPv6, les adresses unicast ont également une « portée » prédéfinie :

- Les adresses de type *Link-Local* (préfixe FE80::/10), uniques sur un lien donné, ne sont valables que sur ce lien (par exemple des interfaces Ethernet connectées sur le même LAN, deux machines établissant une connexion PPP, etc.). Les adresses de type Link-Local ont un gros avantage sur le plan de la sécurité puisqu'un routeur ne doit pas retransmettre un paquet ayant pour source ou pour destination une adresse de ce type.
- Les adresses de type *Global* sont, quant à elles, routées.

De manière générale, une adresse unicast n'a pas besoin d'une portée supérieure au lien si l'interface n'est pas utilisée en tant qu'origine ou destination d'un paquet IPv6 pour ou venant d'un équipement routeur non voisin **[RFC4291]**. Partant de ce principe, et sachant que les adresses link-local sont générées automatiquement pour toute interface d'un hôte IPv6, elles peuvent donc être avantageusement utilisées du point de vue de la sécurité à de nombreux endroits, sous réserve bien sûr que cela ne complique pas la détection des pannes sur le réseau et leur résolution. Il est donc envisageable de les utiliser notamment pour les protocoles de routage. OSPFv3 est par exemple conçu pour tourner sur les adresses de lien pour l'établissement des adjacences entre voisins.

Il serait ainsi possible d'utiliser, de configurer et monter des sessions eBGP sur les adresses unicast de liens plutôt qu'utiliser des adresses globales. Les sessions eBGP sont un bon exemple puisqu'elles ne doivent être montées en principe qu'entre deux voisins directement connectés (sauf exception des sessions eBGP multihop). Les sessions à l'accès vers les clients entre PE et CE ou les sessions vers les autres opérateurs pourraient utiliser ces adresses de lien. Le bémol est que les standards BGP précisent qu'une route IPv6 doit avoir pour *next-hop* au moins une adresse de type global (et éventuellement une adresse de lien en supplément). Ceci n'étant pas implémenté de façon stricte chez certains constructeurs, ce procédé peut être mis en œuvre ; dans tous les cas, il est toujours possible de monter les sessions eBGP sur des adresses de liens, quitte à réécrire les next-hops par des règles de politique de routage.

Une autre solution est d'établir les sessions BGP sur des adresses IPv4 pour échanger des routes IPv6 entre PE-CE. C'est d'ailleurs le cas dans le cœur où les sessions BGP sont montées sur les adresses IPv4 des PE pour l'échange des routes (routes de type IPv6 labélisées dans le 6PE ou vpnv6 dans le VPNv6). Cela simplifie la politique de sécurité et donc de filtrage dans certains cas.

2.2 Annonces des adresses internes du cœur sur l'Internet

En IPv4, lorsqu'une entité se voit attribuer une plage d'adresses IP, elle va parfois la scinder en plusieurs blocs et annoncer ce préfixe en plusieurs fois, phénomène aussi appelé « désagrégation ». Une entité choisit parfois de n'en annoncer qu'une partie et de conserver une plage d'adresses non annoncées sur Internet : ces adresses restent utilisables en interne pour des besoins précis (serveurs internes, adressage de liens, management), tout en étant injoignables depuis l'extérieur, puisque non routées depuis l'Internet. Ceci est souvent utilisé sur les réseaux cœur.

Sur l'Internet v6, la plupart des AS (Système Autonome) filtrent les préfixes plus spécifiques que /32 **[3]**. Attention, des services critiques tels que serveurs DNS anycast sont sur des /48, la règle des /32 n'est pas absolue, mais cela signifie que les préfixes dont les masques sont supérieurs à 32 ont toutes les chances d'être filtrés par de nombreux réseaux et donc de ne pas être visibles sur l'ensemble de l'Internet. Cela signifie également que, si une entité se voit affecter un /32 par un RIR (*Regional Internet Registry*, par exemple le RIPE-NCC **[4]** pour la zone Europe) ou un LIR (*Local Internet Registry*, un opérateur), elle ne pourra pas préserver une partie de ces adresses non annoncées sur l'Internet sous réserve de ne pas être atteignable du tout.

> *...la forte désagrégation des préfixes IPv4 a provoqué l'explosion de la taille des tables de routage sur l'Internet...*

D'autre part, la forte désagrégation des préfixes IPv4 a provoqué l'explosion de la taille des tables de routage ; le cap des 280.000 routes a été atteint début septembre 2008. Plusieurs raisons techniques sont évoquées pour justifier la désagrégation **[RIPE1]** ; certaines sont légitimes (ingénierie de trafic), d'autres non (erreur de configuration, mauvais plan d'adressage, incompétence).

Nous citerons l'excuse sécurité « annoncer un /24 assure qu'aucun AS ne peut annoncer de routes plus spécifiques ». Elle

::/0	Adresse par défaut
::/128	Adresse « non spécifiée » – est parfois utilisée comme source de certains paquets ICMPv6
::1/128	Adresse de loopback
::FFFF::/96	Adresses IPv4 mappées en IPv6 – utilisées en 6PE/6VPE
2001:0000::/32	Préfixe de service Teredo – mécanisme de transition
2002::/16	Préfixe de service 6to4 – mécanisme de transition
3FFE::/16	Ancienne expérimentation du 6bone
2001:DB8::/32	Non routable – réservé pour la documentation

Tableau 1 : Préfixes unicast particuliers (extrait de http://www.iana.org/assignments/ipv6-unicast-address-assignments)

a été récemment plus ou moins validée en février 2008 lorsque l'AS de Pakistan Telecom a annoncé un préfixe /24 contenant les serveurs de Youtube (qui lui annonce entre autres un /22 pour ses serveurs). Les routeurs disposant de deux routes vers la même destination choisissent toujours la plus spécifique, soit ici le /24. Cette annonce plus spécifique ayant été propagée sur l'Internet, l'AS pakistanais a ainsi attiré le trafic à destination de Youtube pendant quelques heures pour la quasi-totalité des clients. Youtube a bien tenté d'annoncer deux /25 recouvrant le /24 pour remédier à ce détournement de trafic, mais ces préfixes trop longs sont filtrés par la plupart des AS. Le *hijack* ne s'est arrêté que lorsque les routes envoyées par Pakistan Telecom ont été supprimées par son propre *provider*. Attention, il n'est toutefois pas recommandé d'annoncer une multitude de /24 sous prétexte de sécurité : en effet, de nombreux opérateurs pourraient choisir de les filtrer et ces /24 sont alors invisibles.

La désagrégation ayant de profonds impacts sur les routeurs en général (mémoire, CPU, temps de convergence), les annonces risquent d'être plus sévèrement filtrées en IPv6. Il faudra alors s'attendre à ce que les adresses IPv6 internes au réseau (*loopback*, management, liens) soient annoncées sur l'Internet, car dans le préfixe alloué à l'entité.

Si en IPv4 il est également fréquent d'utiliser d'autres plages non routables dans le cœur, telles que les adresses privées RFC1918 (10.0.0.0/8, 172.16.0.0/16 et 192.168.0.0/16), il a fallu redéfinir un équivalent d'adresses privées en IPv6 **[RFC4193]** : les adresses ULA (*Unique Local Address*), incluses dans la plage FC00::/7. Elles ne doivent pas être routables sur l'Internet, mais sont censées être routables sur un « site » (ou un AS ou un ensemble d'AS ayant des accords) et avoir un préfixe unique sur Internet ou tout du moins avec une forte probabilité d'unicité. En effet, l'identifiant de réseau d'une longueur de 40 octets doit être généré pseudo-aléatoirement ; il est même possible d'enregistrer son préfixe pour éviter qu'une autre entité ne l'utilise. Ainsi, si une adresse ULA devient visible sur l'Internet suite à une erreur, il ne devrait pas y avoir de conflit avec une autre ULA. Ces adresses sont donc tout indiquées pour remplacer les adresses privées IPv4 (qui elles n'étaient pas uniques et donc délicates à gérer en cas de fusion de réseaux) et sont utilisables sur le cœur ou encore à l'accès plutôt que les adresses unicast provenant du préfixe alloué/affecté par le RIR/LIR.

2.3 Génération des filtres de routage génériques

L'espace des adresses unicast globales attribuées à l'IANA est 2000::/3. Elles ne sont pas encore toutes allouées. Les préfixes unicast particuliers sont notamment : voir tableau 1.

D'autre part, les préfixes multicast sont dans le bloc FF00::/8. 2001:10::/28 est réservé pour les adresses ORCHID (*Overlay Routable Cryptographic Hash Identifiers*). Ce bloc est non-routable **[RFC4843]**, de même que FE00::/9 est réservé par l'IETF **[RFC4193]**, et, comme indiqué précédemment, les ULA sont en FC00::/8. Avec ces informations, il est possible de générer des filtres de type « *bogon/martians* » minimalistes listant les préfixes à refuser sur les sessions eBGP avec des *peers* externes :

Pour Cisco :

```
ipv6 prefix-list EBGP-V6 deny <préfixe-entité> le 128
ipv6 prefix-list EBGP-V6 deny 3ffe::/16 le 128
ipv6 prefix-list EBGP-V6 deny 2001:db8::/32 le 128
ipv6 prefix-list EBGP-V6 deny 2001:10::/28 le 128
ipv6 prefix-list EBGP-V6 deny 0000::/8 le 128
ipv6 prefix-list EBGP-V6 deny fc00::/8 le 128
ipv6 prefix-list EBGP-V6 deny fe00::/9 le 128
ipv6 prefix-list EBGP-V6 deny ff00::/8 le 128
ipv6 prefix-list EBGP-V6 permit any
```

Ou pour Juniper :

```
policy-statement EBGP-V6 {
   from {
        family inet6;
        route-filter <préfixe-entité> orlonger;
        route-filter 3ffe::/16 orlonger;
        route-filter ::/8 orlonger;
        route-filter 2001:db8::/32 orlonger;
        route-filter 2001:10::/28 orlonger;
        route-filter fc00::/8 orlonger;
        route-filter fe00::/9 orlonger;
        route-filter ff00::/8 orlonger;
        route-filter ::/0 upto /48 next policy;
    }
   then reject;
}
```

On refuse bien sûr son propre préfixe (préfixe-entité).

Mais, les préfixes IPv6 déjà alloués étant peu nombreux, des listes plus précises sont utilisables pour ne pas se contenter

de filtrer les bogons, mais plutôt de n'autoriser que les préfixes affectés. Selon les différents RIR, les politiques d'allocations sont variables : pour la zone Europe, le RIPE-NCC a alloué des /35 (ancienne politique), puis /32 minimum plus récemment, les plus gros blocs étant des /19, avec quelques /48 dans 2001:678::/29 pour les anycast DNS. Pour la zone américaine, l'ARIN alloue directement des /48 aux clients finaux ou à certaines infrastructures comme les points d'échange. Les blocs utilisés pour ces plages sont documentés. Les allocations de l'AfriNIC (Afrique), du LACNIC (Amérique Latine) ou de l'APNIC (Asie Pacifique) sont également documentées, ainsi que les préfixes repris par IANA ou réservés. À partir de ces informations, et des plages choisies pour les différents usages internes, il est donc possible de déduire les différents filtres à appliquer sur les sessions de routage interdomaine.

Filtre BGP résultant :

```
ipv6 prefix-list EBGP-V6 deny <préfixe-entité> le 128
ipv6 prefix-list EBGP-V6 deny   3ffe::/16 le 128
ipv6 prefix-list EBGP-V6 permit 2001:500::/30 ge 48 le 48
ipv6 prefix-list EBGP-V6 deny   2001:db8::/32 le 128
ipv6 prefix-list EBGP-V6 deny 2001:10::/28 le 128
ipv6 prefix-list EBGP-V6 permit 2001::/32
ipv6 prefix-list EBGP-V6 permit 2001::/16 ge 35 le 35
ipv6 prefix-list EBGP-V6 permit 2001::/16 ge 19 le 32
ipv6 prefix-list EBGP-V6 permit 2001:0678::/29 ge 48 le 48
ipv6 prefix-list EBGP-V6 permit 2001:0c00::/23 ge 48 le 48
ipv6 prefix-list EBGP-V6 permit 2001:13c7:6000::/36 le 48
ipv6 prefix-list EBGP-V6 permit 2001:13c7:7000::/36 le 48
ipv6 prefix-list EBGP-V6 permit 2001:43f8::/29 ge 40 le 48
ipv6 prefix-list EBGP-V6 permit 2002::/16
ipv6 prefix-list EBGP-V6 permit 2003::/16 ge 19 le 32
ipv6 prefix-list EBGP-V6 permit 2400::/12 ge 19 le 32
ipv6 prefix-list EBGP-V6 permit 2600::/12 ge 19 le 32
ipv6 prefix-list EBGP-V6 permit 2610::/23 ge 24 le 32
ipv6 prefix-list EBGP-V6 permit 2620::/23 ge 40 le 48
ipv6 prefix-list EBGP-V6 permit 2800::/12 ge 19 le 32
ipv6 prefix-list EBGP-V6 permit 2a00::/12 ge 19 le 32
ipv6 prefix-list EBGP-V6 permit 2801:0000::/24 le 48
ipv6 prefix-list EBGP-V6 permit 2c00::/12 ge 19 le 32
ipv6 prefix-list EBGP-V6 deny 0::/0 le 128
```

Ou pour les routeurs Juniper :

```
policy-statement EBGP-V6 {
    term accept {
        from {
            family inet6;
            route-filter <préfixe-entité> orlonger;
            route-filter 3ffe::/16 orlonger reject;
            route-filter 2001:500::/30 prefix-length-range /48-/48;
            route-filter 2001:db8::/32 orlonger reject;
            route-filter 2001::/32 exact;
            route-filter 2001:10::/28 orlonger reject;
            route-filter 2001::/16 prefix-length-range /35-/35;
            route-filter 2001::/16 prefix-length-range /19-/32;
            route-filter 2001:0678::/29 prefix-length-range /48-/48;
            route-filter 2001:0c00::/23 prefix-length-range /48-/48;
            route-filter 2001:13c7:6000::/36 prefix-length-range /36-/48;
            route-filter 2001:13c7:7000::/36 prefix-length-range /36-/48;
            route-filter 2001:43f8::/29 prefix-length-range /48-/48;
            route-filter 2002::/16 exact;
            route-filter 2003::/16 prefix-length-range /19-/32;
            route-filter 2400::/12 prefix-length-range /19-/32;
            route-filter 2600::/12 prefix-length-range /19-/32;
            route-filter 2610::/23 prefix-length-range /24-/32;
            route-filter 2620::/23 prefix-length-range /40-/48;
            route-filter 2800::/12 prefix-length-range /19-/32;
            route-filter 2a00::/12 prefix-length-range /19-/32;
            route-filter 2801:0000::/24 prefix-length-range /24-/48;
            route-filter 2c00::/12 prefix-length-range /19-/32;
        }
        then next policy;
    }
    term reject {
        from family inet6;
        then reject;
    }
}
```

3. Impact sur les règles de sécurité pour chaque équipement

À l'image d'IPv4, des règles de filtrages doivent être implémentées sur les interfaces des routeurs de cœur pour filtrer le trafic (ACL), ainsi que sous forme de politiques de routage pour filtrer les annonces, et assurer la protection du cœur, équipements et plates-formes de service ou de management, ainsi que celle des clients.

Les ACL (*Access Lists*) IPv6 se déclinent et s'appliquent de la même façon qu'en IPv4 sur la plupart des équipements réseau. Ainsi, sur l'IOS de Cisco, on retrouve les mots-clés `permit/deny`, l'utilisation d'adresses et/ou de ports source/destination. Ces ACL sont applicables en entrée ou en sortie sur une interface ; elles s'appliquent aussi aux vty disponibles pour le management. Les ACL étendues existent de même, ainsi que les ACL réflexives – créées dynamiquement lorsqu'un trafic matche une liste d'accès pour en autoriser le trafic retour–, mais attention à la consommation CPU sur le routeur si ces listes sont appliquées dans le plan de contrôle par le CPU générique et non en hardware.

La commande pour appliquer un filtre sur une interface sur Cisco devient en IPv6, ici pour appliquer le filtre `REJECT-IN` sur le trafic entrant :

```
(config-if)#ipv6 traffic-filter REJECT-IN in
```

Il faut également noter que sur Cisco une règle implicite est placée en chaque fin d'ACL pour autoriser la « découverte de voisins », le mécanisme qui remplace l'ARP (*Address Resolution Protocol*) pour établir la correspondance entre une adresse IPv6 et une adresse hardware :

```
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any
```

Il faut toujours au moins une entrée pour que le `deny` prenne effet.

3.1 Règles de filtrage sur les P-routeurs (cœur)

En fonction du mécanisme de transition choisi, les adresses IPv6 ne sont pas nécessaires partout lors de l'introduction d'IPv6. Dans les cas de 6PE ou de VPNv6, le cœur IPv4/MPLS étant inchangé, la politique de sécurité IPv4 sur le cœur est conservée à l'identique. D'autre part, les routeurs de cœur n'activent pas de pile IPv6. Ils restent donc purement IPv4 : management sur IPv4 en utilisant les mêmes adresses qu'avant l'introduction d'IPv6 et les mêmes protocoles (Telnet/SSH, SNMP, NTP, voire le DNS). Simplement, les MIB SNMP pertinentes pour IPv6 seront activées ; de même, des enregistrements de type AAAA pour IPv6 seront ajoutés, même s'ils sont transmis sur IPv4. Enfin, les politiques de trafic sont conservées puisque les routeurs P acheminent toujours du trafic MPLS, quelle que soit la version du protocole IP.

3.2 Règles de filtrage sur les routeurs de périphérie (PE)

Les routeurs de bordure établissant des sessions BGP vers leur provider Internet (*upstream*) doivent appliquer les filtres détaillés dans la section précédente lors de l'importation des routes, sans oublier de rajouter le préfixe IPv6 alloué à leur propre AS. Les sessions BGP montées sur des adresses IPv6 supportent l'authentification MD5, à l'instar d'IPv4.

En outre, les routeurs de périphéries qui établissent des sessions eBGP vers des clients (clients VPN ou clients Internet) doivent appliquer des politiques de routage adéquates. Rappelons qu'en IPv6, il est attendu des réseaux de n'annoncer que quelques voire un préfixe(s), et depuis un seul AS origine. Les routeurs faisant face à des clients Internet peuvent donc de manière explicite préciser la liste des préfixes autorisés c'est-à-dire le(s) préfixe(s) du client, et rejeter le reste. Si l'on prend l'exemple d'un client annonçant 2001:db8::/32, cela donne à la mode Cisco :

```
ipv6 prefix-list FROM-CUST permit 2001:db8::/32
ipv6 prefix-list FROM-CUST deny 0::/0 le 128
```

ou à la mode Juniper :

```
policy-statement FROM-CUST {
    from {
        family inet6;
        route-filter 2001:db8::/32 exact;
    }
    then reject;
}
```

Enfin, pour ce qui est des peers Internet, les filtres sont toujours plus délicats. Comme en IPv4, il s'agit de n'exporter que ses routes clientes, et de n'importer que les routes des clients du peer. Ces filtres sont difficiles à maintenir manuellement, car ils changent plus souvent. Aucune nouvelle fonctionnalité n'est apparue par rapport à la situation en IPv4. Il faut donc :

- soit faire confiance à une base de données externe telle que les IRR –*Internet Routing Registries*–, et mettre à jour dynamiquement les filtres en fonction des objets « route6 » (en espérant que notre ISP partenaire alimente soigneusement et régulièrement ces bases, ce qui est loin d'être le cas pour la plupart des bases en IPv4) ;
- soit produire un filtre générique qui à la fois limite le nombre de préfixes envoyés (à positionner en fonction du peer) et supprime les préfixes de masque trop longs, par exemple de /49 à /128, par exemple sur Cisco :

```
router bgp 65000
(...)
 address-family ipv6
  neighbor 2001:db8::2 activate
  neighbor 2001:db8::2 route-map PEER-V6 in
  neighbor 2001:db8::2 route-map PEER-V6 out
  neighbor 2001:db8::2 maximum-prefix 1000 80 restart 5
 exit-address-family
```

3.3 Lutter contre l'usurpation d'adresses à la périphérie

La lutte contre l'usurpation d'adresses doit être appliquée en IPv6 au même titre qu'en IPv4. Ainsi, il est recommandé d'implémenter une vérification uRPF (*Unicast Reverse Path Forwarding*) sur tous les liens d'interconnexion PE-CE vers les clients pour s'assurer que le paquet arrive sur la bonne interface étant donnée son adresse source. Avant activation, il faut vérifier que le matériel en question supporte cette fonctionnalité en hardware si le flux IPv6 est important ; rappelons qu'il n'est pas recommandé d'activer une telle fonction sur les interfaces vers l'Internet. Dans une architecture de type 6PE, il n'est en outre pas nécessaire de l'activer sur le cœur, puisque cette interface reçoit des paquets labellisés, d'autant plus que le routage a de fortes chances d'être asymétrique sur le cœur. Deux modes sont possibles :

- vérification que l'adresse source du paquet existe dans la table de routage et qu'elle est atteignable par cette interface avec le mode strict :

```
ipv6 verify unicast source reachable-via rx
ipv6 verify unicast reverse-path
```

- simple vérification que l'adresse source est dans la table de routage avec le mode « *loose* » :

```
ipv6 verify unicast source reachable-via any
```

Sur Cisco, il faut s'assurer que CEF (technologie de commutation des paquets « *Cisco Express Forwarding* »)

est activé sur le routeur. Le mode « loose » n'est de plus pas disponible sur tous les routeurs (*% Platform only supports strict RPF with allow-default for IPv6*). L'équivalent sous Juniper – le mode strict est activé par défaut – se configure ainsi :

```
unit 0 {
    family inet6 {
        rpf-check {
            mode loose;
        }
        address 2001:db8::2/64;
    }
}
```

Notons qu'il existe tout un éventail de solutions pour faire de la validation RPF. Si le mode *loose* est très laxiste, le mode *strict* pose parfois problème en cas de clients *multihomés*, pour lesquels le routeur préférerait une seconde route reçue du cœur plutôt que la route directe et rejetterait des paquets légitimes. Le mode *feasible-path* valide l'adresse source du paquet en prenant en compte la meilleure route, mais aussi les chemins secondaires (reçus mais non choisis). En fonction de l'architecture considérée, ce dernier mode est à privilégier.

En ce qui concerne le trafic, il est aussi recommandé de configurer des filtres de trafic à l'entrée des interfaces externes des PE pour supprimer tout paquet à destination des équipements internes. Avec 6PE ou VPNv6, aucune adresse IPv6 de management ni de plateforme de service n'est déployée. Par contre, les adresses d'interconnexion et les adresses attribuées aux clients sont autorisées, d'où l'intérêt de produire un plan d'adressage efficace. En bref, sur ces interfaces, il faut traduire les filtres IPv4 en filtres IPv6, en les adaptant toutefois aux nouveautés IPv6.

4. Nouveautés apportées par IPv6 et quelques mesures de sécurité correspondantes

Chaque nouveau protocole apporte son lot de nouvelles fonctions, mais également de nouveaux services qui sont activés par défaut sur les routeurs.

4.1 ICMPv6

Sur un routeur de type Cisco par exemple, on active l'IPv6 par la ligne ipv6 unicast-routing. Puis, sur chaque interface sur laquelle est configurée une adresse globale unicast, le routeur crée automatiquement une adresse locale au lien, active IPv6 et le transfert de paquets IPv6 sur cette interface, l'interface joint les groupes multicast du lien, etc. Certaines règles de filtrage de paquets de contrôle ICMP sont appliquées par défaut, comme montré ci-dessous :

```
CISCO#show ipv6 interface GigaEthernet2/0/0
GigabitEthernet2/0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::A:B:C:D
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF0C:D
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses

IPv6 Prefix Advertisements GigabitEthernet2/0/0
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default
       N - Not advertised, C - Calendar

PD default [LA] Valid lifetime 2592000, preferred lifetime 604800
AD 2001:100::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```

De même, sur un routeur Alcatel-Lucent (TimOS, extraits) :

```
>config>service>ies>if>ipv6# info detail
----------------------------------------------
                address 2001:32::1:0:0:0:5/126
                icmp
                    packet-too-big 100 10
                    param-problem 100 10
                    redirects 100 10
                    time-exceeded 100 10
                    unreachables 100 10
                exit
                dhcp6-relay
                    shutdown
                    exit
                    no source-address
                    no server
                exit
                dhcp6-server
                    prefix-delegation
                        shutdown
                    exit
                    max-nbr-of-leases 8000
                exit
                no local-proxy-nd
```

4.1.1 Gestion de la MTU

La MTU (*Maximum Transmission Unit*) minimale standardisée pour les paquets IPv6 est de 1280 octets. En IPv6, ce sont les équipements source et destination des paquets qui doivent les fragmenter. Un routeur sur le chemin ne doit pas fragmenter un paquet si sa taille est trop importante. Il est donc capital que tous les éléments cœurs aient une MTU égale ou supérieure à cette valeur. Comme en IPv4, le filtrage de tous les types de paquets ICMP est souvent une très mauvaise idée et rend le *troubleshooting* difficile. Ainsi, la découverte automatique de MTU se faisant grâce à ICMPv6, il ne faut pas filtrer les messages ICMPv6 type 2 « *Packet Too Big* » si l'on veut autoriser les hôtes à découvrir la MTU adéquate. Pour éviter que les routeurs P ne

rejettent des paquets trop gros, et connaissant la MTU minimale du cœur, une solution est de fixer cette MTU minimale sur les liens d'interconnexion des PE et d'autoriser ces PE à renvoyer les paquets ICMPv6 type 2 cités ci-dessus.

4.1.2 Désactivation des annonces de routage

À partir du moment où IPv6 est activé sur l'interface Ethernet d'un routeur Cisco, il envoie des annonces de routage, fonction activée par défaut en général (RA, *Router Advertisement*, dans le cadre de la « découverte de voisin » précédemment expliquée). Or, si les interfaces sont configurées manuellement et que l'autoconfiguration n'est pas utilisée, ces annonces sont inutiles. Pour éviter toute attaque utilisant des annonces RA forgées (cf. **[MISC2]**, **[RFC3756]**), les RA sont désactivables interface par interface sur quasiment tous les routeurs, comme ici :

```
interface GigabitEthernet2/0/0
 description *** 6PE TO CE ***
 logging event link-status
 ipv6 address FE80::A:B:C:D link-local
 ipv6 address 2001:db8::aaaa:1/64
 ipv6 enable
 ipv6 nd ra suppress
```

Sur les équipements qui autorisent par défaut la redirection de messages, cette redirection est supprimée par `no ipv6 redirect`.

Sur Juniper, les annonces de routeur sont activées par configuration explicite :

```
sarah@Jun> show configuration protocols
router-advertisement {
    interface ge-0/2/0.0 {
        prefix 2001:db8:0:ff::/64;
    }
}
sarah@Jun> show ipv6 router-advertisement
Interface: ge-0/2/0.0
  Advertisements sent: 160, last sent 00:03:32 ago
  Solicits received: 0
  Advertisements received: 11
  Advertisement from fe80::a:b:c:d, heard 00:21:21 ago
    Managed: 0
    Other configuration: 0
    Link MTU: 1500 bytes
    Reachable time: 0 ms
    Default lifetime: 0 sec
    Retransmit timer: 0 ms
    Current hop limit: 64
```

Enfin, pour remplir un cache de voisins, la plupart des routeurs acceptent de configurer en dur l'adresse du voisin, par exemple avec la commande :

```
ipv6 neighbor <ipv6-address> <interface-type interface-number> <hardware-address>
```

Ceci évite toute attaque possible, et peut être avantageusement utilisé sur les liens de type PE-CE par exemple. En effet, sur un cœur de réseau, la topologie est relativement stable. L'opérateur est donc à même de configurer statiquement à la fois les adresses link-local et les voisins sur chaque interface des équipements.

Pour conclure sur ICMPv6, les nouveaux types et codes des paquets intéressants à filtrer ou autoriser sont :

- *Destination Unreachable* (1/0) ;
- *Packet too big* (2/0) ;
- *Time/TTL exceeded* (3/0) ;
- *Parameter problem* (4) ;
- *Echo reply* (128/0) ;
- *Echo request* (129/0) ;
- *Router Solicitation* ou RS (133/0);
- *Router Advertisement* ou RA (134/0);
- *Neighbor Solicitation* ou ND-NS (135/0) ;
- *Neighbor Advertisement* ou ND-NA (136/0) ;
- *Redirect* (137/0).

Dans le cas d'un opérateur qui configure en statique les adresses de liens, on autoriserait seulement les six premiers. Dans tous les cas, la redirection doit être interdite. Le document **[RFC4890]** donne de précieuses indications pour l'adaptation des filtres ICMP existants aux nouveautés v6. Le script TCL suivant, de François Ropert, adapte les lignes iptables données en annexe de ce RFC en filtre Cisco IOS: **http://blog.packetfault.org/icmpv6.tcl**.

4.2 Désactivation du multicast IPv6

Sur certaines versions de routeurs, PIM (*Protocol Independent Multicast*, protocole de routage qui construit des arbres multicast sur le cœur) ou MLD (*Multicast Listener Discovery*, par lequel un routeur de bordure IPv6 échange avec ses voisins des informations sur les groupes multicast **[5]**) sont par exemple activés par défaut. En l'absence d'application utilisant le multicast sur un réseau donné, le seul trafic multicast IPv6 autorisé doit être le trafic ICMPv6 pour la découverte de voisins (paquets ND-NS et ND-NA hors « RA »/« RS »). Le reste est à filtrer sur les interfaces dual-stack (PIM, MLD qui fait jouer les paquets ICMPv6 de types 130 131 et 132 et quelques supérieurs, et le transfert IPv6 multicast) :

```
interface GigabitEthernet2/0/0
 no ipv6 mld router
 no ipv6 mfib forwarding
 ipv6 nd suppress-ra
 no ipv6 pim
```

4.3 Remarquage de paquets en entrée de réseau

En ce qui concerne la Qualité de Service et la classification, le champ ToS (*Type Of Service*) des en-têtes IPv4 est traduit en champ `Traffic Class` dans les en-têtes IPv6, qui contient les informations de DSCP. Les paquets en provenance des réseaux externes doivent donc expressément être remarqués à l'entrée

du réseau en accord avec les politiques de trafic et de sécurité pour éviter que des paquets entrants éventuellement marqués ne deviennent prioritaires. La politique de remarquage doit être correctement positionnée sur les PE. Elle est par exemple présente par défaut sur les routeurs Alcatel.

4.4 Le filtrage sur les en-têtes IPv6

En IPv6, il est désormais possible de chaîner les en-têtes des paquets : le champ `next header` ou prochain en-tête peut aussi bien pointer sur un protocole de niveau supérieur (TCP, UDP,...) qu'une extension IPv6. Ces extensions, optionnelles, contiennent des informations qui sont traitées soit par la destination comme AH/ESP ou encore les en-têtes de routage (« *routing-header* »), ou par les équipements traversés comme les en-têtes `hop-by-hop`.

4.4.1 Hop-by-hop

Cette extension est définie pour être traitée par tous les routeurs sur le chemin du paquet ; s'il y a plusieurs extensions, elle se trouve toujours en premier. Elle est utilisée entre autres pour le support de MLD (multicast) ou les datagrammes « jumbo » c'est-à-dire de taille supérieure à 65535 octets. Si un routeur ne sait pas traiter les informations contenues dans ce champ, le paquet est supprimé et le routeur envoie un message ICMP type 4 (code 1, « *unrecognized Next Header type encountered* »). Notons que les paquets contenant un header `hop-by-hop` sont traités en soft par le routeur et donc consommateurs de ressources.

Exemple d'ACL pour rejeter ces paquets :

```
# show firewall
family inet6 {
    filter NO-EXT {
        term reject {
            from {
                next-header hop-by-hop;
            }
            then {
                reject;
            }
        }
    }
}
```

Normalement, toutes les autres extensions doivent ne pas être traitées par les routeurs de cœur pour les paquets en transit : les remarques suivantes ne s'appliquent qu'aux paquets à destination du cœur (blocs d'adresses internes, de management et d'interconnexion). Les paquets en transit ne sont pas filtrés pour ne pas dégrader des services qui utiliseraient ces extensions.

4.4.2 Flow Label

Hormis le champ de classe de trafic, un champ supplémentaire `flow label` a été défini pour gérer de la qualité de service. Si aucun service n'utilise ce champ, certes spécifié, mais dont les applications se font attendre, il faut a minima ignorer les informations contenues dans ce champ, en particulier pour les paquets autorisés à destination du cœur de réseau comme les sessions BGP. Notons que les implémentations IPv6 n'étant pas encore éprouvées, la probabilité de rencontrer des bugs sur les traitements de ces en-têtes par les routeurs ou les terminaux finaux n'est pas négligeable, comme CVE-2006-5619.

4.4.3 Routing header

Plusieurs types de routing header sont normalisés. Le type 0 rappelle le *source routing* IPv4 ou routage par la source, dans lequel on suggère une liste de routeurs intermédiaires à traverser pour joindre la destination. Un des cas d'usage du routage par la source est la mobilité IPv6, où l'on spécifie l'adresse d'un routeur « agent mère » qui se charge de renvoyer les paquets vers des terminaux en situation de mobilité. Rappelons qu'en IPv4 le routage par la source était inutilisé, d'une part parce que consommateur de ressources, et surtout non sécurisé car facilitant le contournement de règles de filtrage. Pour éviter que l'usage des routing headers en IPv6 ne soit supprimé et donc n'empêche l'essor des services fondés sur la mobilité IPv6, les routing headers de type 2 ont été créés, plus limités, dans lesquels seule une adresse est définie (celle de l'agent mère).

Dès le départ, des propositions avaient été faites pour ne faire traiter les en-têtes de routage que par les hôtes ; cela n'avait pas été accepté. Mais suite aux failles de sécurité découvertes et mises en pratique en 2007 sur ces en-têtes de routage **[BIONDI]**, l'IETF a décidé de supprimer l'usage des types 0 tout en conservant la possibilité de traiter les types 2. Sur un réseau 6PE ou VPNv6, il faut donc a minima éviter de traiter tout paquet avec des routing header 0. La commande globale no ipv6 source-route sur les IOS(-XR) récents supprime les types 0 et ne filtre pas les types 2. La règle suivante filtre tout paquet contenant des routing-headers :

```
C10A(config)#ipv6 access-list NO-RH
C10A(config-ipv6-acl)#deny ipv6 any 2001:db8::/32 routing
C10A(config-ipv6-acl)#permit ipv6 any any
C10A(config-ipv6-acl)#exit
C10A(config)#interface Gi2/0/0
C10A(config-if)#ipv6 traffic-filter NO-RH in
```

ou l'équivalent sur JunOS :

```
[edit firewall family inet6 filter NO-EXT]
# term reject {
    from {
        next-header routing;
    }
    then {
        count RT-HEADER;
        log;
        reject;
    }
}
```

Pour un réseau 6PE/VPNv6 qui ne déploie pas de services particuliers, tels que la mobilité IPv6, tous les paquets avec un

routing header à destination des adresses internes au cœur sont suspects et sont à supprimer.

4.4.4 Renforcement des filtres sur les extensions

Une des techniques d'évasion du filtrage des extensions est que, les paquets étant fragmentés par la source, certaines extensions se retrouvent dans des fragments ultérieurs dans des cas défavorables (source malveillante). Pour limiter cet effet, il faut configurer un filtre qui vérifie que tous les fragments sauf le dernier ont une taille minimale de 1280 octets (MTU IPv6), et supprimer les paquets ne répondant pas à cette condition.

Dans le cas de 6PE ou VPNv6 et selon l'offre de service, les filtres peuvent aussi être configurés de manière à n'accepter que les paquets IPv6 à destination du cœur qui ne contiennent pas d'options spécifiques et donc dont le *next-header* est un protocole de couche supérieure (transport TCP, UDP, ICMPv6). Sur un routeur Cisco, le mot clé `undetermined-transport` dans une ACL correspond à tout paquet dont on ne sait déterminer quelle est la couche 4.

Pour les paquets à destination du cœur, si l'on se contente de vérifier que le next-header est bien une application (protocole de routage, ICMPv6), les filtres sont alors appliqués au niveau du plan de transfert. En effet, sur les matériels récents, et à l'exception des paquets contenant une extension `hop-by-hop`, les routeurs de cœur supportent en général des ACL sur les en-têtes en hardware à condition que la chaîne d'en-têtes ne dépasse pas une certaine taille ; ces filtres ne devraient donc pas impacter fortement les performances du routeur.

Conclusion

En activant la cohabitation des piles IPv4 et IPv6 sur des zones limitées, à savoir l'interconnexion des PE vers l'extérieur, le déploiement des mécanismes 6PE et VPNv6 sur le cœur est relativement simple et ne bouleverse pas l'architecture existante. Ces mécanismes passent de plus très facilement à l'échelle, et favorisent une migration en douceur vers une architecture cible dual stack. Toutefois, le déploiement nécessite la configuration de nombreux filtres et fonctions de sécurité.

Les fonctionnalités IPv6 n'ayant pas été très éprouvées jusqu'à présent, il y a toujours des risques de bugs, mais cette solution semble tout de même avantageuse par rapport à d'autres mécanismes de transition plus complexes qui pourraient introduire plus de failles de sécurité. Si les fonctions 6PE sont disponibles et semblent être favorables aux opérateurs pour faire cohabiter des paquets IPv4 et IPv6, il faut également valider les outils de supervision : les différentes sondes de trafic ou protocolaires, les nouvelles MIB SNMP (pas toujours disponibles), les compteurs, le *netflow* et autres outils de vérification de configuration, de façon à assurer un niveau de sécurité au moins identique à celui que l'on connaît aujourd'hui en IPv4.

Notes

[1] Actuellement, tous les routeurs proposant une pile IPv6 (minimale) n'offrent pas encore IPsec par exemple.

[2] L'article sur les sondes de réseau du même dossier présente ces divers protocoles.

[3] Sur l'Internet v4, la plupart des AS acceptent de router des préfixes de tailles /24 ou inférieures.

[4] Réseaux IP Européens – Network Coordination Center

[5] L'équivalent de MLD en IPv4 est l'IGMP (Internet Group Management Protocol).

Références & Liens

[BIONDI] BIONDI (Philippe), EBALARD (Arnaud), « *IPv6 Routing Header Security* », 2007, **http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf**

[MISC1] DENIEL (Philippe), « IPv6 : une brève introduction », MISC#27.

[MISC2] DESFOSSEZ (Julien), LUIGGI (Jean-Philippe), DUSERRE (Anne-Sophie), « Les attaques IPv6 », MISC#27.

[MISC3] DESFOSSEZ (Julien), LUIGGI (Jean-Philippe), DUSERRE (Anne-Sophie), « Mécanismes de transition IPv4 et IPv6, attaques », MISC#27.

[MISC4] DECRAENE (Bruno), NATAF (Sarah), « IPv6 sur MPLS : 6PE et VPNv6 », MISC#27.

[GH1] « *IPv4 address report* » : **http://www.potaroo.net/tools/ipv4/index.html**

[RFC3756] NIKANDER (P.), KEMPF (J.), NORDMARK (E.), « *IPv6 Neighbor Discovery (ND) Trust Models and Threats* », mai 2004, **http://www.ietf.org/rfc/rfc3756.txt**

[RFC4193] HINDEN (R.), HABERMAN (B.), « *Unique local IPv6 unicast address* », oct. 2005, **http://www.ietf.org/rfc/rfc4193.txt**

[RFC4291] HINDEN (R.), DEERING (S.), « *IP version 6 addressing architecture* », fév. 2006, **http://www.ietf.org/rfc/rfc4291.txt**

[RFC4659] CLERCQ DE, OOMS, CARUGI, LE FAUCHEUR, « *BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN* », sept. 2006, **http://www.ietf.org/rfc/rfc4659.txt**

[RFC4798] CLERCQ DE, OOMS, PREVOST, LE FAUCHEUR, « *Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)* », fév. 2007, **http://www.ietf.org/rfc/rfc4798.txt**

[RFC4843] NIKANDER (P.), LAGANIER (J.), DUPONT (F.), « *An Ipv6 Prefix for ORCHID* », avril 2007, **http://www.ietf.org/rfc/rfc4843.txt**

[RFC4890] DAVIES (E.) MOHACSI (J.), « *Recommendations for Filtering ICMPv6 Messages in Firewalls* », sept. 2007, **http://www.ietf.org/rfc/rfc4890.txt**

[RIPE1] SMITH (P.), EVANS (R.), HUGUES (M.), « *RIPE Routing Working Group Recommendations on Route Aggregation* », déc. 2006, **http://www.ripe.net/ripe/docs/ripe-399.html**

⇨ CIZAULT (Gizèle), « IPv6 Théorie et Pratique », disponible en ligne : **http://livre.point6.net/index.php/Accueil**

François Ropert, fropert@packetfault.org – http://blog.packetfault.org

LE TRÈS HAUT DÉBIT – UN CHALLENGE POUR LA SÉCURITÉ

mots clés : *réseaux / très haut débit / monitoring / forensics*

Les réseaux à très haut débit sont une nouvelle tendance résultant d'applications de plus en plus consommatrices en bande passante sur Internet et en entreprise. Cet article explique les changements technologiques et pratiques auxquels feront face les administrateurs réseaux et analystes en sécurité. A commencer par les modifications apportées aux interfaces physiques, puis aux outils de surveillance pour ensuite aborder le récent intérêt du forensics réseau ainsi que les modifications apportées aux équipements de sécurité.

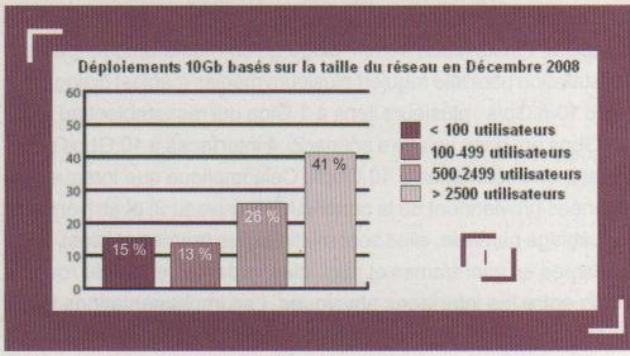
1. Évolution du réseau

1.1 Les réseaux d'entreprises et les datacenters

Nous faisons face au début de la migration des réseaux 10 gigabits. De nos jours, 13% des plus grandes entreprises dans le monde ont déjà migré vers le 10 gb et 11% supplémentaires comptent le faire d'ici la fin de l'année. Les entreprises effectuant cette migration sont des entreprises décrites sur la figure 1. La taille de l'entreprise n'est évidemment pas l'unique argument. Il y a généralement un réel besoin en bande passante supplémentaire ainsi qu'une ingénierie du trafic pour les communications unifiées, la voix sur IP, le Web 2.0, mais aussi l'ajout continuel d'applications métier.

Les utilisateurs deviennent de plus en plus « débitvores » et, plus que jamais, dépendants du réseau. Chacun a pu le constater, un bon réseau est un réseau dont les utilisateurs ne se plaignent pas. En environnement « datacenter », les flux de données IP classiques, SAN (*Storage Area Network*) et HPC (*High Productivity Computing*) vont s'unifier grâce à une trame supplémentaire transportée par Ethernet reléguant dans le passé les architectures classiques en silos. Le Fibre Channel a la particularité d'être *lossless* (il est impensable de perdre des trames). Il est possible de garder cette caractéristique en passant sur Ethernet grâce à la trame PAUSE. Son but est de suspendre la transmission de trafic entre deux commutateurs si l'un des deux est congestionné. Une fonction peu connue, mais qui existe depuis la nuit des temps.

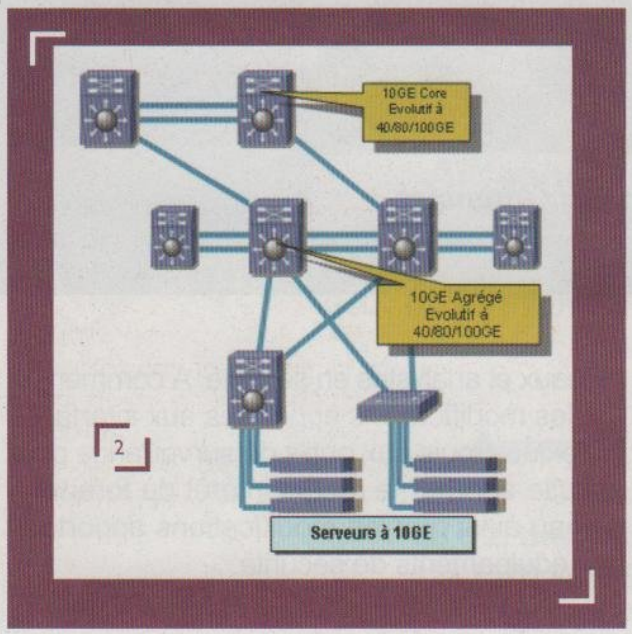
L'arrivée de ces nouveaux réseaux implique une refonte conséquente des équipements, ainsi qu'une nouvelle approche dans la manière de travailler des administrateurs réseau.



2. Les sondes d'analyses multigigabits

2.1 Des interfaces physiques à 10GbE et plus

Un réseau à très haut débit ressemble dans l'idéal à celui illustré à la figure 2.



2

Il est nécessaire de revenir sur quelques fondamentaux du 10 GbE (10 Gigabit Ethernet) qui sont déterminants pour la compréhension et le bon usage du monitoring sécurité du réseau.

Premier point important, la compatibilité entre matériels 10 GbE. Personne de nos jours ne peut certifier que le matériel 10 GbE d'un équipementier sera compatible avec un commutateur 10 GbE d'un autre fabricant. La faute en incombe à la couche PHY (couche physique).

Vient ensuite le câblage. Il existe deux manières d'intégrer le 10GbE au niveau de la couche physique sur le WAN (généralement en fibre optique) : soit en série, soit en parallèle. L'installation série n'exige qu'un média unique (câble). L'installation parallèle requiert plusieurs médias (câbles) dialoguant avec 10/n Gb/s : plusieurs liens à 1 Giga qui rassemblent au total 10 Gbps ou, dans un autre scénario, 4 interfaces à 10 Gbps pour obtenir une connexion à 40 Gbps. Cela implique que lorsque les données proviennent de la couche MAC (niveau 2) et arrivent sur un câblage parallèle, elles sont multiplexées (trames et idles), puis séparées en mini-trames et mini-idles, réparties en mode *round-robin* entre les interfaces physiques. Les implémentations LAN sont légèrement plus rapides grâce au préambule Ethernet dont la taille est de 8 octets comparé aux implémentations WAN de type SONET/SDH et POS (*Packet Over SONET*) qui utilisent une méthode d'encapsulation plus complexe et un *overhead* plus grand qu'Ethernet.

La rétrocompatibilité 1000 Mbps (Gigabit Ethernet) et 10 GbE est également un point à prendre en compte. Non pas dans la perspective d'acheter des commutateurs 10 GbE pour « faire du 1 gbE ». La rentabilité d'une telle opération est relativement douteuse. En revanche, rien n'interdit d'imaginer qu'un hôte à 1 gbps se connecte au commutateur 10 GbE, le port à 10 gbps détectera et négociera la vitesse du port à 1 gbps se connectant à un commutateur 10 GbE. Dans ce cas, le port à 10 gbps détectera et négociera la vitesse du port à 1 gbps. Insistons sur le fait, une fois de plus, que rien ne certifie aujourd'hui qu'une carte réseau 1 gbps puisse fonctionner avec n'importe quel commutateur 10 gbps.

Au-delà de cette particularité de couche 1, les cartes réseau sont elles-mêmes améliorées afin d'être plus performantes grâce à de nouveaux algorithmes d'optimisation.

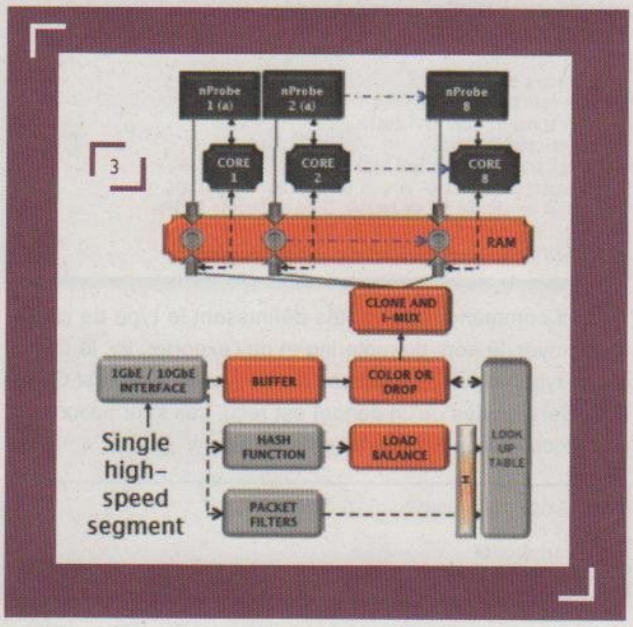
Ouvrons à ce sujet une parenthèse à propos de la perte de trame. Cette perte a trois origines : les collisions, les erreurs de transmissions et la congestion. En 10 GbE, il n'y pas de collisions du fait de la nature *full-duplex* du lien. Les erreurs de transmissions (FCS – *Frame Check Sequence* générant un CRC-16 ou CRC-32) restent rares. Quant à la congestion, elle ne relève pas d'un problème de carte réseau, mais de commutateur.

2.2 Le matériel utilisé pour capturer les paquets

Afin de capturer des paquets de tailles variables sur des liens à 10 Gbps, des améliorations matérielles sont nécessaires sur les cartes réseau. Les solutions de monitoring réseau et sécurité utilisent des cartes spécialement développées pour traiter cette grande quantité de données. Le bus PCI-Express (PCI-X) est utilisé pour transporter les données entre la carte et le reste du système. Au cœur de ces cartes, une FPGA (*Field-Programmable Gate Array*) qui décharge le CPU des opérations lourdes. La particularité de ces cartes est de capturer le plus de paquets possibles sur des bases de la nanoseconde sans décalage dans le temps. Cela a son importance pour des flux financiers ou plus généralement dans le milieu bancaire. Les cartes classiques ne sont pas développées pour avoir un *timestamp* proche de l'exactitude et sont dépendantes de la qualité de gestion des interruptions de la carte réseau et du système hôte. Par exemple, certaines cartes génèrent une

...Les solutions de monitoring réseau et sécurité utilisent des cartes spécialement développées...

interruption seulement après réception de plusieurs paquets au lieu d'une interruption par paquet. Cela a pour conséquence de créer un décalage dans le temps. Il ne faut pas oublier non plus qu'un paquet de 64 octets sur un lien Gigabit arrive à destination en 0.512 µs alors que la plupart des horloges à quartz dans un PC ont une précision d'une microseconde. Ici, la solution est d'utiliser une carte intégrant un récepteur GPS accompagné d'un bout de code intégré au driver de la carte réseau spécifiquement pour la gestion de l'horloge. Celui-ci a une précision de l'ordre de la nanoseconde. La carte ne possède pas d'adresse MAC et ne participe à aucun traitement relevant de la couche 2. Il est par conséquent impossible pour une personne mal intentionnée d'utiliser l'ARP *spoofing* afin de récupérer les paquets traités par la carte. La plupart des systèmes d'exploitation Linux, Windows, FreeBSD et parfois Solaris sont supportés.



À titre d'exemple, l'architecture interne d'un boîtier Endace [1] (voir Figure 3) possède huit cœurs Intel qui se partagent la charge de traitement.

D'autres cartes existent comme la Tilera TILExpress 64. C'est une carte 64 bits programmable en C. Elle est moins intéressante que les cartes Endace du fait qu'elle ne gère pas le *multithreading* et n'a pas de ports 10 GbE intégrés. Ses utilisateurs devront « se contenter » de 12 ports Giga.

Quant aux cartes Intel de génération récente, elles intègrent un *pre-fetch* (un cache) d'en-têtes TCP/IP. Il est possible de partager la file de réception des paquets à travers plusieurs CPU physiques ou logiques. Globalement, on constate une réduction drastique du nombre de cycles CPU et du nombre d'I/O entre les différents composants traversés et indépendamment du système d'exploitation utilisé. Sous Linux, un module noyau est écrit spécialement pour la carte Intel par Myricom. À noter que le *driver* `myri10ge` disponible dans le noyau Linux 2.6 n'est pas optimisé. Il faudra y ajouter à la main le *firmware*, téléchargeable sur le site de Myricom [2] au niveau du processus *hotplug*. La carte Intel coûte environ 1000 dollars.

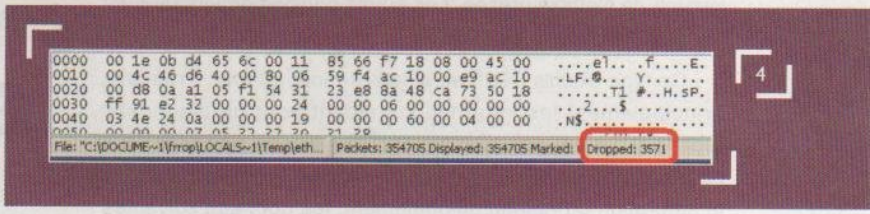
Les principales cartes étant décrites, nous abordons à présent les outils permettant de surveiller un lien multigigabit.

3. Les outils de monitoring

3.1 Les outils embarqués

Il existe deux types de sondes capables de garantir un monitoring efficace et une remontée des alertes de sécurité. Les sondes de *sniffing* intégrées dans les routeurs et commutateurs : SPAN (*Switched Port Analyzer*) et RITE (*Router IP Traffic Export*), ainsi que les Netflow. Les SPAN et RITE effectuent une copie de trafic d'un port unique, de plusieurs ports ou d'un VLAN vers un autre port. Un port auquel est connecté une station équipée d'un sniffer comme *ethereal/wireshark* [3]. Il est important de noter que lorsqu'une station est connectée au port SPAN, elle ne peut plus communiquer sur le réseau.

Ces deux fonctionnalités logicielles possèdent plusieurs défauts : le SPAN (copie de trafic sur un commutateur) ou le RITE (copie de trafic sur un routeur) induisent de la latence, rejettent les trames mal formées jusqu'au niveau 2 et ne sont pas adaptés pour des liens très utilisés. C'est ce dernier point qu'illustre la figure 4 par laquelle un nombre conséquent de trames sont *droppées*. Le trafic capturé ne reflète pas le trafic réel : « **What you see is NOT what you get** ».



La tâche première d'un routeur, ce point est important, consiste à prendre une décision de routage et commuter les paquets, et non d'en réaliser une copie. D'expérience, un analyseur de trames de type wireshark n'est pas du tout adaptable de manière ascendante pour renifler un réseau multigigabit en mode SPAN. Dans ce cas précis, il est vain d'espérer capturer plus d'une minute de trafic lorsque le lien est très utilisé. Et ce, pour deux raisons : la capacité de stockage du disque dur d'une part, et

les performances de wireshark. La dissection des paquets se terminera très probablement par un « *Out of memory* ».

L'autre outil embarqué, Netflow, permet d'établir une matrice du réseau. Elle décrit *Qui parle à qui et en quelle quantité*. Typiquement, Netflow enregistre l'adresse IP source et destination ainsi que le port TCP ou UDP utilisé. Il offre ainsi la possibilité de réaliser des statistiques, portant sur l'utilisation des protocoles et applications sur le réseau. Osons une analogie avec le monde de la téléphonie : Bob et Alice s'appellent durant 30 minutes. L'opérateur téléphonique connaît avec exactitude la durée de la communication, mais ignore tout du contenu de la conversation.

Netflow est intégré en deux parties sur les routeurs et commutateurs :

- Le *metering process* : le processus se charge de récupérer les informations depuis les informations collectées localement par les routeurs/commutateurs grâce aux tables de commutation CEF, dCEF (distribution entre *linecards*) ou encore PXF. Ces tables de commutation ont pour rôle de trouver le meilleur chemin lorsqu'un paquet entre par un port et doit sortir par un autre port du commutateur.
- L'*export process* : le processus se charge d'envoyer les *templates* **[4]** (uniquement pour la version 9 de Netflow) à un collecteur qui se chargera de traiter les données. Un template contient le nom de champs supplémentaires qui seront transmis à l'intérieur du paquet Netflow ; par exemple, un numéro de VLAN ou un numéro d'AS BGP.

Il est souvent dit que Netflow est propriétaire Cisco. C'est une demi-vérité, puisque seul le metering process est propriétaire. L'export process ne l'est pas et fait partie de standards de l'IETF.

Il faut également préciser que Netflow n'est pas supporté sur tous les matériels Cisco. Il existe parfois de subtils problèmes de compatibilité matérielle entre les modèles de cartes supervisor et les gros châssis de commutation (4500, 6500,...). Il existe également des subtilités dépendant de la version d'IOS au niveau des informations récupérables, sans parler des différences de version de Netflow utilisée. Les autres équipementiers utilisent généralement le standard sFlow.

Ce type d'outils (Netflow, sFlow, J-Flow, QFlow...) remonte principalement les informations aidant pour un diagnostic réseau et permet, par exemple, l'observation de pics anormaux de trafic provoqués par un déni de service, lequel occasionne la saturation du réseau. Globalement, les données suivantes sont récupérables :

- adresses IP sources et destination ;
- *top talkers* (les machines les plus bavardes sur le réseau) ;
- identification des flux applicatifs au moyen des ports TCP et UDP.

Ces informations peuvent être complétées grâce aux templates de Netflow v9, lesquels offrent un niveau d'information plus complet. Des champs relatifs au *multicast*, MPLS, IPv6, QoS, les drapeaux TCP, le *payload* (qui débute par les en-têtes de niveau 3) sont récupérables.

L'expérience recommande de ne pas surcharger ces templates, en ne perdant jamais de vue la limitation par la taille de la MTU.

Ce qui suit est un exemple de configuration dans lequel sont récupérés le champ TTL (*Time To Live*) ainsi que la taille en octets des paquets ICMP en transit et à destination du routeur exportant ses Netflow vers la machine 192.168.3.4 :

```
flow record MISCmag
 match ipv4 ttl
 match transport icmp ipv4 code
 collect counter octets
 collect transport icmp ipv4 type
flow exporter SecFLOW <= Vers où envoyer les informations
 destination 192.168.3.4 <= Adresse IP du collecteur Netflow
 ttl 1
 transport udp 2008 <= Port UDP d'écoute du collecteur
```

Les commandes suivantes définissent le type de cache à employer, le nom du metering et de l'exporter. Ici, le cache est de type `immediate`. C'est une file de type FCFS (*First Come First Serve*) : dès qu'un paquet est reçu, ses informations de connexions sont envoyées au collecteur :

```
flow monitor MISCmonitoring
 record MISCmag
 exporter SecFLOW
 cache type immediate
```

Pour terminer, il suffit d'appliquer la configuration à une interface et à la direction du monitoring :

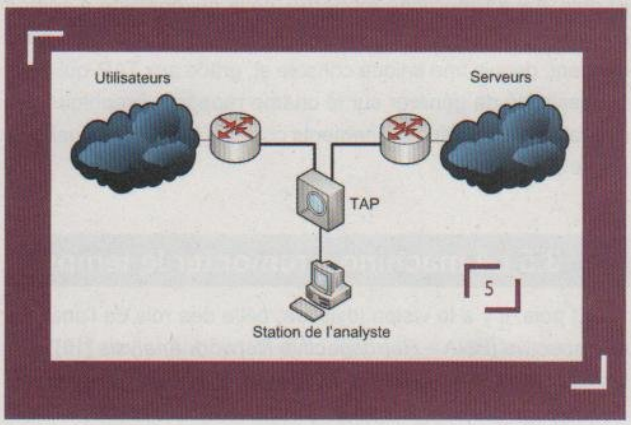
```
interface Serial3/0
ip address 200.100.50.1 255.255.255.252
ip flow monitor MISCmonitoring input
```

Netflow est embarqué dans les routeurs et commutateurs haut de gamme. Il existe des solutions matérielles qui sont dédiées au monitoring du réseau et indépendantes des fonctionnalités embarquées à l'intérieur des équipements réseau.

3.2 Les outils dédiés

Le TAP (*Test Access Ports*) ou robinet est un boîtier dédié passif spécialement conçu pour la surveillance d'un réseau. Son rôle est de capturer les paquets sans la moindre altération ainsi que dans leur intégralité de la couche 1 jusqu'à la couche 7. Il les expédie ensuite à destination d'une ou plusieurs stations distantes qui lanceront une analyse desdits paquets. Le rôle d'une station peut être unique ou multiple : qualité de services, VoIP, sécurité, analyse applicative,... tout n'est qu'une question de besoin et de temps si un développement est nécessaire pour une utilisation particulière comme l'analyse protocolaire d'un produit développé en interne.

Un TAP se place physiquement entre deux équipements réseau dont il est souhaitable d'analyser le trafic échangé (voir Figure 5). Ces équipements peuvent être des routeurs, commutateurs ou pare-feu. Un ou deux câbles (s'il est indispensable de récupérer le trafic en full-duplex) relient le TAP à une station, laquelle remplit généralement la fonction d'analyseur de trames, de collecteur Netflow ou d'IDS. Elle analyse le contenu du trafic entre les deux équipements. Avec un TAP, il n'est pas nécessaire de paramétrer les équipements réseau surveillés a contrario du SPAN [5] et du RITE [6]. D'ailleurs, si aucune station n'est connectée au TAP, son fonctionnement est en mode *fail-open*. C'est-à-dire que le trafic continue de s'écouler entre les deux équipements réseau, même en l'absence de station de surveillance du lien.



D'un point de vue performances et analyse, c'est le meilleur scénario possible. Premièrement, une analyse des liens n'engendre aucune pénalité de performances induites par un traitement logiciel local au routeur puisque aucun processus ne tourne pour exporter le trafic vers le TAP. Deuxièmement, les TAP ont l'avantage, par rapport aux SPAN/RITE, de transporter toutes les trames même si elles sont mal formées. Le TAP ne *drop* aucun trafic d'une manière générale, ni ne génère un décalage dans le chronodiagramme (*timeline*).

Ajoutons enfin que certains TAP sont capables d'exporter les données reçues vers un collecteur Netflow en version 9.

Il est bon de rappeler que si un TAP tombe en panne, cela n'entraîne aucune incidence sur le lien surveillé (qu'il soit cuivré ou fibré), du fait de la nature passive du boîtier. La connexion physique sera donc toujours disponible. Par mesure de précaution, ces équipements possèdent généralement une double alimentation afin que le lien entre la station de monitoring et le TAP lui-même soit toujours disponible.

Quoi qu'il en soit, sur un brin de réseau très utilisé et critique, il faut définitivement écarter toute idée de copie de trafic en SPAN/RITE. Ces modes ne sont à utiliser qu'en cas de problèmes de connectivité au niveau du port d'une machine ou à la rigueur, en amont d'un accès Wi-Fi.

3.3 Les outils libres

Les plus aventureux peuvent installer un système libre BSD/Linux associé à des cartes réseau dédiées et haut de gamme. Il est ainsi envisageable de constituer un système de surveillance de hautes performances. Encore ne faut-il pas perdre de vue les limites « physiques » de la carte réseau utilisée et du système d'exploitation. À force de patience et d'astuces d'optimisation, les plus acharnés parviendront à passer de 110kpps en *userland* à 300kpps, après des heures de travail sur un module noyau fabriqué pour l'occasion. Il est peut-être plus sage d'investir dans une carte réseau sérieuse, telles que celles citées précédemment.

Ajoutons que si cette solution « open » s'avère très peu chère en comparaison des produits commerciaux, elle ne possédera pas leurs perfectionnements techniques : redondance d'alimentation électrique, mode de *bypass* en cas de défaillance de la machine (n'oublions pas que ce PC est un élément actif qui, en cas de panne, peut « isoler » une partie du réseau sur lequel il est intercalé. En outre, le logiciel libre le plus utilisé, fprobe, n'est capable d'exporter qu'en Netflow version 1, 5 ou 7. Ce qui vous interdit de pouvoir utiliser un template et de prendre en compte des informations telles que le numéro de VLAN ou la QoS. Reste à la disposition de l'administrateur que la possibilité d'obtenir une matrice simple du réseau créée à partir d'informations de niveau 3 et 4.

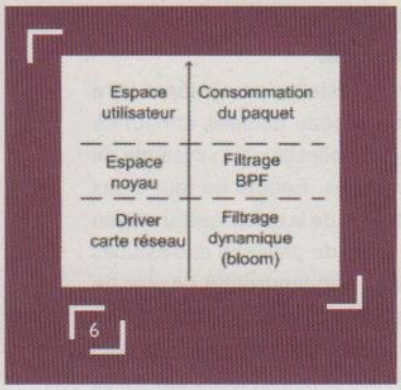
Le principal logiciel libre utilisé pour envoyer des données Netflow vers un collecteur, s'appelle donc fprobe [7] (dépendant de `libpcap`). Sous Linux, on lui préférera l'utilisation de fprobe-ulog (fork de fprobe) et `libipulog` qui sont plus performants en environnement Netfilter grâce à l'utilisation de la cible ULOG d'IPtables. Cette cible IPtables permet de rediriger les paquets réceptionnés par les deux cartes réseau (*bridgés* pour l'occasion avec la commande `brctl`) et de les envoyer au processus fprobe-ulog qui enverra les paquets Netflow vers un collecteur (ici 192.168.3.4 :2008) en UDP. Voici un exemple de configuration :

```
insmod ipt_ULOG
iptables -A INPUT -j ULOG
iptables -A OUTPUT -j ULOG
iptables -A FORWARD -j ULOG
fprobe-ulog 192.168.3.4:2008
```

L'auteur note l'existence de l'outil softflowd [8] présenté à la *BlackHat Las Vegas 2008*. Cet outil est compatible avec Netflow v9, mais est aujourd'hui immature.

Afin d'obtenir une solution complète, il reste à sélectionner de manière optimale les flux transitant dans le tuyau pour une analyse des trames réseau circulant à un instant « T ».

Pour cela, il y a les *blooms* [9]. Ils se situent en amont de BPF (*Berkeley Packet Filter*). Grâce à eux, plus de limite à un unique filtre. Ils sont en outre modifiables dynamiquement, ce qui n'est pas le cas de tcpdump, qu'il faut stopper puis relancer à chaque



6

fois avec un autre filtre BPF. Enfin, les blooms agissent au plus bas niveau dans le système, fournissant de meilleures performances comme l'illustre la figure 6.

Les blooms sont pilotables en userland via `/proc/net/ethX/enable`, `/proc/net/ethX/reset` et `/proc/net/ethX/rules`. `Enable` et `reset` sont utilisés respectivement pour activer le filtrage dynamique et le désactiver en positionnant la valeur à 1.

La commande suivante est utilisée pour ajouter un filtre :

```
echo "+ip=192.168.0.1,port=80" > /proc/net/eth1/rules
```

Et pour enlever un filtre :

```
echo "-proto=tcp" > /proc/net/eth1/rules
```

Pour l'heure, il ne s'agit que de la capture des paquets et de l'exportation vers un collecteur Netflow grâce à fprobe-ulog. Il est ensuite de votre responsabilité d'analyser les données capturées et de prendre des décisions.

Libre à chacun de coupler ensuite cette configuration à d'autres outils libres comme le système de détection d'intrusions Snort. Il est possible d'imaginer l'enregistrement des trames répondant à un pattern précis (voir le paragraphe « La Machine à remonter le temps ») en fonction d'une alerte remontée pendant par exemple 2 minutes.

L'analyse de patterns réseau n'est pas toujours efficace. La notion de « faux-positif » est largement connue dans le monde de la sécurité et il est prouvé que, dans bon nombre de situations, elle est dépendante d'un jugement erroné. Personne n'est à l'abri d'une mauvaise interprétation du trafic. Quoi qu'il en soit, il faut à présent analyser les données collectées.

3.4 Le network forensics est à la mode

Les entreprises possédant un réseau important rencontrent fréquemment des problèmes réseau ou de sécurité difficiles à dépanner. En l'absence de surveillance réseau, il ne peut exister le moindre indicateur pouvant aider à la résolution de problèmes. Les recherches peuvent alors durer plusieurs jours, plusieurs semaines, voire, dans le pire des cas, demeurer vaines. C'est le cas par exemple d'une tempête de *broadcast* qui inonde temporairement le réseau. Le monitoring du réseau apporte un niveau élevé d'identification et de compréhension des problèmes, ainsi qu'une réponse plus rapide à un incident. Il apporte également des solutions spécifiques à l'identification de problèmes sécurité, par exemple une violation d'accès réseau ou système, un problème de conformité normative, un détournement de sous-réseau appartenant à un AS BGP tierce.

Si le monitoring ne résout pas tout, il facilite l'interprétation et fournit des pistes. La résolution effective du problème, la compréhension de ses conséquences relèvent de l'interprétation humaine dans la plupart des cas. Reste que pour parvenir à ce stade, il faut savoir exactement ce qu'il se passe et où cela s'est passé sur le réseau. C'est là que deux visions du monde s'opposent : une pauvre et une riche. La pauvre, c'est celle de l'artisan réseau un peu passéiste, qui ne peut voir plus loin que le bout de son analyseur de trames ethereal ou wireshark, celle du stagiaire qui parcourt tous les étages et commutateurs de l'entreprise pour localiser une machine un peu trop bavarde. Et puis, il y a l'approche moderne, celle qui consiste à sniffer à partir de n'importe quel endroit du réseau, à n'importe quel moment, depuis une unique console et, grâce aux TAP, qui offre la possibilité de générer sur le champ rapports, graphiques et diagrammes à partir d'événements corrélés à partir de plusieurs points du réseau.

3.5 La machine à remonter le temps

Et puis, il y a la vision idyllique, celle des rois de l'analyse rétrospective (RNA – *Retrospective Network Analysis* [10]). Un luxe réservé aux administrateurs réseau disposant d'un d'espace disque plus que confortable et qui peuvent stocker les paquets circulant sur le réseau. Dès qu'un problème est identifié (hausse soudaine de l'utilisation de CPU des équipements réseau, plaintes des utilisateurs,...), il suffit de rechercher les paquets ayant circulés au moment précis de l'accident, puis de remonter dans le temps jusqu'à analyse complète du contenu de niveau 5-7.

Tout cela est possible de deux manières :

- en enregistrant la totalité du trafic ;
- en déclenchant l'enregistrement des paquets sur la détection d'une alerte.

Dans le premier cas, un vaste espace de stockage est nécessaire, qui offre une visibilité maximale : avant, pendant et après un événement notoire.

Dans le second cas, les contraintes de stockage sont minimes, mais la visibilité réduite, car l'enregistrement des paquets ne débute que lorsque survient un événement précis, telle la présence d'un label MPLS inconnu. Ensuite, libre à chacun de décider pendant combien de temps il est nécessaire d'enregistrer les paquets.

À titre d'information, Network Instruments commercialise un boîtier d'enregistrer en boucle jusqu'à 288 TeraOctets de données. Autrement dit, la possibilité de remonter sur plusieurs jours voire plusieurs semaines de trafic dans le temps. L'export des flux collectés est aussi possible vers un SAN.

Il faut toutefois faire attention à un détail. S'il existe de nombreux outils d'analyses dites « expertes », capables d'identifier des anomalies en regroupant plusieurs trames, ils ne sont jamais fiables à 100%.

3.6 Aucun outil d'analyse experte n'est parfait

D'expérience, il peut arriver que certains analyseurs de trames soient en proie à des faux positifs lors de l'identification d'une anomalie sur le réseau. Prenons pour exemple le cas des retransmissions TCP. Il arrive que certains analyseurs interprètent mal la fermeture *graceful* (pas de flag RST) d'une session TCP. Cette fermeture de session s'effectue avec quatre paquets : FIN-ACK, ACK, FIN-ACK, ACK comme l'illustre la figure 7.

Il peut arriver que certaines applications ferment la connexion d'une autre manière. Par exemple, avec cette séquence : FIN-ACK, FIN-ACK, ACK, FIN-ACK. Comme l'illustre la figure 8, il y a un FIN-ACK de trop alors qu'un ACK aurait normalement était attendu. Un sniffer interprétant mal cette fermeture de session pense que le quatrième paquet (le dernier FIN-ACK) est une retransmission de paquet, car le numéro de séquence est identique au deuxième paquet et contient les mêmes flags (FIN-ACK). En conséquence, le compteur du nombre de retransmissions TCP est incrémenté bien que la connexion soit fermée par l'applicatif lequel est mal codé pour le coup ;-)

En cas de doute, n'hésitez pas à enregistrer le trafic suspect dans un fichier (au format PCAP par exemple) afin de l'ouvrir dans un autre analyseur de trames.

Il est important de garder à l'esprit que pour analyser correctement le trafic d'une manière globale, il est nécessaire de déployer plusieurs sondes aux emplacements-clés du réseau ou l'art du « diviser pour mieux régner ».

7

Source Address	Dest Address	Summary
[64.233.167.104	[192.168.11.8]	TCP: D=4967 S=80 FIN ACK=453115230 SEQ=1875941380 LEN=0 WIN=8704
[192.168.11.8]	[64.233.167.104	TCP: D=80 S=4967 ACK=1875941381 SEQ=453115230 LEN=0 WIN=65535
[192.168.11.8]	[64.233.167.104	TCP: D=80 S=4967 FIN ACK=1875941381 SEQ=453115230 LEN=0 WIN=65535
[64.233.167.104	[192.168.11.8]	TCP: D=4967 S=80 ACK=453115231 SEQ=1875941381 LEN=0 WIN=8704

8

Source Address	Dest Address	Summary
Client	Server	TCP: D=443 S=1432 FIN ACK=3450559799 SEQ=4209927829 LEN=0 WIN=17047
Server	Client	TCP: D=1432 S=443 FIN ACK=4209927829 SEQ=3450559799 LEN=0 WIN=5485
Client	Server	TCP: D=443 S=1432 ACK=3450559800 SEQ=4209927830 LEN=0 WIN=17047
Server	Client	TCP: D=1432 S=443 FIN ACK=4209927830 SEQ=3450559799 LEN=0 WIN=5485

4. Modifications de l'écosystème

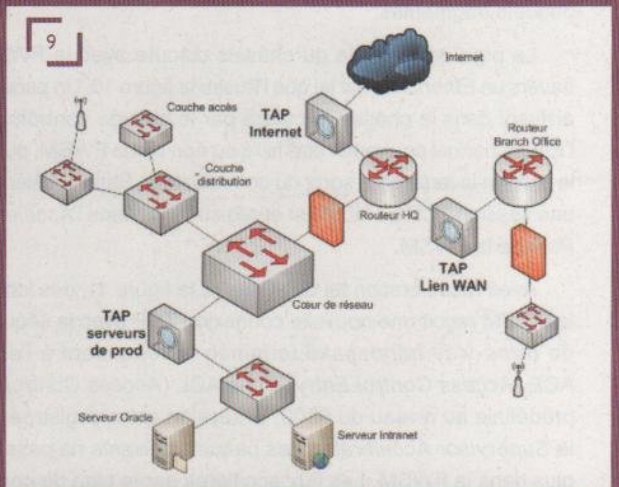
4.1 Placement des sondes

Considérant le design des architectures réseau d'entreprises d'aujourd'hui qui sont dans la plupart des cas quasi identiques, il est judicieux de placer les sondes de préférence aux endroits-clés du réseau afin d'en tirer le meilleur résultat possible.

Il n'existe pas de design miracle répondant à tous les scénarii, mais ici un cas d'entreprise assez générique est pris pour exemple (voir schéma 9). Il est possible de tirer un excellent aperçu des flux applicatifs et transactionnels générés par les utilisateurs près des serveurs de production. Si ces derniers sont aussi habitués à travailler sur des applications passant par un lien WAN, il sera utile d'ajouter des sondes près de ces connexions. Si la menace d'une intrusion est forte sur ces liens WAN, cet emplacement est absolument stratégique.

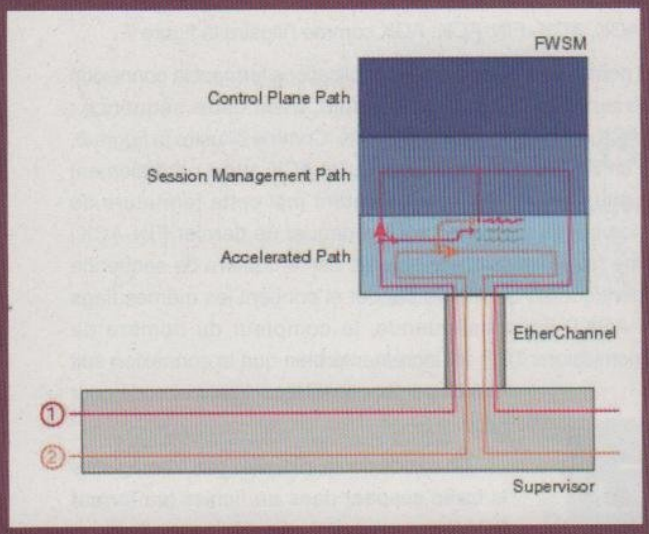
Il n'est, par exemple, pas toujours possible de mettre en place physiquement des TAP. Parfois, le réseau n'est pas adapté de par sa conception : P2P, liens chiffrés au niveau de la couche 3 (IPSEC ou SSL) ou même en couche 2 (802.1AE). Dans ce cas, redéfinissez plus précisément vos besoins ou optez pour un autre emplacement au sein de votre infrastructure. Les routeurs et commutateurs ne sont pas les seuls composants d'un réseau. Il y a aussi les équipements de sécurité comme les pare-feu.

9

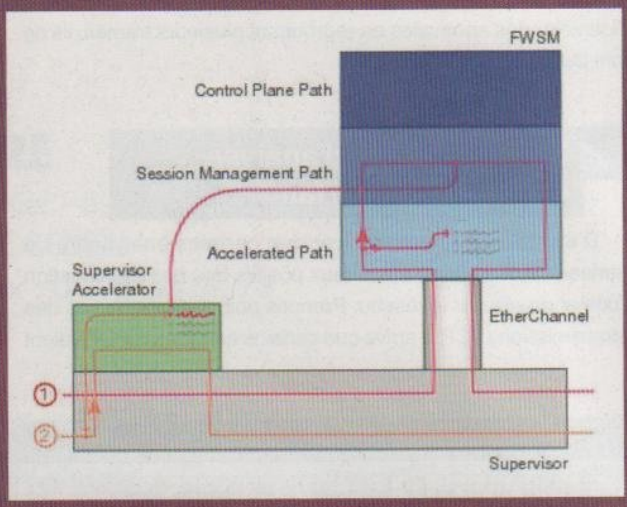


4.2 Optimisation des pare-feu

Afin de supporter la charge d'une ou plusieurs dizaines de gigabits par seconde, les constructeurs doivent faire évoluer



10 *Sans accélération*



11 *Avec accélération*

les pare-feu afin qu'ils puissent gérer ces débits. C'est le cas du module FWSM qui est une carte de services optionnelle dans les châssis Cisco 6500 et 7600. Elle effectue une fonction de filtre de paquets à l'intérieur du châssis. Un « hack » **[11]** dont le nom marketing est *Trusted Flow Acceleration* a été réalisé afin de supporter un maximum de débit, en particulier sur les flux FTP et de sauvegardes. Certains flux ne peuvent bénéficier de l'accélération comme le multicast ou les paquets fragmentés.

Le plan de contrôle du châssis discute avec la FWSM à travers un *EtherChannel* tel que l'illustre la figure 10. Un paquet (1) arrivant dans le châssis circulera par le plan de contrôle, puis l'EtherChannel pour enfin être filtré ou non par la FWSM, puis fait le chemin inverse pour sortir du commutateur. Sans accélération, une session TCP ou UDP est enregistrée (2) dans l'*Accelerated Path* de la FWSM.

Avec l'accélération tel que l'illustre la figure 11, dès lors que la FWSM reçoit une nouvelle connexion TCP avec la séquence de *three-way handshake* terminée et répondant à l'entrée ACE (*Access Control Entry*) d'une ACL (*Access Control List*) prédéfinie au niveau du 6500, la session est enregistrée dans le *Supervisor Accelerator.* Les paquets suivants ne passeront plus dans la FWSM. Les flux accélérés par le plan de contrôle sont visibles avec la commande `show mls netflow ip sw-installed` depuis la CLI du 6500. Pour une connexion UDP, l'accélération est effective après que la FWSM a reçu le deuxième paquet. Pour les flux nécessitant une inspection protocolaire, les paquets du canal de contrôle (typiquement une ouverture de session et la commande PORT de FTP) ne sont pas optimisés et remontent jusqu'au *control plane path*. En revanche, les paquets du canal de flux (exemple d'un transfert de fichiers en FTP) sont accélérés. L'explication technique derrière cette technique vaudou vient du fait qu'habituellement le trafic allant être filtré a pour adresse MAC de destination l'adresse de la FWSM. Quand l'accélération par le plan de contrôle est active, elle voit la connexion et s'approprie temporairement l'adresse MAC de la FWSM. Le flux ayant déjà été filtré une première fois par la FWSM, le reste des paquets n'est pas considéré malicieux.

Il est important de garder à l'esprit que les flux NATés ou nécessitant une réécriture des numéros de séquences TCP feront toujours chuter les performances globales.

Un lien réseau multigigabit très utilisé sera générateur de bien plus de messages de *logs* qu'un lien à 100 Mb/s. Il est nécessaire de s'adapter face à cette situation tout en ayant conscience que Syslog n'est plus du tout adapté pour ce type de trafic.

4.3 Les logs dans un réseau à très haut débit

Un pare-feu, en particulier le Cisco ASA5580 (cible les très grandes entreprises et datacenters) externalise en partie ses logs au format Syslog. Ce dernier n'étant déjà pas très fiable sur des liens « bas débit », peu importe le protocole utilisé pour le transport des logs que ce soit en UDP ou TCP. Il était nécessaire de trouver une solution plus efficace. L'astuce consiste donc à s'appuyer sur NETFLOW version 9 pour les événements de connexions.

Le tableau 1 décrit la liste des messages SYSLOG possédant un équivalent NETFLOW.

ID Syslog	Description
106100	Une ACL vient de matcher un flux (qu'il soit autorisé ou interdit)
106015	Un flux TCP a été interdit car le premier paquet ne contenait pas le flag SYN
106023	Un flux vient d'être interdit par une ACL attachée à une interface
302013, 302015, 302017, 302020	Création de sessions TCP, UDP, GRE, ICMP
302014, 302016, 302018, 302021	Suppression de sessions TCP, UDP, GRE, ICMP
313001	Un paquet ICMP à destination du pare-feu vient d'être bloqué
313008	Un paquet ICMPv6 à destination du pare-feu vient d'être bloqué
710003	Un paquet de management (TELNET, SSH, SNMP, ...) à destination du pare-feu vient d'être bloqué

Tableau 1

La configuration est très explicite. La première ligne exporte les messages du tableau précédent vers le port 2008 la machine 192.168.3.4 qui est accessible en sortant depuis l'interface *inside*. La seconde ligne indique au processus SYSLOG de désactiver l'envoi des messages qui sont désormais envoyés via NETFLOW :

```
pello(config)# flow-export destination inside 192.168.3.4 2008
pello(config)# logging flow-export syslogs disable
```

Maintenant que votre architecture réseau est surveillée de bout en bout, il peut venir à l'idée de l'administrateur de tester la réaction du réseau et de ses applications lorsque survient une surcharge ou une attaque. Libre au lecteur de soumettre son installation à très haut débit à des scripts de génération de flux DNS, HTTP ou autres services (Voir *MISC* n°37).

Néanmoins, il est vain de démarrer ce genre d'essais sans avoir pleinement connaissance des protocoles et applications impliquées dans de telles procédures de tests.

Expédier des montagnes de paquets sans rime ni raison ne prouvera rien, n'invalidera rien. Il faut, à chaque instant, avoir conscience de ce que l'on fait et des objectifs que l'on souhaite atteindre.

Conclusion

Le réseau évolue. Le passage, même partiel en 10 GbE est un nouveau défi à affronter.

Avec des cartes dix fois plus performantes, le réseau devient théoriquement dix fois plus vulnérable aux dénis de services. Il faut en outre s'assurer que les systèmes de détection d'intrusions (pare-feu, IDS, VPN, proxy,...) soient correctement dimensionnés.

Du côté des journaux de connexions, plus de trafic implique plus de logs et donc plus de stockage.

Le challenge dans les prochaines années ne sera pas de savoir s'il est possible de garantir un flux de données à 10, 40 voir 100 gbps, mais de trouver un moyen pour faciliter l'analyse et la résolution de problèmes, accrus par une volumétrie de plus en plus astronomique et d'origines de plus en plus variées (data, VoIP, Communications Unifiées, Web2.0,...).

Références

[1] http://www.endace.com/

[2] http://www.myri.com/scs/download-Myri10GE.html

[3] http://www.wireshark.org

[4] http://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9.html

[5] http://www.cisco.com/en/US/products/hw/commutateures/ps708/products_tech_note09186a008015c612.shtml

[6] http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/ht_rawip.html

[7] http://fprobe.sourceforge.net/

[8] http://www.mindrot.org/projects/softflowd/

[9] http://luca.ntop.org/Blooms.pdf

[10] http://www.networkinstruments.com/assets/pdf/rna_wp.pdf

[11] http://www.cisco.com/en/US/prod/collateral/modules/ps2706/product_bulletin_c25-478751.html

Cédric Llorens & Denis Valois
cedric.llorens@wanadoo.fr, denis.valois@laposte.net

LES NOUVELLES SONDES DE SÉCURITÉ DANS LES RÉSEAUX MULTISERVICES

mots clés : ***réseau / sécurité / routage / MPLS / IGP / BGP / MP-BGP***

Nous présentons dans cet article de nouvelles sondes mises en œuvre au sein des cœurs de réseaux afin d'assurer la sécurité du réseau et de ses services.

1. Les problématiques de contrôle du routage et du trafic pour les réseaux multiservices

Les réseaux multiservices ont pour vocation d'offrir une palette de services réseau sur une même architecture physique. L'accroissement des différents services offerts mettent en exergue deux problématiques portant sur le routage et sur le trafic réseau.

- Les protocoles de routage sont fondamentaux pour la sécurité (en termes de disponibilité) d'un réseau. Toute perturbation du routage peut entraîner des impacts majeurs pour le cœur de réseau (plus d'acheminement du trafic d'un point A à un point B), ainsi que pour les services qu'il offre (car aucun chemin réseau n'est connu pour acheminer le trafic). De plus, la plupart des ressources mémoire et processeur des équipements réseau sont utilisés pour le calcul du routage. Le contrôle/analyse/supervision du routage est donc fondamental pour assurer la sécurité d'un réseau.
- Les réseaux multiservices reposent généralement sur une architecture MPLS, permettant grâce à des extensions protocolaires, de créer de nombreux et nouveaux services. L'analyse du trafic est nécessaire pour protéger un service et requiert d'analyser le trafic MPLS ainsi que ses labels.

Nous aborderons dans un premier temps l'analyse du routage, puis celle de l'analyse du trafic avant de conclure.

2. Rappels sur les réseaux MPLS

2.1 Description générale

Une des problématiques récurrentes des réseaux est de faire transiter des données le plus rapidement et le plus sûrement possible. La disponibilité des services réseau est généralement couverte par une topologie redondante. Quant à l'intégrité de ces services, elle est généralement couverte par les protocoles réseau. Cependant, MPLS n'assure pas au sens fort la confidentialité, ni l'intégrité des données transportées.

Dans les réseaux IP, le routage des paquets s'effectue en fonction des adresses IP (*Internet Protocol*), ce qui nécessite de lire les en-têtes IP à chaque passage sur un nœud réseau.

Pour réduire ce temps de lecture, deux protocoles ont vu le jour afin d'améliorer le transit global par une commutation des paquets au niveau 2 et non plus 3, comme le fait IP.

Plutôt que de décider du routage des paquets dans le réseau à partir des adresses IP, le principe de commutation MPLS (*Multi Protocol Label Switching*) s'appuie sur des labels. La commutation de paquets se réalise donc sur ces labels et ne consulte plus les informations relatives au niveau 3 incluant les adresses IP. En d'autres termes, l'acheminement ou la commutation des paquets sont fondés sur les labels et non plus sur les adresses IP **[MPLS] [RFC3031]**.

Un réseau MPLS est composé de routeurs P (*Provider* : dédiés à la commutation), de routeurs PE (*Provider Edge* : dédiés à la création des MPLS/VPN BGP et à la connectivité avec les équipements localisés chez les clients) et de routeurs CE (*Customer Edge* : installés chez les clients et connectés aux routeurs PE) comme l'illustre la figure 1.

Même si l'amélioration des équipements hardware ne rend plus aussi nécessaire qu'auparavant la commutation au niveau 2 plutôt qu'au niveau 3, une architecture MPLS couplée à d'autres protocoles permet de créer de nouveaux services à valeur ajoutée (VPWS, VPLS, etc.).

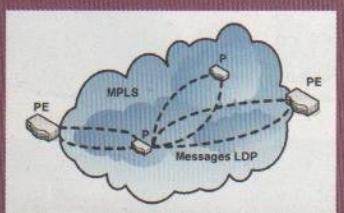
2.2 Le protocole LDP

LDP (*Label Data Protocol*) est un protocole de distribution de proche en proche défini par l'IETF. LDP fonctionne sur le modèle des protocoles de routage IP. Il utilise la table de routage générée IP pour construire la table de commutation MPLS. Les classes d'équivalence ou FEC (*Forwarding Equivalence Class*) sont découvertes automatiquement lors de l'exploration des tables de routage IP. Elles correspondent généralement à des préfixes de routage IP classiques **[LDP] [RFC5036]**.

Le protocole LDP permet donc d'échanger des messages entre les routeurs de cœur de réseau afin d'attribuer les labels pour chaque FEC (ou préfixe de routage IP) comme l'illustre la figure 2.

Quelle que soit la méthode de distribution choisie (distribution à la demande, distribution ordonnée, etc.), les chemins MPLS (ou *Label Switched Path*) pour chacune des FEC s'établissent.

1 *Réseau MPLS*



2 *Échange de messages LDP*

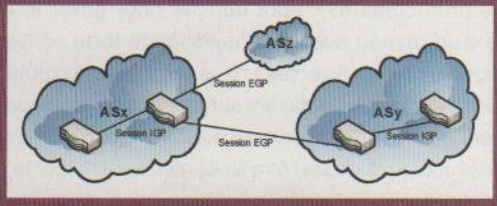
3. Les sondes d'analyse du routage

Une nouvelle famille de sondes de cœur de réseau, analysant le trafic de routage, permet d'assurer le contrôle et la stabilité des protocoles de routage s'exécutant dans le réseau. Après une brève introduction sur le routage, le protocole de routage IGP et BGP, nous détaillerons les caractéristiques principales de telles sondes dans des contextes de routage IGP et EGP.

3.1 Rappel des notions élémentaires du routage

D'une manière générale, tous les protocoles de routage ont pour objectif de maintenir les tables de routage du réseau dans un état intègre et cohérent. Pour y parvenir, les protocoles diffusent des informations de routage aux autres systèmes du réseau afin de transmettre les modifications des tables de routage. Ces protocoles réceptionnent en contrepartie les informations de routage d'autres systèmes du réseau afin de mettre à jour les tables de routage.

Le déploiement de réseaux IP de grande taille a rapidement nécessité la mise au point de protocoles de routage dynamique chargés de déterminer le plus efficacement possible la meilleure route pour atteindre une destination donnée. Il a aussi été nécessaire de découper le réseau en différents systèmes autonomes ou AS (*Autonomous System*), afin de réduire cette complexité. Les systèmes autonomes du cœur de réseau Internet sont gérés par les opérateurs de télécommunications comme l'illustre la figure 3.

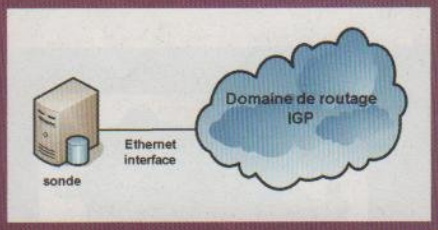


3 *Topologie de routage IGP & EGP*

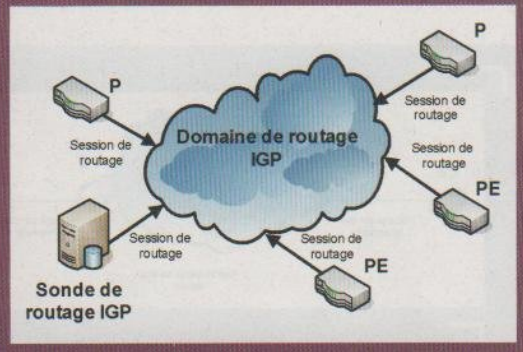
Ces considérations ont donné lieu à une classification des protocoles de routage dynamique en deux grandes familles : les protocoles IGP (*Interior Gateway Protocol*), qui échangent des informations d'accessibilité au sein d'un système autonome, et les protocoles EGP (*Exterior Gateway Protocol*), qui échangent des informations d'accessibilité entre systèmes autonomes.

3.2 Description générique de la sonde

Une sonde d'analyse de routage embarque généralement un système d'exploitation de type UNIX/Linux et se connecte à un domaine de routage par une simple interface Ethernet comme l'illustre la figure 4.



4 *Sonde d'analyse de routage*



5 *Emplacement d'une sonde de routage*

La sonde embarque aussi par défaut les couches logicielles suivantes :

- une couche logicielle émulant le protocole de routage choisi (ISIS, OSPF, BGP, MP-BGP, etc.) afin de se connecter à un domaine associé **[ZEBRA]**.
- une couche logicielle de base de données permettant de stocker tout l'historique des échanges de routage (repose sur une couche SQL : *Structured Query Language*).
- une couche logicielle d'accès et de présentation des données, des analyses, des audits, etc. (repose sur une couche HTTP).

3.3 L'analyse du routage IGP

3.3.1 Présentation

Les protocoles IGP sont conçus pour gérer le routage interne d'un réseau avec des objectifs de forte convergence des nouvelles routes injectées dans les tables de routage. Les décisions de routage s'appuient sur une unique métrique afin de favoriser la fonction de convergence. Le nombre d'entrée dans les tables de routage doit aussi être limité afin de renforcer la fonction de convergence.

Les protocoles parmi les plus utilisés de nos jours sont les suivants :

- OSPF (*Open Shortest Path First*). Protocole de routage à état des liens fondé sur le calcul des chemins les plus courts et sur une architecture hiérarchique constituée de zones OSPF **[RFC2328]**.
- IS-IS (*Intermediate System to Intermediate Systems*). Protocole de routage à état des liens fondé sur le calcul des chemins les plus courts et sur une architecture hiérarchique constituée de domaines IS-IS **[RFC0995]**.

D'autres protocoles, tels RIP (*Routing Information Protocol*) ou EIGRP (*Enhanced Interior Gateway Routing Protocol*) sont des protocoles de routage à vecteur de distance.

3.3.2 L'algorithme mis en œuvre

Le routage IGP repose généralement sur l'algorithme de Dijkstra. Il s'agit d'un algorithme permettant de trouver, à partir d'un sommet origine unique, le plus court chemin dans un graphe $G = (S, A)$ pondéré (S est l'ensemble des nœuds et A l'ensemble des arcs), où les arêtes ont des coûts positifs ou nuls. Il s'agit donc d'un algorithme à fixation d'étiquettes (*label setting algorithm*) traitant définitivement un sommet et son étiquette (ou distance) à chaque itération. Il exploite en outre la propriété que les sous-chemins de plus courts chemins sont de plus courts chemins.

Sachant que tout algorithme est lié à la fois à son temps d'exécution (complexité en temps), mais aussi à sa consommation mémoire (complexité en mémoire), toute perturbation sur l'algorithme de routage peut avoir des effets dévastateurs.

3.3.3 Les impacts du routage sur les ressources des équipements

Le temps processeur nécessaire pour le calcul des tables de routage par un équipement réseau peut être non négligeable. Par exemple, avec un graphe dense, l'algorithme de Dijkstra a une complexité en temps de l'ordre de $O(S^2)$. Dans le/la pire des cas/configurations possibles (pas de routage partiel, etc.) et si l'on modifie 10 préfixes par seconde dans un graphe comportant 900 sommets, le temps nécessaire pour mettre à jour les tables de routage nécessite de l'ordre de plusieurs millions d'opérations par seconde.

Si un équipement réseau consomme trop de ressources pour le calcul des tables de routage, il impacte le routage proprement

dit et, par conséquent, le trafic réseau **[Llorens, Valois]**. Il est donc fondamental de surveiller le trafic de routage.

3.3.4 L'emplacement de la sonde d'analyse

La spécification IGP permet à un nœud/sonde dans un domaine de routage donné de connaître la topologie complète comme l'illustre la figure 5 **[RouteExplorer]**.

Par l'écoute passive de tous les messages de routage échangés, la sonde va permettre d'offrir de nombreux bénéfices comme nous décrivons par la suite.

3.4 L'analyse du routage EGP

Les protocoles EGP sont conçus pour gérer le routage externe d'un réseau avec des objectifs de faible convergence des nouvelles routes injectées dans les tables de routage. Les décisions de routage s'appuient sur un ensemble de critères et le nombre d'entrée dans les tables de routage est généralement important (de l'ordre de 280.000 routes dans un contexte Internet, jusqu'au million de routes dans un contexte VPN BGP/MPLS).

3.4.1 Présentation

Le protocole BGP s'appuie sur la couche TCP (port 179) et fait partie de la famille des protocoles EGP. Le mode de fonctionnement du protocole BGP entre deux routeurs consiste à établir une connexion TCP et à échanger d'une manière dynamique les annonces de routes **[RFC1774]**.

L'algorithme mis en œuvre

Le routage BGP repose généralement sur l'algorithme de Bellman-Ford distribué. Il s'agit d'un algorithme réparti et autostabilisant, dans lequel chaque sommet x maintient une table des distances donnant le voisin z à utiliser pour joindre la destination y. On le note $D^x(y,z)$.

L'algorithme se fonde sur le calcul de l'invariant suivant pour chaque sommet et pour chacune de ses destinations :

$D^x(y,z) = c(x,y) + \min_w D^z(y,w)$

où w désigne les voisins de z.

L'algorithme exploite la propriété que les sous-chemins de plus courts chemins sont des plus courts chemins. Lorsqu'un nœud calcule un nouveau coût minimal pour une destination lors d'une mise à jour de routage provenant de ses voisins ou lorsque le coût d'une de ses adjacences a changé, il informe ses voisins de cette nouvelle valeur. Il s'agit donc d'un algorithme à correction d'étiquettes (*label correcting algorithm*) pouvant affiner à chaque itération l'étiquette (ou distance) de chaque sommet.

Sachant que tout algorithme est lié à la fois à son temps d'exécution (complexité en temps), mais aussi à sa consommation mémoire (complexité en mémoire), toute perturbation sur l'algorithme de routage peut avoir des effets dévastateurs.

3.4.2 Les impacts du routage sur les ressources des équipements

Le temps processeur nécessaire pour le calcul des tables de routage par un équipement réseau peut être non négligeable. Par exemple, si l'on considère qu'un équipement réseau a de l'ordre de 20 voisins en moyenne et que chaque voisin envoie une mise à jour de routage modifiant 5 000 préfixes par seconde, il faut de l'ordre de plusieurs millions d'opérations par seconde dans le pire des cas pour mettre à jour les tables de routage

Si un équipement réseau consomme trop de ressources pour le calcul des tables de routage, il impacte le routage proprement dit et par conséquent le trafic réseau **[Llorens, Valois]**. Il est donc fondamental de surveiller le trafic de routage.

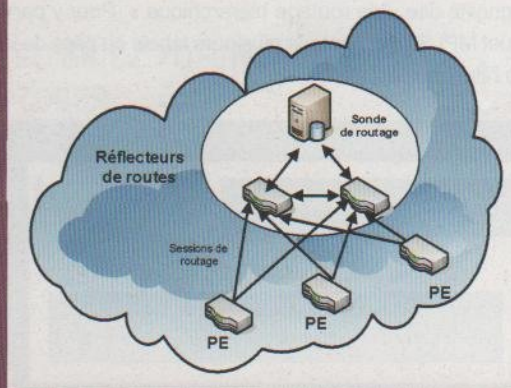
3.4.3 L'emplacement de la sonde d'analyse

La spécification initiale de BGP suppose qu'un graphe complet (modèle « complet ») de sessions iBGP soit configuré au sein du système autonome pour distribuer les routes interdomaines.

Par conséquent, il doit y avoir $n(n-1)/2$ sessions iBGP au sein d'un système autonome si n est le nombre de routeurs. La raison à cela est que les sessions iBGP ne redistribuent par les routes apprises en iBGP, afin d'éviter les phénomènes de bouclage. Par exemple, pour un réseau contenant 100 routeurs, il serait nécessaire de configurer de l'ordre de 5 000 sessions iBGP au total dans les configurations des routeurs.

Le modèle réflecteur de routes a été proposé pour réduire le nombre de configurations des sessions iBGP. Sachant que le sous-graphe associé aux réflecteurs de routes doit être complet, il doit y avoir $n(n-1)/2$ sessions iBGP entre les réflecteurs de routes.

Cependant, le nombre de réflecteurs de routes nécessaires est, par architecture, très inférieur comparé au nombre de routeurs dans le système autonome. La sonde se localisera donc dans le nuage des réflecteurs de routes comme l'illustre la figure 6.



6 *Emplacement de la sonde EGP*

Par l'écoute passive de tous les messages de routage échangés, la sonde va permettre d'offrir de nombreux services d'analyse comme nous décrivons par la suite.

3.5 Les bénéfices de mise en œuvre

Les bénéfices de la mise en œuvre d'une telle sonde sont les suivants (de nombreuses captures d'écran, exemples d'audit, etc. peuvent être consultés sur le site **[Route Explorer]**) :

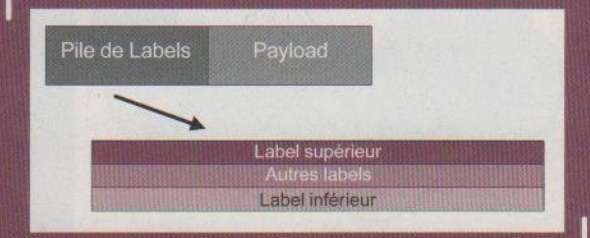
- Visualisation en temps réel des topologies de routage. Différentes topologies de routage peuvent être prises en compte telles qu'IGP, EGP, MP-BGP, etc.
- D'enregistrer tous les échanges de routes et de pouvoir rejouer à la demande ces échanges pour analyser plus finement un problème.
- D'analyser en temps réel les échanges de routes et de lever des alertes si l'on détecte par exemple des instabilités de routes ou des échanges de routes provoqués par des erreurs de configuration, etc.
- D'auditer en temps réel les topologies de routage et de lever des alertes si des propriétés topologiques sont violées (le graphe doit être connecté, il ne doit pas avoir de points d'articulation, etc.).
- Permet d'envoyer à un système de corrélation les événements réseau afin de détecter des attaques potentielles.
- D'anticiper l'évolution du réseau et la montée en charge de nouveaux services et clients comme le nombre de routes routées, la consommation des ressources des équipements liée au routage, la stabilité et le temps de convergence des algorithmes de routage, etc.
- Une seule sonde permet de contrôler plusieurs domaines de routage réduisant ainsi les investissements.
- La sonde est passive en termes de routage (même si elle a une session active) et ne peut pas par défaut perturber le trafic de routage. Seuls des actes de malveillance et d'ajout de couches logicielles peuvent rendre la sonde attaquante.

4. Les sondes d'analyse du trafic MPLS

Une nouvelle famille de sondes de cœur de réseau, analysant le trafic MPLS, permet de contrôler le trafic de données transporté sur un réseau multiservice. Après une brève introduction sur le réseau MPLS, le protocole de signalisation LDP et le routage hiérarchique, nous détaillerons les caractéristiques principales de telles sondes.

4.1 Le routage hiérarchique dans un réseau MPLS

Au sein d'un réseau MPLS, les paquets IP transitent dans un tunnel ou LSP (*Label Switch Path*), MPLS généralise cette fonctionnalité dite « de routage hiérarchique ». Pour y parvenir, un paquet MPLS peut contenir plusieurs labels ou piles de labels comme l'illustre la figure 7.



7 *Pile de labels*

Le label de « tête de pile » est utilisé pour prendre les décisions de routage au sein de réseau MPLS. Les labels suivants sont alors utilisés lorsque ce label a été enlevé. Un équipement du réseau MPLS peut modifier la valeur du premier label, modifier la valeur du premier label et empiler un autre label ou dépiler le premier label.

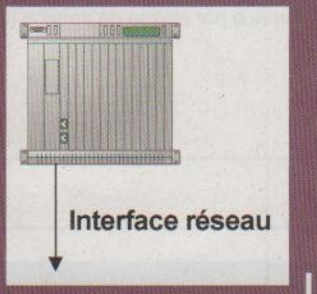
L'objectif de ce routage hiérarchique est d'offrir une très grande souplesse pour construire de nouveaux services où un deuxième niveau de label permettra d'adresser ces services. D'autres applications sont aussi possibles comme pour agréger du trafic au cœur du réseau, mettre en place deux plans de routage différents ou émuler un circuit au-dessus de MPLS, etc.

4.2 Description générique de la sonde d'analyse

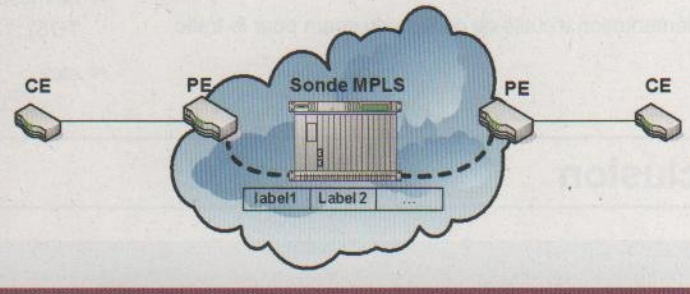
Une sonde d'analyse de trafic est un équipement réseau composé d'une baie (7U à 14U) incluant des cartes dédiées comme l'illustre la figure 8.

La baie embarque donc des logiciels spécialisés sur des cartes dédiées telles que :

- une carte dédiée pour l'analyse des dénis de services ;
- une carte dédiée pour la détection d'intrusion ;
- une carte dédiée pour l'analyse en profondeur du trafic ;
- etc.



8 *Sonde d'analyse de trafic MPLS*



9 *Réseau MPLS*

4.3 L'emplacement de la sonde

La sonde MPLS se situe donc dans le cœur de réseau et suivant le trafic que l'on souhaite contrôler, le chemin MPLS (*Label Switched Path*) passe par cette sonde comme l'illustre la figure 9.

Une sonde d'analyse MPLS doit donc pouvoir analyser cette pile de labels pour contrôler les services réseau associés tels que :

- Un niveau de label pour un accès IP standard.
- Deux niveaux de labels pour un accès VPN BGP/MPLS, le premier niveau de label pour le nuage interne MPLS et le deuxième pour le VPN **[RFC3031]**.
- Deux niveaux de labels pour un accès ATMoMPLS, le premier niveau de label pour le nuage interne MPLS et le deuxième pour le circuit ATM **[RFC4717]**.
- Deux niveaux de labels pour un accès EoMPLS, le premier niveau de label pour le nuage interne MPLS et le deuxième pour le circuit Ethernet **[RFC4448]**.
- Etc.

4.4 Les bénéfices de mise en œuvre d'une telle sonde

Les bénéfices de la mise en œuvre d'une telle sonde sont les suivants (de nombreuses captures d'écran, exemples d'audit, etc. peuvent être consultés sur le site **[BladeCenter]**) :

- de limiter les coûts d'investissement et de gestion opérationnelle par la mise en œuvre d'un système central en comparaison avec des systèmes installés par client ;
- d'augmenter facilement les capacités de performance si nécessaire ;
- de mettre en œuvre facilement des services à valeur ajoutée comme :
  - l'analyse du trafic voix ;

- l'implémentation de filtrage virtuel réseau et applicatif par client ;
- l'implémentation d'outils de gestion du spam pour le trafic smtp ;
- etc.

⇨ de mesurer la qualité de service par classe de service (champ TOS) ;

⇨ etc.

Conclusion

Sachant que les protocoles réseau évoluent et que les techniques de *tunneling* s'étoffent, de nouveaux outils d'analyse sont nécessaires pour assurer la sécurité des services.

Dans ce contexte, l'explosion de l'utilisation des protocoles de routage est à noter et représente par ailleurs un risque majeur pour le réseau en cas d'instabilité de routage, de consommation mémoire et processeur excessives pour le calcul des routes ou d'arbres de diffusion *multicast*, d'erreurs de configuration des topologies de routage, etc.

De nouvelles sondes apparaissent donc pour maîtriser cette évolution technologique et maintenir une visibilité sur la sécurité.

Références

[BladeCenter] sonde d'analyse du trafic, **http://www-03.ibm.com/servers/eserver/telecom/bcht.html**

[Llorens, Valois] LLORENS ((C.), LEVIER (L.), VALOIS (D.), *Tableaux de bord de la sécurité réseau*, 2ème édition, Eyrolles, 560 pages, ISBN 2-212-11973-9, septembre 2006.

[MPLS] BONNIN (Jean-marie), « Le protocole MPLS », *Techniques de L'ingénieur*, TE7540, **http://www.techniques-ingenieur.fr**

[LDP] BONNIN (Jean-marie), « Le protocole LDP », *Techniques de L'ingénieur*, TE7535, http://www.techniques-ingenieur.fr

[RFC0995] *International Organization for Standardization, End System to Intermediate System Routing Exchange Protocol for use in conjunction with ISO 8473*, avril 1986, **http://www.rfc-editor.org/rfcsearch.html**

[RFC1774] TRAINA (P.), « *BGP-4 Protocol Analysis* », mars 1995, **http://www.rfc-editor.org/rfcsearch.html**

[RFC2328] MOY (J.), « *OSPF Version 2* », avril 1998, **http://www.rfc-editor.org/rfcsearch.html**

[RFC3031] ROSEN (E.), VISWANATHAN (A.), CALLON (R.), « *Multiprotocol Label Switching Architecture* », janvier 2001, **http://www.rfc-editor.org/rfcsearch.html**

[RFC4448] MARTINI (L.), Ed., ROSEN (E.), EL-AAWAR (N.), HERON (G.), « *Encapsulation Methods for Transport of Ethernet over MPLS Networks* », avril 2006, **http://www.rfc-editor.org/rfcsearch.html**

[RFC4717] MARTINI (L.), JAYAKUMAR (J.), BOCCI (M.), EL-AAWAR (N.), BRAYLEY (J.), KOLEYNI (G.), « *Encapsulation Methods for Transport of Asynchronous Transfer Mode (ATM) over MPLS Networks* », décembre 2006, **http://www.rfc-editor.org/rfcsearch.html**

[RFC5036] ANDERSSON (L.), MINEI (I.), THOMAS (B.), « LDP specifications », octobre 2007, **http://www.rfc-editor.org/rfcsearch.html**

[Route Explorer] sonde d'analyse de routage, **http://www.packetdesign.com/**

[ZEBRA] *Free routing software distributed under GNU General Public License*, **http://www.zebra.org/**

Abréviations

ATM : *Asynchronous Transfer Mode*
BGP : *Border Gateway Protocol*
CE : *Customer Edge*
EGP : *Exterior Gateway Protocol*
IGP : *Interior Gateway Protocol*
IOS : *Internetworking Operating System*
IP : *Internet Protocol*
ISO : *International Standard Organisation*
IETF : *Internet Engineering Task Force*
IS_IS : *Intermediate System to Intermediate Systems*
LAN : *Local Area Network*
LDP : *Label Distribution Protocol*
LSP : *Label Switch Path*
LTD : *Label Tag Distribution*
MP-BGP : *Multi Protocol Border Gateway Protocol*
MPLS : *Multi Protocol Label Switching*
P : *Provider*
PE : *Provide Edge*
RFC : *Request For Comments*
RR : *Route Reflector*
VRF : *Virtual Routing Forwarding*
VPN : *Virtual Private Network*

Denis Valois & Cédric Llorens
denis.valois@laposte.net, cedric.llorens@wanadoo.fr

UNE NOUVELLE APPROCHE DANS L'ANALYSE DES CONFIGURATIONS

mots clés : *réseau / sécurité / configuration / automate*

Nous présentons dans cet article une nouvelle approche pour réaliser des contrôles de configuration avancée. L'outil HAWK, présenté dans cet article, sert à réaliser cette nouvelle approche.

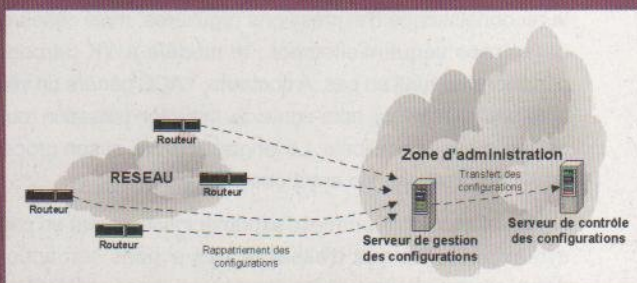
1. La problématique sécurité des configurations

Les réseaux multiservices comportent plusieurs dizaines de milliers d'équipements réseau représentant plusieurs millions de lignes de configurations.

Par exemple, si vous avez de l'ordre de 1000 équipements réseau dont chacun contient près de 10.000 lignes de configuration, votre cœur de réseau compte de l'ordre de 10 millions de lignes de configuration et de nombreuses questions se posent :

- Comment vérifier alors que les listes de filtrage contrôlant l'accès aux équipements sont définies et appliquées ?
- Comment vérifier que les communautés SNMP sont bien celles attendues et filtrées ?
- Comment s'assurer que les mots de passe sont définis et appliqués ?
- Comment définir une approche pragmatique et efficace permettant de tenir compte de la taille des configurations et des types de contrôle à réaliser ?

Pour y parvenir, il est alors désirable d'utiliser des outils bien ciblés afin de contrôler la conformité des configurations à la politique de sécurité. Bien que cette problématique soit ancienne, c'est assez récemment que sa complexité et son importance ont été identifiées **[Valois, Llorens] [Llorens] [Llorens, Valois]**. Dans ce contexte, nous nous limitons à la vérification de configuration « off-line » et nous supposons que les fichiers de configuration sont directement disponibles comme l'illustre la figure 1.

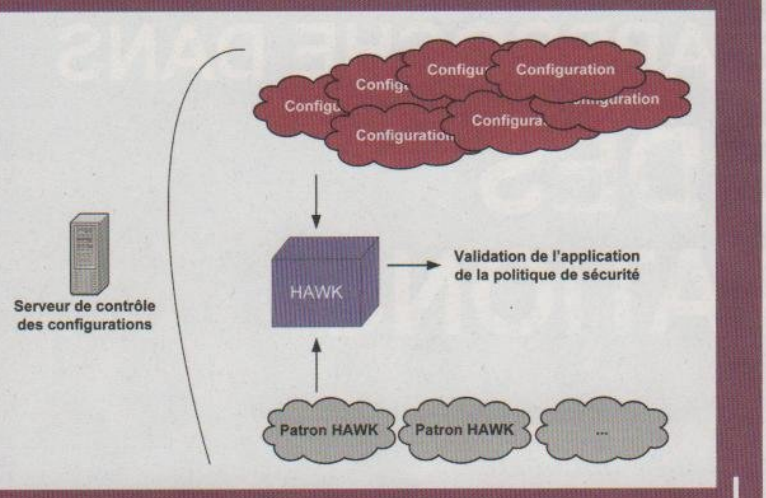


Contrôle des configurations en mode « off-line »

À partir d'une zone d'administration, on rapatrie les configurations des équipements réseau sur un serveur dédié. On les transfère ensuite vers un autre serveur spécialisé dans le contrôle « off-line » des configurations.

Historiquement, les approches suivantes ont permis d'apporter une première réponse à des questions portant sur les configurations :

- L'approche TRIPWIRE : *cette configuration a-t-elle été modifiée ?* Cette approche se base sur une comparaison littérale et se restreint au niveau lexical.



2 *Mise en œuvre de HAWK*

- L'approche ISS : *cette configuration comporte-t-elle une mauvaise configuration de sécurité?* Cette approche repose sur un ensemble de vulnérabilités connues, mais les tests sont souvent indépendants de tout contexte particulier.
- Notre approche : *cette configuration implémente-t-elle la politique voulue?* Cette vérification peut requérir une analyse de niveau sémantique, mais quelquefois une analyse de niveau syntaxique est suffisante.
- D'autres approches plus récentes qui offrent différentes types d'approches (vérification des configurations avant ou après une modification) **[Wandl, Opnet]**.

L'outil HAWK que nous présentons en détail par la suite est présent sur le serveur de contrôle et permet de vérifier l'application de la politique de sécurité sur l'ensemble du réseau à partir de patrons de sécurité comme l'illustre la figure 2.

2. HAWK, le langage et le processeur

La vérification de configuration demande fréquemment une analyse syntaxique, ainsi qu'une analyse sémantique. En revanche, les outils existants sont soit trop lourds, soit trop limités dans leur puissance d'expression, soit coûteux **[Wandl] [Opnet]**. Ainsi, le langage AWK permet un parcours syntaxique fondé sur la reconnaissance d'expressions régulières, mais celles-ci sont organisées séquentiellement ; le modèle AWK parcourt ses conditions de haut en bas. A contrario, YACC génère un véritable analyseur syntaxique hors-contexte, mais son utilisation routinière est fastidieuse et délicate. Le langage HAWK et son processeur se situent à mi-chemin entre ces deux extrêmes.

En effet, HAWK permet d'exprimer intuitivement un parcours syntaxique simple et d'associer des actions sémantiques à des règles syntaxiques. De plus, le processeur HAWK est un interprète et non un générateur de code ; son utilisation est donc aussi facile que AWK ou PERL. Essentiellement, HAWK est un analyseur syntaxique orienté « ligne par ligne » avec lequel on peut exprimer des tests sémantiques.

Rappelons qu'une expression régulière est un modèle de texte constitué de caractères ordinaires (par exemple les lettres de a à z) et de caractères spéciaux, appelés « métacaractères ». Le modèle décrit une ou plusieurs chaînes à mettre en correspondance lors d'une recherche effectuée sur un texte.

L'originalité de HAWK consiste à structurer les expressions régulières avec des méta-opérateurs réguliers.

L'objectif de cet outil est d'exprimer simplement un patron relativement complexe afin de répondre, par exemple, le contrôle d'accès **BACKBONE** existe et est conforme à la politique de sécurité réseau ou encore toutes les interfaces **ETHERNET** ont leur sous-paramètre **IPREDIRECT** désactivé conformément à la politique de sécurité réseau.

2.1 Le patron HAWK

HAWK permet d'exprimer un patron comme une suite de blocs (`DECLARE`, `BEGIN`, `SUCCESS`, `FAILURE`) et un pattern entre le bloc `BEGIN` et le bloc `SUCCESS`.

Un patron classique en HAWK s'écrit de la manière suivante :

```
DECL {
 déclaration1
 etc.
}

BEGIN {
 intruction1
 etc.
}

PATTERN


SUCCESS {
 intruction1
 etc.
}

FAILURE {
 intruction1
 etc.
}
```

Le bloc DECL contient la déclaration des variables (chaîne de caractères ou entière), des tableaux (contenant des chaînes ou des entiers) et des définitions de macros. La notion de « fonction » n'existe pas en HAWK. Il n'y a donc pas de récursivité possible (une programmation itérative devra être mis en place). Toutes les variables doivent être déclarées.

Le bloc optionnel BEGIN contient une suite d'instructions qui sera exécutée avant la validation du patron.

Le PATTERN entre le bloc DECLARE et le bloc BEGIN correspond au patron de conformité que HAWK valide sur le fichier d'input.

Le bloc optionnel SUCCESS contient des instructions qui seront exécutées si le fichier d'input correspond au patron syntaxique.

Le bloc optionnel FAILURE contient des instructions qui seront exécutées si le fichier d'input ne correspond pas au patron syntaxique ; c'est-à-dire si le moteur ne peut plus trouver une expression régulière pour une ligne d'input.

Les deux derniers blocs sont exécutés à la fin du processus et sont mutuellement exclusifs.

2.2 Les instructions HAWK

Comme en AWK, HAWK permet d'ajouter des instructions dans les blocs BEGIN, dans le PATTERN HAWK via des accolades {...} et dans les blocs SUCCESS et FAILURE. La liste des instructions possibles est riche et le lecteur est invité à se référer à la documentation disponible **[HAWK]**.

Deux types de variables ou tableaux peuvent être définis dans le bloc DECL :

⇨ Des variables de type string (chaîne de caractères)

```
DECL {
  str this_line;
}
```

⇨ Des variables de type int (entier)

```
DECL {
  int this_line_number;
}
```

HAWK implémente des tableaux associatifs à la mode AWK dont l'index est une chaîne de caractères. La taille du tableau s'ajuste dynamiquement.

```
DECL {
  str line[];
}
```

En complément des variables, HAWK permet de définir des macros PATTERN et d'instructions. L'écriture des patrons est grandement simplifiée par la référence (et donc l'expansion) des macros.

De plus, le langage HAWK implémente des instructions de condition, de boucle, etc. dans une syntaxe C :

⇨ l'instruction « if *(expression)* then *statement* else *statement* » permettant de définir une condition de branchement ;

```
DECL {
  str this_line;
}

if (this_line == "line") then
  {..}
else
  { ..}
```

⇨ l'instruction « forall (*value-identifier* = *array-identifier*[*index-identifier*]) *statement* » permettant de définir une itération sur l'ensemble des index et des valeurs contenues dans un tableau donné.

```
DECL {
  str line[], this_line, line_index;
}

forall (this_line = line[line_index])  {
  -
}
```

Enfin, des fonctions prédéfinies existent dans HAWK comme :

⇨ str field(n, s, fs) : cette fonction renvoie le « n » ième champ de la chaîne de caractère « s » séparé par « fs », au sens de AWK.

⇨ str FILENAME : cette fonction renvoie le nom du fichier qui est lu.

⇨ int length(s) : cette fonction renvoie la longueur de la chaîne « s ».

⇨ etc.

Il n'y a pas de variable prédéfinie.

Nous verrons dans le chapitre « exemples » la mise en œuvre de ces fonctions et variables.

2.3 Le PATTERN HAWK

Le PATTERN HAWK correspond donc au template de conformité que HAWK valide. Il peut être constitué d'une simple expression régulière de base telle que (elle indique qu'il doit y avoir une ligne vty) :

```
[eis]:^line vty.*$
```

Une telle expression est constituée de flags entre crochets « [...] » suivis du délimiteur « : », et enfin de l'expression régulière. Le PATTERN peut aussi être constitué d'une suite d'expressions régulières telle que (elle indique qu'il doit y avoir une ligne vty et une access-class) :

```
[fx] :line vty.*$
[fx] : access-class 99 in
```

HAWK permet aussi de définir une notion de bloc d'expressions régulières par des parenthèses « (...) » qui sont utilisées pour regrouper des patterns ou des expressions mathématiques (elle indique qu'il doit y avoir 0 ou plusieurs « une ligne `vty` » et `access-class` associées).

```
*(
   [fx] :line vty.*$
   [fx] : access-class 10 in
)
```

De plus, HAWK permet d'utiliser des opérateurs de structures qui peuvent être appliqués sur les patterns tels que :

- La disjonction logique : pattern1 | pattern2 | pattern3 ... : Elle se traduit, dans le langage logique ou mathématique, par l'opérateur « OU logique ». Dans l'exemple ci-dessous, on réalise une disjonction entre deux expressions régulières (on a soit une `access-class`, soit un `transport input none`) :

```
   :^ access-class 99 in$
|
   :^ transport input none$
```

- La conjonction : pattern1 & pattern2 & pattern3 .... : Elle se traduit, dans le langage logique ou mathématique, par l'opérateur « ET logique ». Dans l'exemple ci-dessous, on réalise une conjonction entre deux expressions régulières (on a une `access-class` et un `transport input telnet`) :

```
   :^ transport input
&
   :^ transport input telnet
```

- La négation : ! pattern : Elle traduit, dans le langage logique ou mathématique, par l'opérateur « NON logique ». Dans l'exemple ci-dessous, on réalise une conjonction entre deux expressions régulières (on a un `transport input`, mais pas un `transport input telnet`) :

```
   :^ transport input
&
   !:^ transport input telnet
```

Le méta-opérateur régulier de disjonction est classique. D'autre part, les méta-opérateurs de conjonction et de négation sont originaux à HAWK. Bien qu'il soit facile de démontrer que ces opérateurs sont effectivement réguliers, seule la négation est implémentée via l'option `-v` de GREP, et aucune implémentation de la conjonction n'est connue. La conjonction permet une expression intuitive et puissante.

Les autres méta-opérateurs (fermeture stricte, fermeture large) sont également implémentés ; un patron HAWK est donc une expression régulière, où chaque élément est lui-même une expression régulière. Ce modèle ne permet pas d'exprimer une construction régulière récursive.

2.4 Le moteur HAWK

Un moteur tel que celui de HAWK permet de parcourir un fichier d'entrée en fonction du patron syntaxique. Les méta-opérateurs réguliers sont implémentés par un automate non déterministe ; le moteur HAWK est donc purement non déterministe, a contrario de HDIFF **[HDIFF]** qui était purement déterministe.

En conséquence, il peut donc y avoir plusieurs patterns évalués « en parallèle » et il peut aussi y avoir plusieurs actions exécutées « en parallèle ». L'ordre d'évaluation d'un pattern versus un autre dans une conjonction n'est pas garanti.

HAWK est écrit en moins de 10.000 lignes de code C et les sources de cet outil sont disponibles **[HAWK]**. L'outil HAWK implémente des algorithmes efficaces de la théorie des automates. En conséquence, HAWK a le même comportement asymptotique que GREP ; le temps d'exécution de HAWK est donc proportionnel au nombre de lignes de son input. En fait, le temps total est dominé par le traitement d'ouverture et de lecture des fichiers, le temps consommé par le parcours syntaxique de HAWK est négligeable. Évidemment, ces considérations ne tiennent pas compte du temps d'exécution d'éventuelles instructions.

En situation réelle sur un PC récent (FreeBSD 6.2-RELEASE-p8), environ 70.000 fichiers de configuration (36 millions de lignes de configurations) sont validés dans l'ordre de 4 minutes avec un patron HAWK contenant 15 règles.

3. Exemples

3.1 Line vty

Ce premier exemple imprime toutes les `LINE VTY` d'une configuration de type CISCO :

```
*!                      :^line vty
* (
                        :^line vty
                        { printf("%s\n", LINE); }
                        *!:^line vty
)
```

Ce deuxième affiche toutes les `LINE VTY` d'une configuration de type CISCO, mais en imposant qu'il en existe au moins une comme l'illustre le *template* suivant :

```
*!                      :^line vty

# au moins une ligne doit être présente
+ (
                        :^line vty
                        { printf("%s\n", LINE); }
```

```
                    *!:^line vty
)

FAILURE
{
  printf("FAIL at line %ld '%s'\n", LINENO, LINE);
}
```

Cet exemple impose que le bloc FAILURE soit défini afin d'imprimer un message d'erreur en cas de non validation du template (il n'existe pas de ligne VTY).

L'exemple suivant ajoute la contrainte supplémentaire d'avoir une liste de filtrage (access-class xx in) pour le trafic à destination du routeur. On notera aussi la déclaration de macro pattern permettant de simplifier la syntaxe du patron.

```
DECL
{
  macro sub_block       :^[ ]
                        ;
  macro no_access_class ( sub_block & !:^ access-class
                        );
}

*!:^line vty
+ (
   :^line vty
   (
     * no_access_class
       :^ access-class .* in$
     * no_access_class
   )
   *!:^line vty
)

FAILURE
{
  printf("FAIL at line %ld '%s'\n", LINENO, LINE);
}
```

Si on souhaite préciser que la liste de filtrage ne doit être vérifiée si la ligne est utilisée à une fin d'administration de l'équipement (telnet, ssh) et non à une fin de service, alors on écrira le template de la manière suivante :

```
DECL
{
  macro sub_block       :^[ ]
                                ;
}
*!:^line vty

+ (
       :^line vty

        (
              * sub_block
                :^ access-class .* in$
              * sub_block
            |
              * sub_block
              (
                    :^ transport input
              &
                    ! [e]:^ transport input.*(telnet|all|ssh)
              )
              * sub_block
            )

         *!:^line vty
)

FAILURE
{
  printf("FAIL at line %ld '%s'\n", LINENO, LINE);
}
```

En cas de non-conformité avec le template, HAWK sort à la première ligne de configuration qui viole le template :

```
[cedric@yogi ~/hawk]$ hawk -f ./aux_line_v3.tp ./bpar510
FAIL at line 14064 ' password 7 07192B7D740E482E1A'
[cedric@yogi ~/hawk]$
```

3.2 ACL définies et non référencées, ACL référencées et non définies

HAWK fonctionne aussi pour une analyse purement sémantique comme la détection d'ACL référencée et non définie, et la détection d'ACL définie et non référencée. Ici, le parcours syntaxique n'est utilisé que pour collecter les informations analysées a posteriori.

Pour y parvenir, on définit deux tableaux qui contiendront les ACL référencées et les ACL définies :

```
DECL
{
  str acl_def[],acl_ref[],this_acl,i;
}
```

On enregistre ensuite les ACL définies et référencées (on ne couvre ici que le cas des ACL définies sur des line vty et référencée pour snmp) :

```
#------------
# ACL defined
#------------
*!:^access-list [0-9].*
* (
   :^access-list [0-9].*
   {acl_def[field(2)]=LINE;}
   *!:^access-list [0-9].*
)

#--------------
# ACL referenced
#--------------
*!:^snmp-server community .* RO [0-9].*$
* (
   :^snmp-server community .* RO [0-9].*$
   {acl_ref[field(5)]=LINE;}
   *!:^snmp-server community .* RO [0-9].*$
)
```

On boucle enfin pour détecter les ACL définies et non référencés et vice et versa :

```
SUCCESS
{
  forall(this_acl = acl_def[i]) {
    if (acl_ref[i] == "") {
       printf("%s;acl %s defined and not referenced\n",FILENAME,i);
    }
  }

  forall(this_acl = acl_ref[i]) {
    if (acl_def[i] == "") {
       printf("%s;acl %s referenced and not defined\n",FILENAME,i);
    }
  }
}
```

3.3 Détection de vulnérabilité

HAWK peut être aussi utilisé pour la détection de vulnérabilités dans les configurations des équipements. Récemment, une vulnérabilité CISCO portant sur le protocole SSH **[SSH]** a été déclarée exploitable si la version d'IOS est 12.4, si SSH est configuré pour l'administration du routeur et si la `line` n'est pas protégée par une ACL (filtrant les adresses IP autorisées à accéder à l'équipement).

Voici le patron HAWK capable de réaliser cette vérification :

```
DECL {
        macro   anything        * :.*
                                ;
        macro   indent          :^[ ]
                                ;
        macro   reachable       (
                                        indent
                                &
                                        ! [ex] :^ access-class [^ ]+ in
                                );
        str     vty, vuln;
}
```

Le corps du patron contrôle la version IOS, la présence de la configuration SSH et si des « lignes `vtys` » ne sont pas protégés :

```
anything
:^version 12\.4
anything

:^crypto
(
        * indent
        :^ rsakeypair
        * indent
)

anything
:^line vty
{ vty = LINE; }
(
        * reachable
        :^ transport input .*ssh
        * reachable
) { vuln = vty; }

anything
```

En cas de succès du patron, on imprime alors que l'équipement est vulnérable :

```
SUCCESS
{
        printf("%s vulnerable %s\n", FILENAME, vuln);
}
```

Conclusion

Nous avons décrit le langage HAWK en soulignant sa puissance d'expression et la facilité intuitive avec laquelle on peut écrire un parcours syntaxique enrichi d'actions sémantiques. Les concepts originaux de HAWK en font un outil souple et accessible. Enfin, son implémentation est efficace.

En revanche, HAWK est naturellement limité au parcours « ligne par ligne » ; l'analyse de configurations en format libre n'est pas possible dans notre contexte. De plus, une bonne connaissance des expressions régulières est nécessaire, et la complexité des patterns peut facilement occulter le sens général d'une vérification. Il convient donc de fragmenter une validation complexe en plusieurs patterns distincts.

Références

[HAWK] Les sources de HAWK sont disponibles sur le site web : **http://tableaux.levier.org**

[Llorens, Valois] LLORENS (C.), LEVIER (L.) VALOIS (D.), *Tableaux de bord de la sécurité réseau*, 2ème édition, Eyrolles, 560 pages, ISBN 2-212-11973-9, septembre 2006.

[Valois, Llorens] VALOIS (D.), LLORENS (C.), « *Detection of security holes in router configurations* », conférence FIRST, Hawaii, juin 2002, **http://www.first.org/events/progconf/2002/d4-04-valois-slides.pdf**

[Llorens] LLORENS (C.), *Mesure de la sécurité « logique » d'un réseau d'un opérateur de télécommunications*, thèse de l'École Nationale Supérieure des Télécommunications de Paris, **http://pastel.paristech.org/bib/archive/00001492/01/these_cedric_llorens.pdf**

[NSA] Guides de sécurité, **http://www.nsa.gov/snac/downloads_all.cfm**

[Opnet] **http://www.opnet.com/solutions/network_planning_operations/sp_sentinel.html**

[SSH] **http://www.cisco.com/warp/public/707/cisco-sa-20080521-ssh.shtml**

[Wandl] **http://www.wandl.com**

cedric.foll@(laposte.net|education.gouv.fr),
Architecte système et réseaux, Ingénieur de recherche, http://cedric.foll.name/

ÉMULATION D'ARCHITECTURES RÉSEAU

mots clés : ***réseau / sécurité / VLAN / 802.1q / virtualisation / Linux***

Cet article est le premier d'une série présentant des solutions permettant la conception de réseaux virtuels à partir d'un simple PC sous Linux et de logiciels libres dans une perspective de prototypage, d'enseignement ou encore de bac à sable pour le pen-tester. Dans le premier article nous étudierons Netkit, un dispositif émulant des PC sous Linux.

La virtualisation de serveurs et de postes de travail est aujourd'hui une pratique extrêmement répandue. Elle est devenue indispensable à tous les administrateurs système pour effectuer des tests de pré-production ou optimiser les ressources matérielles des *data centers*. Nous exposons dans cet article ce que les mécanismes de virtualisation peuvent apporter aux administrateurs et architectes réseau dans une optique de prototypage. Ces outils servent également dans le cadre d'enseignements ou comme outil d'étude pour le *pen-tester* souhaitant répliquer l'architecture d'une partie du réseau audité pour effectuer des tests avant de lancer l'attaque en réel.

La reproduction en laboratoire de réseaux réalistes avec du matériel dédié est souvent laborieuse Le matériel est volumineux, cher et surtout extrêmement bruyant. Virtualiser des réseaux complexes à partir d'un simple poste de travail présente de nombreux avantages.

Les briques présentées permettent par exemple de tester l'attaque contre DNS décrite par Dan Kaminsky dans différentes configurations et avec une architecture DNS complète (*root(s)* serveur(s), *master(s)* de zone, cache(s) et *forwarder(s)*) sur un simple PC sous Linux.

Elles peuvent également être mises à contribution pour reproduire l'attaque contre YouTube par Pakistan Telecom (quelle bande de farceurs !) [**http://www.ripe.net/news/study-youtube-hijacking.html**] ou encore tester l'attaque décrite par Anton Kapela et Alex Pilosov sur le détournement de trafic réseau exploitant les faiblesses de BGP et présentée à la DefCon 2008.

1. Présentation de Netkit

Netkit [**http://www.netkit.org**] est un logiciel libre sous licence GPL développé par le groupe « *computer network research* » de l'université italienne Rome 3 et par le LUG (*Linux User Group*) « Roma 3 ».

Il est composé de différents scripts permettant le lancement et l'arrêt des machines virtuelles, d'un noyau Linux UML et de l'image d'une distribution issue de Debian disposant d'outils liés au réseau dont voici une liste non exhaustive :

- support de 802.1q (VLAN), 802.1d (*spanning tree*) ;
- démons de routage dynamiques (*quagga*) avec support de MPLS et distribution de labels par LDP ;
- support des tunnels IPsec, GRE et MPLS (*IP over MPLS* et *Ethernet over MPLS*) ;
- support d'IPv6 ;
- outils de filtrage (iptables, ebtables) ;
- DNS coté serveur (Bind) et client (host et dig) ;
- SMTP avec Exim ;

- FTP avec Proftpd et TFTP avec atftpd ainsi que des clients respectifs ;
- Apache, Squid et différents clients web en mode texte ;
- Telnet et ssh côtés clients et serveurs ;
- Samba ;
- outils de *sniffing* (tcpdump, ettercap, dnsiff,...) ;
- outils de détection d'intrusion (snort, arpwatch,...) ;
- outils offensifs (nmap, hping, arpspoof, ...) ;
- ...

Le site diffusant Netkit met également à disposition un très grand nombre de *laboratoires* prêts à fonctionner (architecture DNS complète, routage dynamiques RIP, BGP, ...) avec une documentation associée décrivant de manière détaillée le fonctionnement.

Les machines virtuelles peuvent accéder à l'extérieur via une interface TAP (ce sont des interfaces virtuelles sous Linux liées à un ou des processus). Dès lors, les machines Netkit étant dérivées de DEBIAN, un simple `apt-get install` permettra d'installer n'importe quel paquet de la branche *unstable*, le fichier `sources.list` n'a même pas besoin d'être édité pour ceci.

Netkit fonctionne sur Linux et son installation extrêmement simple ne sera pas détaillée. Il suffit de télécharger les trois archives correspondant respectivement aux scripts, au noyau Linux UML et au système de fichiers, de les décompresser et d'initialiser quelques variables d'environnement. L'installation ne nécessite pas les droits root et il en est de même pour l'utilisation sauf pour la création éventuelle d'une interface TAP sur le système hôte.

2. Découverte au travers d'un premier lab

2.1 Lancement de deux PC

Nous commençons par lancer deux machines virtuelles dans un même LAN que nous appellons « A ».

```
$ vstart client --eth0=A
$ vstart pirate --eth0=A
```

Un terminal X est associé à chacune des machines virtuelles (`client` et `pirate`) lors de leur création. Chacune dispose d'une interface réseau (`eth0`) reliée au même hub virtuel du domaine de *broadcast* « A » (c'est-à-dire sur le même domaine de collision). Tous les paquets émis sur celui-ci seront transmis à toutes les interfaces des machines Netkit connectées à ce hub.

Nous disposons maintenant de deux machines virtuelles raccordées toutes les deux au hub virtuel « A ». Il ne reste plus qu'à configurer nos deux cartes réseau :

Sur `client` :

```
client:~# ifconfig eth0 172.30.0.1
```

Puis sur `pirate` :

```
pirate:~# ifconfig eth0 172.30.0.66
pirate:~# arp -an
pirate:~# ping -c 1 172.30.0.1
PING 172.30.0.1 (172.30.0.1) 56(84) bytes of data.
64 bytes from 172.30.0.1: icmp_seq=1 ttl=64 time=10.7 ms

--- 172.30.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 10.789/10.789/10.789/0.000 ms
routeur:~# arp -an
? (172.30.0.1) at CE:38:C3:A7:D6:72 [ether] on eth0
```

Attention

Remplacer le hub virtuel par un switch

Il est également possible de remplacer les hubs virtuels par des *switchs* virtuels en modifiant les scripts de lancement de Netkit.

Pour ceci, il conviendra d'éditer le fichier `bin/script_utils` et de remplacer la ligne suivante :

```
HUB_COMMAND="$NETKIT_HOME/bin/uml_switch -tap $TAP_DEVICE -hub -unix $1 </dev/null 2>&1"
```

par

```
HUB_COMMAND="$NETKIT_HOME/bin/uml_switch -tap $TAP_DEVICE -unix $1 </dev/null 2>&1"
```

et la ligne suivante :

```
HUB_COMMAND="$NETKIT_HOME/bin/uml_switch -hub -unix $1 </dev/null 2>&1"
```

par

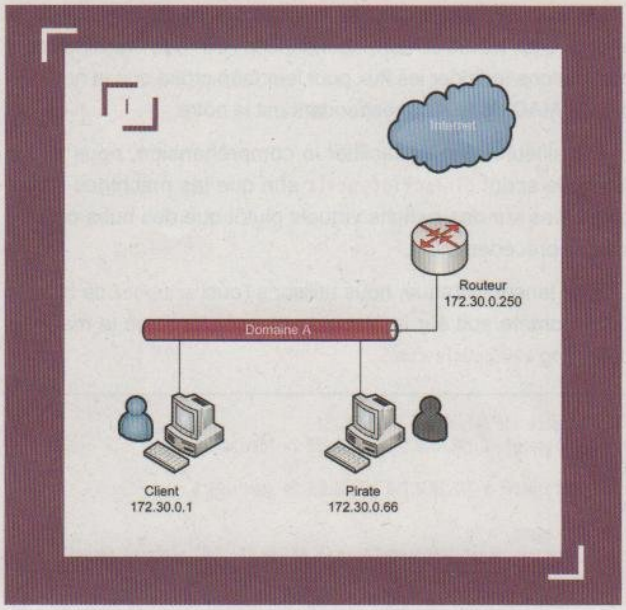
```
HUB_COMMAND="$NETKIT_HOME/bin/uml_switch -unix $1 </dev/null 2>&1"
```

Il est également possible de créer une machine Netkit faisant office de bridge comme nous le verrons par la suite.

2.2 Routeur avec accès à l'extérieur

Pour accéder à l'extérieur, nous créons un routeur disposant d'une interface `eth0` sur le hub virtuel « A » et d'une interface `eth1` (interface TAP du système hôte), afin de faire communiquer l'ensemble des machines virtuelles vers l'extérieur et donc de pouvoir installer de nouveaux paquets.

Le réseau ressemble alors à ceci : voir figure 1.



Attention

⇨ Interfaces TAP

La création d'une machine virtuelle disposant d'une interface TAP nécessite que l'utilisateur dispose des droits root sur le système hôte.

La commande peut être lancée avec les droits sans privilège, l'utilisateur sera invité, au moment de la création de l'interface TAP, à fournir le mot de passe root.

Nous pouvons noter l'apparition de l'interface `nk_tap_cedric` avec l'adresse IP `10.0.0.1` sur le système hôte :

```
$ vstart routeur --eth1=tap,10.0.0.1,10.0.0.2 --eth0=A
$ ifconfig
(...)
nk_tap_cedric Link encap:Ethernet  HWaddr 00:ff:c4:e2:54:9a
          inet adr:10.0.0.1  Bcast:10.255.255.255  Masque:255.0.0.0
          adr inet6: fe80::2ff:c4ff:fee2:549a/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Packets reçus:0 erreurs:0 :0 overruns:0 frame:0
          TX packets:26 errors:0 dropped:4 overruns:0 carrier:0
          collisions:0 lg file transmission:500
          Octets reçus:0 (0.0 B) Octets transmis:3817 (3.7 KB)
```

De même, une interface `eth1` avec l'IP `10.0.0.2` a été créée sur la machine virtuelle « routeur » qui peut maintenant joindre l'extérieur.

En outre, dans sa grandeur et afin de nous faciliter la vie, Netkit a effectué les opérations suivantes sur le système hôte :

⇨ ajout d'une règle de translation d'adresse ;

⇨ ajout d'une règle autorisant les flux émis par notre interface TAP ;

⇨ activation du routage :

```
$ sudo iptables-save
# Generated by iptables-save v1.3.8 on Mon Aug 11 22:30:56 2008
*nat
:PREROUTING ACCEPT [1:105]
:POSTROUTING ACCEPT [1:149]
:OUTPUT ACCEPT [13:2343]
-A POSTROUTING -j MASQUERADE
COMMIT
# Completed on Mon Aug 11 22:30:56 2008
# Generated by iptables-save v1.3.8 on Mon Aug 11 22:30:56 2008
*filter
:INPUT ACCEPT [41715:40819632]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [35749:4377205]
-A FORWARD -i nk_tap_+ -j ACCEPT
COMMIT
# Completed on Mon Aug 11 22:30:56 2008

$ cat /proc/sys/net/ipv4/ip_forward
1
```

Netkit a également ajouté une règle de routage sur le routeur précisant que la passerelle par défaut est l'interface TAP du système hôte.

Il ne reste plus qu'à finir de configurer le DNS sur notre routeur (fichier `/etc/resolv.conf`), son adresse interne (disons `172.30.0.250`) et de s'assurer que le routage est activé (il l'est par défaut sur toutes les machines Netkit).

```
routeur:~# cat > /etc/resolv.conf
nameserver 192.168.2.1
routeur:~# ifconfig eth0 172.30.0.250
routeur:~# ping -c 1 www.google.com
PING www.l.google.com (209.85.129.99) 56(84) bytes of data.
64 bytes from fk-in-f99.google.com (209.85.129.99): icmp_seq=1 ttl=241
time=64.1 ms

--- www.l.google.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 64.163/64.163/64.163/0.000 ms
```

Puis sur `client` et `pirate` :

```
client:~# cat > /etc/resolv.conf
nameserver 192.168.2.1
client:~# route add default gw 172.30.0.250
```

Cela suffit-il pour que les machines autres que le routeur puissent joindre l'extérieur ?

Non ! Le système hôte sera incapable de router les paquets retour. Il n'a en effet aucune connaissance du plan d'adressage internet des machines Netkit (dans notre cas `172.30.0.0/16`). Nous avons deux solutions :

⇨ Réaliser une seconde translation d'adresse au niveau du routeur pour que les paquets qu'il émet vers l'interface TAP le soient avec l'adresse IP `10.0.0.2`.

⇨ Ajouter une route sur le système hôte pour router les paquets `172.30.0.0/16` vers l'interface TAP.

C'est la première solution que nous choisirons.

Sur le routeur :

```
routeur:~# iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```

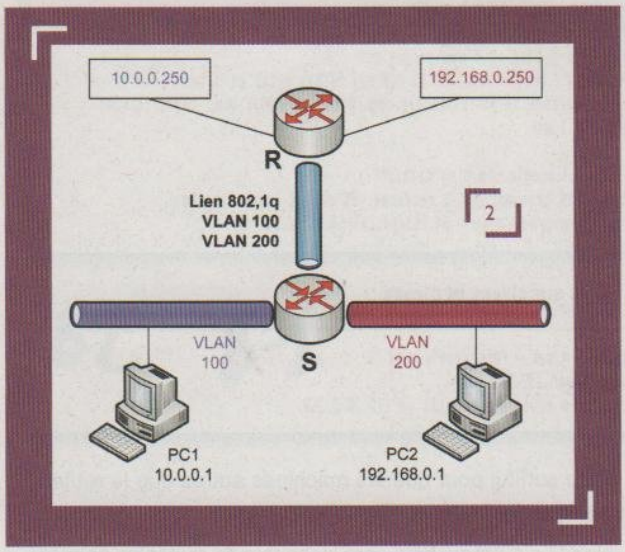
Vérifions que tout fonctionne comme escompté sur le client :

```
client:~# ping -c 1 www.google.com
PING www.l.google.com (209.85.129.104) 56(84) bytes of data.
64 bytes from fk-in-f104.google.com (209.85.129.104): icmp_seq=1 ttl=240 time=64.0 ms

--- www.l.google.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 64.071/64.071/64.071/0.000 ms
```

Il est maintenant possible d'installer des paquets supplémentaires sur les machines virtuelles ou de mettre à jour les paquets présents. Pour ceci, il est toutefois nécessaire d'augmenter la mémoire de la machine concernée grâce à l'option `-M` afin d'utiliser `apt-get` confortablement.

2.3 Attaque de type Man in The Middle

Nous allons maintenant nous essayer à une attaque de type *Man In The Middle* par *arp cache poisoning*. Ce type d'attaque a déjà été évoqué dans *MISC* et la littérature sur le sujet est abondante.



De manière synthétique, le principe de l'attaque est de corrompre les tables de correspondances ARP des machines dont nous voulons rediriger les flux pour leur faire croire que la nouvelle adresse MAC de leur correspondant est la nôtre.

Par ailleurs, afin de faciliter la compréhension, nous avons modifié le script `bin/script_utils` afin que les machines soient connectées sur des switchs virtuels plutôt que des hubs comme expliqué précédemment.

Pour lancer l'attaque, nous utilisons l'outil `arpspoof` de la suite `dsniff` comme suit sur la machine `pirate` alors que la machine `client` *ping* `www.google.com` :

```
pirate:~# route add default gw 172.30.0.250
pirate:~# arpspoof -t 172.30.0.1 172.30.0.250 2> /dev/null &
[1] 438
pirate:~# arpspoof -t 172.30.0.250 172.30.0.1 2> /dev/null &
[2] 439
pirate:~# tcpdump -n ip
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
20:50:28.207517 IP 172.30.0.1.32768 > 192.168.2.1.53: 37172+ A? www.google.com. (32)
20:50:28.210729 IP 172.30.0.66 > 172.30.0.1: ICMP redirect 192.168.2.1 to host
172.30.0.250, length 68
20:50:28.211176 IP 172.30.0.1.32768 > 192.168.2.1.53: 37172+ A? www.google.com. (32)
20:50:28.208438 IP 192.168.2.1.53 > 172.30.0.1.32768: 37172 4/0/0 CNAME www.l.google.
com.,[|domain]
20:50:28.208461 IP 192.168.2.1.53 > 172.30.0.1.32768: 37172 4/0/0 CNAME www.l.google.
com.,[|domain]
20:50:28.215245 IP 172.30.0.1 > 209.85.129.99: ICMP echo request, id 46849, seq 1, length 64
20:50:28.215353 IP 172.30.0.1 > 209.85.129.99: ICMP echo request, id 46849, seq 1, length 64
20:50:28.279674 IP 209.85.129.99 > 172.30.0.1: ICMP echo reply, id 46849, seq 1, length 64
20:50:28.279717 IP 209.85.129.99 > 172.30.0.1: ICMP echo reply, id 46849, seq 1, length 64
20:50:28.281864 IP 172.30.0.1.32768 > 192.168.2.1.53: 21907+ PTR? 99.129.85.209.in-
addr.arpa. (44)
20:50:28.281929 IP 172.30.0.66 > 172.30.0.1: ICMP redirect 192.168.2.1 to host
172.30.0.250, length 80
20:50:28.281953 IP 172.30.0.1.32768 > 192.168.2.1.53: 21907+ PTR? 99.129.85.209.in-
addr.arpa. (44)
20:50:28.283556 IP 192.168.2.1.53 > 172.30.0.1.32768: 21907 1/0/0 (78)
20:50:28.283596 IP 192.168.2.1.53 > 172.30.0.1.32768: 21907 1/0/0 (78)
```

Il est intéressant de noter que les paquets apparaissent en double. Ils arrivent sur l'interface, puis sont re-routés sur cette même interface vers le destinataire légitime. Une telle décision de routage n'est d'ailleurs pas particulièrement propre et le moteur de routage de linux en avertit l'émetteur par un message `ICMP redirect` l'informant que le paquet devrait mieux être directement envoyé vers `172.30.0.250` (ce que croit faire le client).

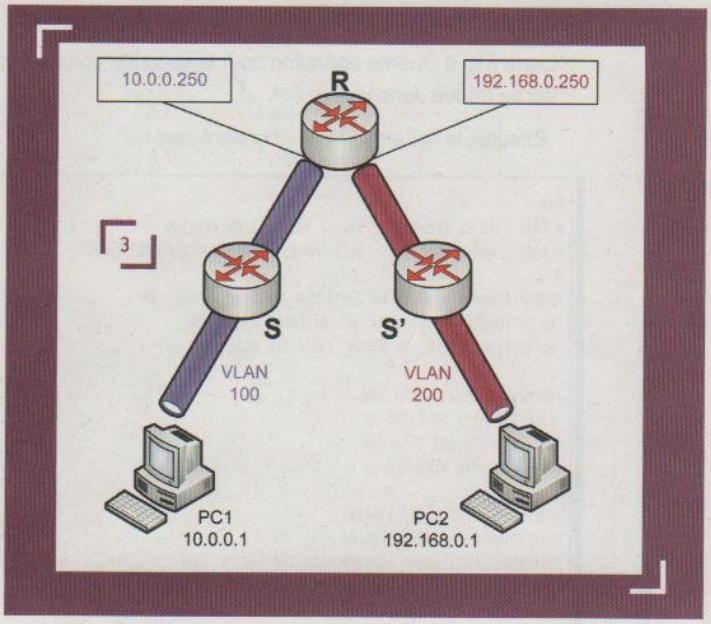
L'émission de ces paquets peut être désactivée sous Linux de la manière suivante :

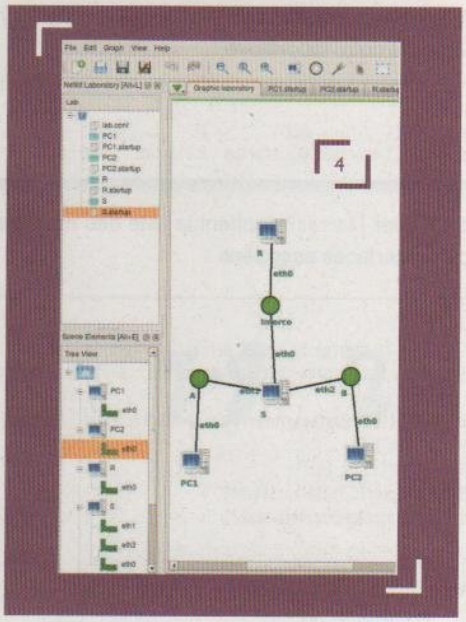
```
# echo 0 > /proc/sys/net/ipv4/conf/all/send_redirects
```

3. Un routeur au bout d'un bâton

L'objet de ce lab est d'introduire le concept de VLAN, ainsi que cette merveille d'architecture réseau nommée « *router on a stick* » : voir figure 2.

Ce type d'architecture permet de comprendre les mécanismes de routage inter-VLAN. Nous avons un routeur disposant d'une seule interface physique et qui réalise du routage entre les zones





10.0.0.0/24 et 192.168.0.0/24. Dans cet exemple, il est connecté à deux zones, mais il pourrait très bien par la même interface router des paquets vers beaucoup plus de VLAN. Ceci permet d'économiser des ports, souvent coûteux, sur les équipements de type routeurs et firewalls.

La représentation logique en couche 3 de cette architecture est celle-ci : voir figure 3.

3.1 Rappel sur les VLAN

Les VLAN sont une technologie permettant de faire coexister, de manière étanche, différents LAN (c'est-à-dire domaines de broadcast).

Sur chacun des ports d'un switch supportant les VLAN, l'administrateur spécifie à quel VLAN appartient le port. Deux ports appartenant au même VLAN peuvent communiquer tandis que les échanges entre deux ports appartenant à des VLAN différents sont impossibles (comme s'ils étaient sur deux switchs différents).

Le second concept à la base des VLAN est l'encapsulation 802.1Q. Ce mécanisme permet le multiplexage de VLAN sur un lien. Il est en effet possible de spécifier qu'un port appartient à plusieurs VLAN. Dans ce cas, le switch ajoutera un tag 802.1Q de 4 octets sur la couche Ethernet des paquets émis par cette interface. Les deux premiers octets déterminent le numéro de VLAN auquel appartient le paquet. Dans la terminologie Cisco, ces ports sont qualifiés de « *trunk* ».

Par ce moyen, il est possible :

- De propager nos VLAN en chaînant des switchs via des liens 802.1Q.
- De limiter le nombre d'interfaces des équipements réalisant du routage (routeur et firewalls). Il est en effet possible de router un paquet d'un VLAN vers un autre en ne disposant que d'une seule interface physique. On parle alors de routage inter-VLAN. Par exemple, le paquet entre avec un tag 802.1q spécifiant qu'il appartient au `vlan 100`, l'équipement prend une décision de routage et réémet le paquet sur la même interface avec un tag 802.1q spécifiant qu'il appartient maintenant au `vlan 200`.

Les VLAN sont aujourd'hui supportés par la quasi-totalité des switchs, routeurs et firewalls utilisés dans un contexte professionnel, ainsi que sur les principaux OS (en particulier Windows ou Linux). Cette technologie est utilisée dans la plupart des réseaux d'envergure (grandes entreprises, administrations, fournisseurs d'accès,...).

Dans notre exemple, nous allons « émuler » un switch supportant les VLAN par une machine sous Linux utilisant des fonctionnalités de type bridge.

3.2 Création de l'architecture

Nous avons dans ce laboratoire un routeur virtuel (R) disposant d'une seule interface, d'un switch (S) disposant de 3 interfaces et de deux PC. Lancer tout ceci en ligne de commande sans se tromper peut paraître un peu complexe, mais Netkit offre un système de fichiers de configuration permettant d'automatiser le lancement de laboratoires préconfigurés.

Afin de construire cette architecture, nous nous appuyons sur une interface graphique de Netkit, VisualNetkit [**http://code.google.com/p/visual-netkit/**], aidant à la génération de ces fichiers de configuration.

Le paquet se compile sans difficulté sur une Ubuntu Hardy et le réseau ci-dessus se configure en quelques minutes à la souris : voir figure 4.

Voici ce qui apparaît dans le répertoire où nous avons sauvegardé notre laboratoire :

```
$ ls
lab.conf  PC1          PC2          R         S
lab.xml   PC1.startup  PC2.startup  R.startup  S.startup
```

Le fichier `lab.conf` contient la liste des machines virtuelles avec les interfaces associées :

```
###
# This file is createb by Visual Netkit 1.0b version
# http://www.netkit.org ~ http://code.google.com/p/visual-netkit/
#
LAB_DESCRIPTION="Routage inter-vlan par Cedric Foll"
LAB_VERSION="1.0"
LAB_AUTHOR="Cedric Foll"
LAB_EMAIL="cedric.foll@laposte.net"
LAB_WEB="http://cedric.foll.name/"

PC1[0]="A"
PC2[0]="B"
R[0]="Interco"
S[0]="Interco"
S[1]="A"
S[2]="B"
```

Les fichiers `*.startup` contiennent la liste des commandes exécutées après lancement de la machine virtuelle. VisualNetkit se contentera de les créer en préconfigurant éventuellement les adresses IP. Il conviendra ensuite d'éditer ces fichiers afin de d'automatiser l'exécution des commandes nécessaires à notre architecture.

Par exemple, `R.startup` contient les lignes suivantes :

```
1: ###
2: # This file is createb by Visual Netkit 1.0b version
3: # http://www.netkit.org ~ http://code.google.com/p/visual-netkit/
4: #
5: /sbin/ifconfig eth0 up ## 'Interco' collision domain ##
6: /sbin/vconfig add eth0 100
7: /sbin/ifconfig eth0.100 10.0.0.250
8: /sbin/vconfig add eth0 200
9: /sbin/ifconfig eth0.200 192.168.0.250
```

Quelques explications :

Sous Linux, la création de sous-interfaces liées à des VLAN se fait via la commande `vconfig`. Le premier appel à `vconfig` ci-dessus a la signification suivante :

- Ligne 5 : création de l'interface `eth0`, qui n'a pas besoin d'adresse.
- Ligne 6 : création d'une sous-interface à `eth0`. Cette sous-interface sera nommée `eth0.100`.
- Les paquets Ethernet avec un tag 802.1q arrivant sur l'interface `eth0` spécifiant qu'ils appartiennent au `vlan 100` sont transmis à la sous-interface `eth0.100`.
- Les paquets émis via la sous-interface `eth0.100` sont envoyés par l'interface `eth0` avec un tag 802.1q spécifiant qu'ils appartiennent au `vlan 100`.
- Ligne 7 : attribution d'une adresse à cette sous-interface.
- Ligne 8 et 9 : même opération pour la seconde sous-interface qui se trouve dans le `vlan 200`.

Ensuite, le fichier `S.startup` contient ceci :

```
###
# This file is createb by Visual Netkit 1.0b version
# http://www.netkit.org ~ http://code.google.com/p/visual-netkit/
#
/sbin/ifconfig eth0 up ## 'Interco' collision domain ##
/sbin/ifconfig eth1 up ## 'A' collision domain ##
/sbin/ifconfig eth2 up ## 'B' collision domain ##

/sbin/vconfig add eth0 100
/sbin/ifconfig eth0.100 up
/sbin/vconfig add eth0 200
/sbin/ifconfig eth0.200 up

/usr/sbin/brctl addbr vlan100
/usr/sbin/brctl addif vlan100 eth1
/usr/sbin/brctl addif vlan100 eth0.100
/sbin/ifconfig vlan100 up

/usr/sbin/brctl addbr vlan200
/usr/sbin/brctl addif vlan200 eth2
/usr/sbin/brctl addif vlan200 eth0.200
/sbin/ifconfig vlan200 up
```

Sur cette machine, nous créons deux sous-interfaces à l'interface `eth0` (`eth0.100` et `eth0.200`). Ensuite nous *bridgeons* (commande `brctl`) les interfaces `eth0.100` avec `eth1` et `eth0.200` avec `eth2`.

Aussi, nous nous retrouvons avec un switch dont l'interface `eth1` se trouve dans le `vlan 100`, l'interface `eth2` dans le `vlan 200` et l'interface `eth0` est en mode 802.1q propageant les `vlan 100` et `200`.

En bridgeant nos interfaces et sous-interfaces, nous avons décrit la définition d'un switch configuré avec des VLAN (seules les interfaces dans les mêmes VLAN peuvent communiquer, c'est-à-dire que les interfaces dans les mêmes VLAN sont bridgées).

Enfin, les répertoires ayant pour nom ceux des machines virtuelles (`PC1`, `PC2`, `R` et `S` dans notre exemple) peuvent contenir des fichiers qui seront copiés dans l'arborescence des machines virtuelles correspondantes afin, par exemple, d'automatiser la configuration des démons.

Il ne reste plus qu'à tester notre laboratoire et vérifier que tout fonctionne comme escompté :

Sur `PC1` :

```
PC1:~# ping -c 1 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=63 time=1.04 ms

--- 192.168.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.049/1.049/1.049/0.000 ms
```

Sur `R` :

```
R:~# tcpdump -n -i eth0
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
23:09:30.328238 vlan 100, p 0, IP 10.0.0.1 > 192.168.0.1: ICMP echo request, id 42497,
seq 1, length 64
23:09:30.340558 vlan 200, p 0, IP 10.0.0.1 > 192.168.0.1: ICMP echo request, id 42497,
seq 1, length 64
23:09:30.328674 vlan 200, p 0, IP 192.168.0.1 > 10.0.0.1: ICMP echo reply, id 42497,
seq 1, length 64
23:09:30.328707 vlan 100, p 0, IP 192.168.0.1 > 10.0.0.1: ICMP echo reply, id 42497,
seq 1, length 64
```

Nous notons, avec émerveillement, le paquet `icmp request` entré avec un tag spécifiant qu'il appartient au `vlan 100`, puis ressorti avec un tag spécifiant qu'il appartient au `vlan 200`. Notre routeur a fait son travail.

Il est également possible de réaliser le `tcpdump` à partir d'une sous-interface et, dans ce cas, il n'y a plus de tag 802.1q :

```
R:~# tcpdump -n -i eth0.100
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0.100, link-type EN10MB (Ethernet), capture size 96 bytes
23:09:46.647203 IP 10.0.0.1 > 192.168.0.1: ICMP echo request, id 42753, seq 1, length 64
23:09:46.647580 IP 192.168.0.1 > 10.0.0.1: ICMP echo reply, id 42753, seq 1, length 64
```

3.3 Petite digression sur l'incommunicabilité dans les réseaux IP

Que se passe-t-il si un paquet de 1500 octets arrive sur une interface non taguée (par exemple `eth2`) avant d'être transmis vers une sous-interface (par exemple `eth0.200`) et se voir ajouter ainsi 4 octets ?

Nous nous retrouvons alors devant un problème aussi classique que souvent complexe des mécanismes liés à l'encapsulation et autre *tunneling*. En effet, comme le 802.1q ajoute 4 octets sur la couche Ethernet, les paquets déjà au maximum du MTU avant l'ajout de ce tag vont poser problème et être détruits.

Dans des cas aussi simples que celui-ci, les équipements récents, à la différence d'un Linux transformé en switch, savent s'en sortir, mais dans des cas plus compliqués (lorsque l'*overhead* est plus important) comme avec du tunneling (IPSec, GRE, PPPoE,...), il est nécessaire de trouver une solution satisfaisante.

Comment ce type de problème peut-il être résolu de manière transparente pour les administrateurs système (c'est-à-dire sans repasser sur tous les serveurs pour baisser de quatre octets leur MTU) ?

- La **fragmentation**. Pour ceci, un équipement de couche 3 (un routeur) doit détecter que le paquet est trop gros et envoyer un paquet ICMP « *need to fragment* » pour provoquer une fragmentation du paquet incriminé. Dans notre cas, le problème se produit avant qu'un équipement de couche 3 soit atteint. De plus, ce mécanisme est jugé obsolète et beaucoup d'OS ajoutent le tag DF (*Don't Fragment*) sur tous leurs paquets pour interdire la fragmentation.
- **Path MTU discovery** (RFC1191). Le mécanisme est similaire au précédent sauf qu'au lieu de fragmenter les paquets à la réception du message d'erreur ICMP, le client va envoyer des paquets avec un MTU plus faible. Cependant, le problème est le même que la fragmentation. La difficulté provient d'un équipement de couche 2 en amont de tout équipement de couche 3. Il n'y a donc pas d'ICMP possible.
- La RFC 4821. Celle-ci prévoit de diminuer le MTU lorsque des paquets sont perdus. Malheureusement, elle n'est pas encore largement implémentée (la RFC date de mars 2007).
- Le champ MSS (*Maximum Segment Size*) de la couche TCP. Il informe le destinataire des paquets de la taille maximum des données TCP que nous sommes à même d'accepter (ce qui a une incidence directe sur la taille des paquets IP). Pour notre plus grand bonheur, iptables est capable d'altérer dynamiquement les paquets qu'il transmet pour adapter le MSS à son MTU. Ceci se fait par la commande suivante :

```
# iptables -A FORWARD -p tcp --tcp-flags SYN,RST SYN -j TCPMSS  --clamp-mss-to-pmtu
```

Cette manipulation ne fonctionnant que pour les flux TCP l'administrateur réseau superstitieux brûlera un cierge afin qu'il n'y ait pas trop de paquets UDP de plus de 1496 octets qui transitent...

Conclusion

Au travers de cet article, nous avons vu comment avec un simple PC simuler des architectures réseau réalistes. L'éventail de possibilités inexploitées dans cet article (routage dynamique, MPLS, large éventails de services réseau, *firewalling*, IDS,...) est lui aussi impressionnant au regard des pré-requis matériels et logiciels nécessaires pour les mener à bien.

Dans un prochain article, nous verrons comment émuler des matériels Cisco tels que des routeurs ou des firewalls PIX.

Remerciements

Merci à Fabrice Flauss pour sa connaissance encyclopédique de Cisco, à Paul Tavernier pour ses tests et éléments de réflexion sur le problème de MTU, à Gilles Chaideyrou pour ses remarques tant sur le fond que sur la forme, aux enseignants du département ASI de l'INSA de Rouen pour m'avoir fait découvrir Netkit et à tous les relecteurs pour leurs corrections et conseils.

Christian Pélissier

COMPRENDRE LES RÔLES DE SOLARIS™ ET D'OPENSOLARIS

mots clés : *contrôle d'accès / rôles*

Le contrôle d'accès par rôles ou RBAC (Role-Based Access Control) de Solaris introduit avec Solaris 8 permet d'attribuer des privilèges aux utilisateurs pour leur permettre d'agir dans un certain nombre de domaines avec les mêmes droits que ceux dont dispose l'administrateur système. RBAC qui fonctionne en mode « userland » sous Solaris 8 et 9 et repose sur l'identité (uid) et les permissions a été modifié en profondeur dans Solaris 10 qui introduit un modèle de privilèges « Process Rights Management » au niveau « kernel ». Ce modèle remplace le privilège lié à l'uid zéro par un ensemble de privilèges pouvant être individuellement délégués ou révoqués. La compatibilité ascendante avec le modèle super-user est maintenue en accordant à ce dernier la totalité de ces privilèges.

Avec RBAC et les privilèges, Solaris 10 entre dans le 21e siècle avec les dispositifs permettant de définir le degré de sécurité adaptés aux exigences les plus strictes : être ou ne pas être root n'est plus la question, puisqu'il devient possible de mettre en œuvre une politique du moindre privilège chaque fois qu'on le jugera nécessaire.

Vu de l'administrateur système, RBAC est visible par :

⇨ cinq nouveaux fichiers de configuration :

```
/etc/security/auth_attr
/etc/security/prof_attr
/etc/security/exec_attr
/etc/user_attr
/etc/security/policy.conf
```

⇨ des *shells* modifiés permettant la prise en compte du rôle :

```
/usr/bin/pfsh
/usr/bin/pfcsh
/usr/bin/pfksh
```

⇨ une commande suid `pfexec` permettant de prendre en compte un profil d'exécution :

```
/usr/bin/pfexec
```

⇨ des commandes d'administration :

```
useradd, roleadd
usermod, rolemod
userdel, roledel
```

⇨ des commandes utilisables sans privilèges :

```
roles
profiles
auths
```

Dans l'exposé qui suit, nous allons nous intéresser tout d'abord au rôle du fichier `/etc/security/exec_attr`.

1. Le fichier /etc/security/exec_attr

Ce fichier contient la définition d'un certain nombre de profils d'exécution prédéfinis. L'examen de ce fichier permet de comprendre qu'un profil est défini par un nom comme *Mail Management*, qu'un certain nombre de commandes sont associées à ce nom et qu'il est précisé pour chacune de ces commandes sous quel *uid, euid, gid, egid* elle sera exécutée par le compte normal ou par le compte rôle auquel on aura associé le profil en question. En l'absence d'indication pour ces dernières valeurs, la commande est exécutée sans changer son identité initiale.

Un extrait de ce fichier `/etc/security/exec_attr` est représenté ci-contre.

Le premier profil `All` correspond à l'exécution de toutes les commandes sans modifier les identifiants d'exécution et on devine aisément à quoi correspond la dernière ligne `Primary Administrator`. Il est possible voire souhaitable d'ajouter dans ce fichier autant de profils qu'on le souhaite, d' enrichir, d'adapter voire de corriger les profils existants.

```
All:suser:cmd:::*:
...
Mail Management:suser:cmd:::/etc/init.d/sendmail:uid=0;gid=sys
Mail Management:suser:cmd:::/usr/lib/sendmail:uid=0
Mail Management:suser:cmd:::/usr/sbin/editmap:euid=0
Mail Management:suser:cmd:::/usr/sbin/makemap:euid=0
Mail Management:suser:cmd:::/usr/sbin/newaliases:euid=0
...
Maintenance and Repair:suser:cmd:::/etc/init.d/sysetup:uid=0;gid=sys
Maintenance and Repair:suser:cmd:::/etc/init.d/syslog:uid=0;gid=sys
Maintenance and Repair:suser:cmd:::/usr/bin/adb:euid=0
Maintenance and Repair:suser:cmd:::/usr/bin/date:euid=0
Maintenance and Repair:suser:cmd:::/usr/bin/ldd:euid=0
Maintenance and Repair:suser:cmd:::/usr/bin/vmstat:euid=0
Maintenance and Repair:suser:cmd:::/usr/sbin/crash:euid=0
Maintenance and Repair:suser:cmd:::/usr/sbin/eeprom:euid=0
Maintenance and Repair:suser:cmd:::/usr/sbin/halt:euid=0
Maintenance and Repair:suser:cmd:::/usr/sbin/init:euid=0
Maintenance and Repair:suser:cmd:::/usr/sbin/poweroff:uid=0
Maintenance and Repair:suser:cmd:::/usr/sbin/prtconf:euid=0
Maintenance and Repair:suser:cmd:::/usr/sbin/reboot:uid=0
Maintenance and Repair:suser:cmd:::/usr/sbin/syslogd:euid=0
...
FTP Management:suser:cmd:::/usr/sbin/ftpaddhost:uid=0
FTP Management:suser:cmd:::/usr/sbin/ftpconfig:uid=0
FTP Management:suser:cmd:::/usr/sbin/ftprestart:euid=0
FTP Management:suser:cmd:::/usr/sbin/ftpshut:euid=0;egid=sys
FTP Management:suser:cmd:::/usr/sbin/privatepw:uid=0;egid=sys
...
Primary Administrator:suser:cmd:::*:uid=0;gid=0
...
```

2. Création et définition d'un compte rôle

Un rôle est un compte particulier créé avec la commande `roleadd`, supprimé avec la commande `roledel` et modifié avec la commande `rolemod`. Notez qu'il est possible de transformer un compte normal en compte rôle en utilisant la commande `usermod`. Un compte rôle diffère d'un compte normal, car il est impossible d'ouvrir un login ou une session en utilisant un rôle. On ne peut qu'endosser le rôle en utilisant la commande `su`.

Les commandes `roleadd`, `rolemod` et `roledel` présentent une grande similitude avec les commandes `useradd`, `usermod`, `userdel` et un simple listage montre un lien hardware entre chaque couple :

```
$ ls -l /usr/sbin/useradd /usr/sbin/roleadd
-r-xr-xr-x   2 root     sys        35252 août 14  2007 /usr/sbin/roleadd
-r-xr-xr-x   2 root     sys        35252 août 14  2007 /usr/sbin/useradd
```

Rappelons brièvement la syntaxe de ces 2 commandes qui en réalité ne font qu'une (leur nom sert d'option) :

```
usage:  useradd [-u uid [-o] | -g group | -G group[[,group]...] | -d dir |
                -s shell | -c comment | -m [-k skel_dir] | -f inactive |
                -e expire | -A authorization [, authorization ...] |
                -P profile [, profile ...] | -R role [, role ...]]
                -p project [, project ...] login
        useradd -D [-g group | -b base_dir | -f inactive | -e expire
                -A authorization [, authorization ...] |
                -P profile [, profile ...] | -R role [, role ...]] |
                -p project

usage:  roleadd [-u uid [-o] | -g group | -G group[[,group]...] | -d dir |
                -s shell | -c comment | -m [-k skel_dir] | -f inactive |
                -e expire | -A authorization [, authorization ...] |
                -P profile [, profile ...]] login
        roleadd -D [-g group | -b base_dir | -f inactive | -e expire
                -A authorization [, authorization ...] |
                -P profile [, profile ...]]
```

3. Exemple de création d'un rôle

De façon simplifiée, on peut se contenter de créer un rôle par :

```
# roleadd -m -P "Maintenance and Repair" operator
```

Si on veut être plus précis, on fera :

```
# groupadd -g 101 operator
# roleadd -u 101 -g 101 -s /bin/pfksh -m -d /export/home/operator -P
"Maintenance and Repair" -c 'rôle opérateur' operator
```

Cette deuxième commande crée le rôle `operator` en renseignant les fichiers `/etc/passwd` et `/etc/shadow` comme l'aurait fait la commande `useradd` pour un compte ordinaire. Elle ajoute toutefois l'information complémentaire suivante dans le fichier `/etc/user_attr` se matérialisant par cette ligne indiquant le statut de rôle de ce compte :

```
operator::::type=role;profiles=Maintenance and Repair
```

Ce fichier doit être considéré comme une extension des fichiers `/etc/passwd` et `/etc/shadow`.

Pour le moment, le rôle est créé, mais il n'est affecté à aucun utilisateur et, comme les utilisateurs qui seront déclarés comme autorisés à utiliser ce rôle devront s'y rendre avec la commande `su`, il faut commencer par lui attribuer un mot de passe exactement comme on le ferait pour un compte normal :

```
# passwd operator
...
```

On autorise ensuite un utilisateur (voire plusieurs) à endosser ce rôle et ce n'est possible que si l'utilisateur qui va bénéficier de cette autorisation n'a pas une session en cours :

```
# usermod -R "operator" paulo
```

Ou ce qui revient au même :

```
# usermod -K role=operator paulo
```

Cette commande attribue le rôle `operator` à `paulo` et cela se traduit par l'ajout de la ligne suivante dans le fichier `/etc/user_attr` :

```
paulo::::type=normal;roles=operator
```

Si l'utilisateur a une session en cours, il est possible de déclarer le rôle en éditant le fichier. Il faudra toutefois que l'utilisateur se connecte à nouveau pour bénéficier de la déclaration.

L'utilisateur peut vérifier les rôles qu'il possède avec la commande :

```
$ roles
operator
```

Et nous pouvons faire de même en donnant un nom de login en argument à cette commande :

```
# roles paulo
operator
```

L'utilisateur endossera le rôle en utilisant la commande `su` :

```
$ su - operator
Mot de passe :
```

Et il pourra vérifier quels sont les profils qui sont accordés à ce rôle :

```
$ profiles
Maintenance and Repair
Basic Solaris User
All
```

Il pourra par exemple arrêter le système avec la commande `init` faisant partie du profil `Maintenance and Repair` associé au rôle `operator` qu'il vient d'endosser :

```
$ init 0
...
```

La suppression de l'autorisation de prendre le rôle sera effectuée comme ceci :

```
# usermod -R "" paulo
```

4. Associer un profil directement à un utilisateur

En associant un profil d'exécution à un compte rôle, puis en autorisant un ou plusieurs utilisateurs à endosser ce rôle avec la commande `su`, on a rompu le tout ou rien des premiers Unix puisqu'il est désormais possible d'accorder des privilèges sans en donner la totalité et d'avoir une traçabilité de leur utilisation, qui par défaut est celle de la commande `su`. Certains lecteurs trouveront toutefois cette façon de procéder trop contraignante ou la considéreront bien adaptée pour un serveur partagé par plusieurs intervenants au niveau système et pas du tout pour un poste de travail.

En autorisant d'associer un profil non pas à un compte rôle, mais à un compte normal, RBAC montre qu'il a été bien pensé et qu'il est souple et peut s'adapter aux diverses exigences de sécurité qu'on peut rencontrer avec un système généraliste comme Solaris.

L'association d'un profil à un compte normal s'effectuera lors de la déclaration initiale de ce compte avec la commande `useradd` ou ultérieurement en utilisant la commande `rolemod`. Là encore, il est nécessaire que l'utilisateur n'ait pas une session ouverte. Les exemples qui suivent ont été testé sous Solaris 9 x86.

```
# usermod -P "Printer Management" paulo
```

Ou ce qui est équivalent :

```
# usermod -K profiles='Printer Management' paulo
```

Cette commande aura pour effet d'ajouter ou de modifier dans le fichier `/etc/user_attr` les données relatives à l'utilisateur `paulo` qui deviendront :

::/0	Adresse par défaut
::/128	Adresse « non spécifiée » – est parfois utilisée comme source de certains paquets ICMPv6
::1/128	Adresse de loopback
::FFFF::/96	Adresses IPv4 mappées en IPv6 – utilisées en 6PE/6VPE
2001:0000::/32	Préfixe de service Teredo – mécanisme de transition
2002::/16	Préfixe de service 6to4 – mécanisme de transition
3FFE::/16	Ancienne expérimentation du 6bone
2001:DB8::/32	Non routable – réservé pour la documentation

Tableau 1 : Préfixes unicast particuliers (extrait de http://www.iana.org/assignments/ipv6-unicast-address-assignments)

a été récemment plus ou moins validée en février 2008 lorsque l'AS de Pakistan Telecom a annoncé un préfixe /24 contenant les serveurs de Youtube (qui lui annonce entre autres un /22 pour ses serveurs). Les routeurs disposant de deux routes vers la même destination choisissent toujours la plus spécifique, soit ici le /24. Cette annonce plus spécifique ayant été propagée sur l'Internet, l'AS pakistanais a ainsi attiré le trafic à destination de Youtube pendant quelques heures pour la quasi-totalité des clients. Youtube a bien tenté d'annoncer deux /25 recouvrant le /24 pour remédier à ce détournement de trafic, mais ces préfixes trop longs sont filtrés par la plupart des AS. Le *hijack* ne s'est arrêté que lorsque les routes envoyées par Pakistan Telecom ont été supprimées par son propre *provider*. Attention, il n'est toutefois pas recommandé d'annoncer une multitude de /24 sous prétexte de sécurité : en effet, de nombreux opérateurs pourraient choisir de les filtrer et ces /24 sont alors invisibles.

La désagrégation ayant de profonds impacts sur les routeurs en général (mémoire, CPU, temps de convergence), les annonces risquent d'être plus sévèrement filtrées en IPv6. Il faudra alors s'attendre à ce que les adresses IPv6 internes au réseau (*loopback*, management, liens) soient annoncées sur l'Internet, car dans le préfixe alloué à l'entité.

Si en IPv4 il est également fréquent d'utiliser d'autres plages non routables dans le cœur, telles que les adresses privées RFC1918 (10.0.0.0/8, 172.16.0.0/16 et 192.168.0.0/16), il a fallu redéfinir un équivalent d'adresses privées en IPv6 **[RFC4193]** : les adresses ULA (*Unique Local Address*), incluses dans la plage FC00::/7. Elles ne doivent pas être routables sur l'Internet, mais sont censées être routables sur un « site » (ou un AS ou un ensemble d'AS ayant des accords) et avoir un préfixe unique sur Internet ou tout du moins avec une forte probabilité d'unicité. En effet, l'identifiant de réseau d'une longueur de 40 octets doit être généré pseudo-aléatoirement ; il est même possible d'enregistrer son préfixe pour éviter qu'une autre entité ne l'utilise. Ainsi, si une adresse ULA devient visible sur l'Internet suite à une erreur, il ne devrait pas y avoir de conflit avec une autre ULA. Ces adresses sont donc tout indiquées pour remplacer les adresses privées IPv4 (qui elles n'étaient pas uniques et donc délicates à gérer en cas de fusion de réseaux) et sont utilisables sur le cœur ou encore à l'accès plutôt que les adresses unicast provenant du préfixe alloué/affecté par le RIR/LIR.

2.3 Génération des filtres de routage génériques

L'espace des adresses unicast globales attribuées à l'IANA est 2000::/3. Elles ne sont pas encore toutes allouées. Les préfixes unicast particuliers sont notamment : voir tableau 1.

D'autre part, les préfixes multicast sont dans le bloc FF00::/8. 2001:10::/28 est réservé pour les adresses ORCHID (*Overlay Routable Cryptographic Hash Identifiers*). Ce bloc est non-routable **[RFC4843]**, de même que FE00::/9 est réservé par l'IETF **[RFC4193]**, et, comme indiqué précédemment, les ULA sont en FC00::/8. Avec ces informations, il est possible de générer des filtres de type « *bogon/martians* » minimalistes listant les préfixes à refuser sur les sessions eBGP avec des *peers* externes :

Pour Cisco :

```
ipv6 prefix-list EBGP-V6 deny <préfixe-entité> le 128
ipv6 prefix-list EBGP-V6 deny 3ffe::/16 le 128
ipv6 prefix-list EBGP-V6 deny 2001:db8::/32 le 128
ipv6 prefix-list EBGP-V6 deny 2001:10::/28 le 128
ipv6 prefix-list EBGP-V6 deny 0000::/8 le 128
ipv6 prefix-list EBGP-V6 deny fc00::/8 le 128
ipv6 prefix-list EBGP-V6 deny fe00::/9 le 128
ipv6 prefix-list EBGP-V6 deny ff00::/8 le 128
ipv6 prefix-list EBGP-V6 permit any
```

Ou pour Juniper :

```
policy-statement EBGP-V6 {
  from {
      family inet6;
      route-filter <préfixe-entité> orlonger;
      route-filter 3ffe::/16 orlonger;
      route-filter ::/8 orlonger;
      route-filter 2001:db8::/32 orlonger;
      route-filter 2001:10::/28 orlonger;
      route-filter fc00::/8 orlonger;
      route-filter fe00::/9 orlonger;
      route-filter ff00::/8 orlonger;
      route-filter ::/0 upto /48 next policy;
  }
  then reject;
}
```

On refuse bien sûr son propre préfixe (préfixe-entité).

Mais, les préfixes IPv6 déjà alloués étant peu nombreux, des listes plus précises sont utilisables pour ne pas se contenter

6. Définir des nouveaux profils

Plutôt que d'utiliser des profils prédéfinis qui ne sont pas forcément adaptés à ce qu'on veut faire, et de les associer à un rôle, nous allons définir 2 nouveaux profils appelés SHUTDOWN et VOLMGT. Sur un poste de travail, ce genre d'amélioration rendra le quotidien plus agréable et permettra d'éviter l'utilisation de la commande su pour lancer l'arrêt. Pour définir un nouveau profil, il est nécessaire de le déclarer dans 2 fichiers. À l'aide de l'éditeur favori, on rajoutera pour commencer ces quelques lignes dans le fichier de définition des profils /etc/security/exec_attr :

```
SHUTDOWN:suser:cmd:::/usr/sbin/halt:euid=0
SHUTDOWN:suser:cmd:::/usr/sbin/init:euid=0
SHUTDOWN:suser:cmd:::/usr/sbin/poweroff:uid=0
SHUTDOWN:suser:cmd:::/usr/sbin/reboot:uid=0
VOLMGT:suser:cmd:::/etc/init.d/volmgt:uid=0;gid=sys
```

Puis, on fera de même dans le fichier /etc/security/prof_attr :

```
SHUTDOWN:::Halt or Restart the system:
VOLMGT:::Stop, Start vold:
```

En attribuant ces profils à un compte utilisateur, celui-ci pourra arrêter son poste de travail par :

```
$ pfexec /usr/sbin/poweroff
```

Ou bien relancer le gestionnaire de volume vold comme cela peut parfois être nécessaire avec certaines clés USB.

```
$ pfexec /etc/init.d/volmgt stop
$ pfexec /etc/init.d/volmgt start
```

Les lecteurs attentifs auront remarqué dans l'extrait du fichier de définition des profils, présenté en début d'article, la présence de la ligne suivante :

```
Primary Administrator:suser:cmd:::*:uid=0;gid=0
```

Cette ligne définit le profil d'exécution Primary Administrator et le caractère * dans le champ commande associé à uid=;gid=0 indique que l'utilisateur à qui on affectera ce profil pourra exécuter toutes les commandes en prenant un uid et un gid réel égal à 0 donc avec tous les privilèges. Il pourra donc faire toutes les opérations d'administration courantes en utilisant la commande pfexec.

```
$ pfexec /usr/bin/vi /etc/hosts
```

Associer le profil Primary Administrator à un compte utilisateur normal est déconseillé et on évitera de le faire pour tout environnement dans lequel un niveau de sécurité élevé est requis.

7. Transformer root en un compte rôle

Transformer root en compte rôle permet de rendre obligatoire l'utilisation de la commande su pour prendre l'identité de root. Notons que, sous Solaris, les valeurs par défaut du fichier de configuration /etc/default/login rendent déjà cette pratique obligatoire et il est interdit d'ouvrir directement une session root autrement que depuis la console système (/dev/console). De ce fait, cette opération présente un caractère le plus souvent superflu. Décrivons-la néanmoins.

Un préalable consiste à autoriser les utilisateurs ayant le droit d'endosser le rôle root avec la commande su en étant bien conscient qu'il faut en autoriser au moins un :

```
# usermod -R root paulo
# usermod -R root sysadm
```

Il faut ensuite indiquer que root est un rôle en éditant le fichier /etc/user_attr et en changeant la ligne :

```
root::::auths=solaris.*,solaris.grant;profiles=All
```

par :

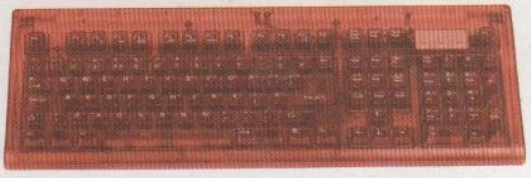
```
root::::type=role;auths=solaris.*,solaris.grant;profiles=All
```

On peut obtenir le même résultat avec cette commande :

```
# usermod -K type=role root
```

Notons que l'opération inverse consistant à rétablir root comme un compte privilégié « normal » sera effectuée non pas avec la commande usermod puisque root est devenu un rôle, mais avec la commande rolemod suivante :

```
# rolemod -K type=normal root
```



8. Les autorisations

Nous n'avons pas encore complètement exploré RBAC et nous allons voir qu'il y existe encore d'autres points à dévoiler. En effet, nous n'avons pas encore parlé de la commande `auths` qui permet d'afficher les autorisations potentiellement accordées à un utilisateur. Ces autorisations sont utilisées par certaines commandes pour déterminer si un utilisateur à l'autorisation d'exécuter la commande en question.

L'ensemble des autorisations possibles – une bonne centaine – sont décrites par des noms complètement qualifiés (identifiant si possible l'organisme qui les a définies) dans le fichier des autorisations `/etc/security/auth_attr` dont voici un court extrait :

```
solaris.admin.printer.:::Printer Information::help=AuthPrinterHeader.html
solaris.admin.printer.read:::View Printer Information::help=AuthPrinterRead.html
solaris.admin.printer.modify:::Update Printer
solaris.admin.printer.delete:::Delete Printer
solaris.device.cdrw:::CD-R/RW Recording Authorizations::help=DevCDRW.html
solaris.jobs.grant:::Delegate Cron & At Administration::help=JobsGrant.html
solaris.mail.mailq:::Mail Queue::help=MailQueue.html
...
```

Les autorisations par défaut accordées à un utilisateur sont celles indiquées dans le fichier `/etc/security/policy.conf`. Elles s'appliquent à tous les utilisateurs. Elles sont complétées spécifiquement par utilisateur à l'aide des indications contenues dans le fichier `/etc/user_attr`. En l'absence de directives particulières, un utilisateur est créé avec les autorisations par défaut définies par les 2 lignes suivantes du fichier `/etc/security/policy.conf`.

```
AUTHS_GRANTED=solaris.device.cdrw
PROFS_GRANTED=Basic Solaris User
```

Si `AUTHS_GRANTED` définit directement une autorisation, `PROFS_GRANTED` agit par indirection en allant voir dans le fichier `/etc/security/prof_attr` la liste des autorisations correspondant à `Basic Solaris User`.

Si nous utilisons la commande `auths` pour lister les autorisation accordées à root, nous voyons qu'il possède l'autorisation `solaris.*`, autrement dit que toutes les autorisations sont accordées à root :

```
$ auths root
solaris.*
```

Pour un utilisateur normal, nous avons une liste finie inférieure à la totalité des autorisations :

```
$ auths paulo
solaris.device.cdrw,solaris.profmgr.read,solaris.jobs.users,solaris.mail.
mailq,solaris.admin.usermgr.read,solaris.admin.logsvc.read,solaris.admin.
fsmgr.read,solaris.admin.serialmgr.read,solaris.admin.diskmgr.read,solaris.
admin.procmgr.user,solaris.compsys.read,solaris.admin.printer.read,solaris.
admin.prodreg.read,solaris.admin.dcmgr.read,solaris.snmp.read,solaris.project.
read,solaris.admin.patchmgr.read,solaris.network.hosts.read,solaris.admin.
volmgr.read
```

On pourra utiliser ce petit script pour obtenir un affichage bi-colonne plus lisible :

```
$ for a in $(auths | tr , ' ')
> do
> print $a
> done | pr -2 -t -11
```

solaris.device.cdrw	graver des CD
solaris.profmgr.read	Lire les profils
solaris.jobs.users	Gérer des travaux avec at et cron
solaris.mail.mailq	Utiliser la commande mailq
solaris.admin.volmgr.read	Lister les volumes logiques
solaris.admin.usermgr.read	Lister les utilisateurs et les rôles
solaris.admin.logsvc.read	Examiner les fichiers de log
solaris.admin.fsmgr.read	Lister les points de montage et les partages NFS
solaris.admin.serialmgr.read	Lister les ports série
solaris.admin.diskmgr.read	Lister les disques
solaris.admin.procmgr.user	Gérer ses propres processus
solaris.compsys.read	Lister l'information de l'équipement
solaris.admin.printer.read	Lister l'information au sujet des imprimantes
solaris.admin.dcmgr.read	Lister services et patchs des clients sans disques
solaris.snmp.read	Lire l'information SNMP
solaris.project.read	Lister les projets
solaris.admin.patchmgr.read	Lister les patchs
solaris.network.hosts.read	Lister les équipements et les réseaux

Tableau 1 : Liste des autorisations

On accordera une autorisation supplémentaire à un compte normal ou rôle en utilisant la commande `usermod`. Par exemple :

```
# usermod -A solaris.system.shutdown paulo
```

Ou ce qui est strictement identique :

```
# usermod -K auths=solaris.system.shutdown paulo
```

Elle se traduit par l'ajout dans `/etc/user_attr` de :

```
paulo::::type=normal;auths=solaris.system.shutdown;roles=operator
# auths
solaris.system.shutdown,solaris.device.cdrw,solaris.profmgr.read,solaris.
jobs.users,solaris.mail.mailq,solaris.admin.volmgr.read,solaris.admin.usermgr.
read,solaris.admin.logsvc.read,solaris.admin.fsmgr.read,solaris.admin.serialmgr.
read,solaris.admin.diskmgr.read,solaris.admin.procmgr.user,solaris.compsys.
read,solaris.admin.printer.read,solaris.admin.prodreg.read,solaris.admin.dcmgr.
read,solaris.snmp.read,solaris.project.read,solaris.admin.patchmgr.read,solaris.
network.hosts.read
```

9. Le fichier /etc/security/policy.conf

Ce fichier détermine le profil par défaut pour les utilisateurs, les autorisations supplémentaires accordées et l'algorithme de chiffrement utilisé pour le mot de passe (voir code ci-contre).

On voit que la seule autorisation supplémentaire accordée en complément aux autorisations fournies via le profil `Basic Solaris User` est `solaris.device.cdrw`. Elle permet tout simplement d'autoriser les utilisateurs à graver des CD avec la commande `cdrw` sans qu'il soit utile d'être root.

```
AUTHS_GRANTED=solaris.device.cdrw
PROFS_GRANTED=Basic Solaris User
CRYPT_ALGORITHMS_ALLOW=1,2a,md5
#CRYPT_ALGORITHMS_DEPRECATE=__unix__
CRYPT_DEFAULT=__unix__
```

10. Le fichier /etc/user_attr

Ce fichier contient les autorisations spécifiques accordées aux utilisateurs. Sur un système Solaris 10 venant d'être installé, on ne dénombre que 3 comptes privilégiés et root. Il sera complété chaque fois qu'on attribuera un rôle, un profil ou une autorisation.

Concernant root, on remarque que l'autorisation `solaris.grant` vient compléter `solaris.*`. Cette particularité indique que root possède l'autorisation d'accorder aux autres utilisateurs toute autorisation qu'il possède lui-même.

```
adm::::profiles=Log Management
lp::::profiles=Printer Management
postgres::::type=role;profiles=Postgres Administration,All
root::::auths=solaris.*,solaris.grant;profiles=Web Console Management,All;lock_after_retries=no;min_label=admin_low;clearance=admin_high
```

11. Le fichier /etc/security/prof_attr

Cet extrait montre la définition des autorisations accordées à l'utilisateur de base et la définition du profil `Printer Management` : voir code ci-dessous.

On voit donc que l'attribution d'un profil supplémentaire que ce soit pour un compte normal ou pour un compte rôle permet non seulement d'associer au moyen du fichier `exec_attr` de définir un certain nombre de commandes qui seront exécutées avec des privilèges supérieurs à ceux de l'utilisateur, mais aussi que le fichier `prof_attr` associe zéro, une ou plusieurs autorisations supplémentaires. Dans le cas du profil `Printer Management`, ces autorisations sont au nombre de 3.

```
All:::Execute any command as the user or role:help=RtAll.html

Basic Solaris User:::Automatically assigned rights:auths=solaris.profmgr.read,solaris.jobs.users,solaris.mail.mailq,solaris.admin.volmgr.read,solaris.admin.usermgr.
read,solaris.admin.logsvc.read,solaris.admin.fsmgr.read,solaris.admin.serialmgr.read,solaris.admin.diskmgr.read,solaris.admin.procmgr.user,solaris.compsys.read,solaris.
admin.printer.read,solaris.admin.prodreg.read,solaris.admin.dcmgr.read,solaris.snmp.read,solaris.project.read,solaris.admin.patchmgr.read,,solaris.network.hosts.read;prof
iles=All;help=RtDefaul
t.html
Printer Management:::Manage printers, daemons, spooling:help=RtPrntAdmin.html;auths=solaris.admin.printer.read,solaris.admin.printer.modify,solaris.admin.printer.delete
```

12. Le contrôle des autorisations

Il faut bien comprendre que les autorisations sont un contrôle supplémentaire permettant de renforcer la sécurité en particulier celle des commandes suid root considérées comme dangereuses. L'autorisation ne donne pas des droits supplémentaires. Elle permet simplement de limiter, par codage, plus finement les droits accordés par d'autres mécanismes, comme les permissions ou le changement d'identificateur par commande suid ou profil interposé. Les autorisations permettent

donc de limiter l'usage de certaines commandes aux seuls utilisateurs autorisés.

C'est la commande elle-même qui va effectuer le contrôle en utilisant la fonction `chkauthattr`. Cette fonction permet de s'assurer que l'utilisateur qui exécute une commande possède bien les droits exigés par cette commande.

Nous avons vu que l'autorisation `solaris.device.cdrw` est globalement accordée à tous les utilisateurs, ce qui leur permet d'utiliser la commande `cdrw` pour graver des CD et DVD. Si l'on retire l'autorisation globale, alors aucun utilisateur, à l'exception de root, ne pourra plus graver de CD. Dans l'extrait de code assurant ce contrôle, la macro-définition `CDRW_AUTH` correspond à l'autorisation `solaris.device.cdrw`.

(voir code ci-contre)

Des contrôles similaires peuvent être effectués dans une procédure shell en utilisant la commande `auths`.

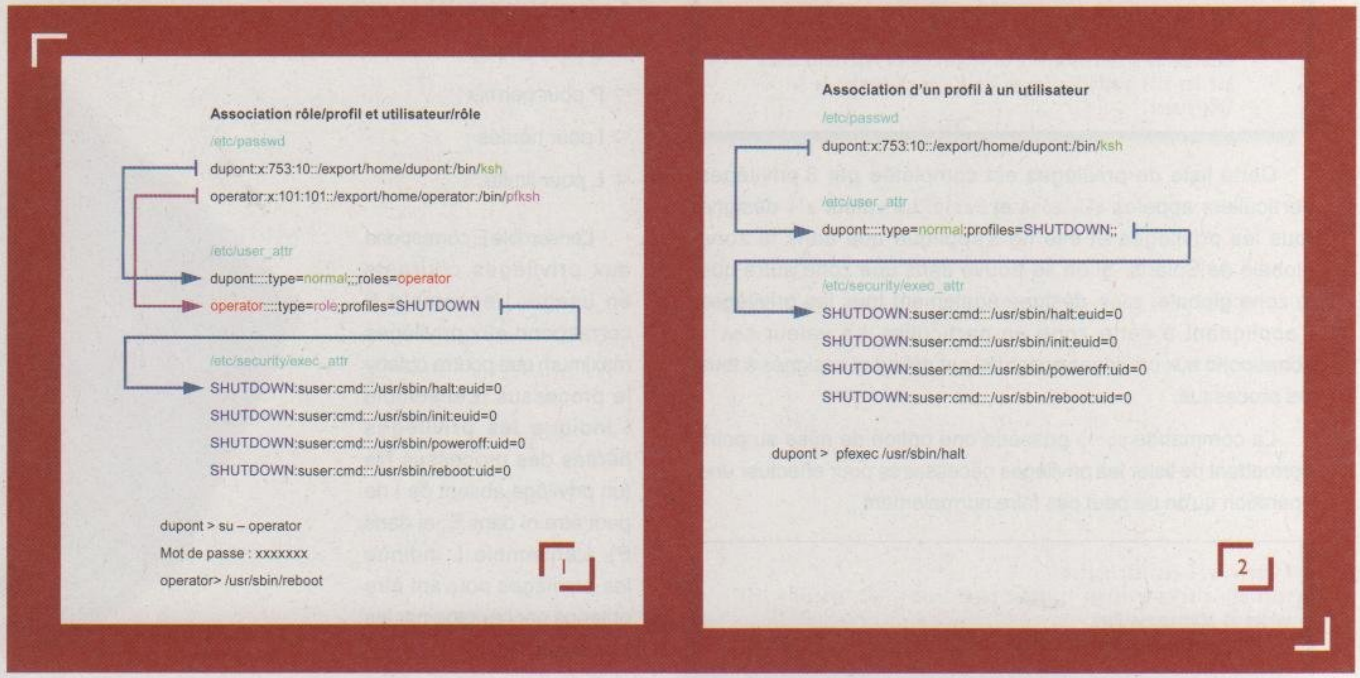
```
#include <auth_attr.h>
#include <auth_list.h>

...
int check_auth(uid_t uid)
{
    struct passwd *pw;
    pw = getpwuid(uid);

    if (pw == NULL) {
        return (0);      // Erreur inconnu dans /etc/passwd
    }
    // L'utilisateur possède t-il l'autorisation CDRW_AUTH
    if (chkauthattr(CDRW_AUTH, pw->pw_name) != 1) {
        return (0);      // Erreur pas le droit
    } else {
        return (1);      // OK
    }
}

...

ruid = getuid();
cur_uid = geteuid();

if (check_auth(ruid) != 1)  {
     err_msg(gettext("Authorization failed, Cannot access disks.\n"));
     exit(1);
}
```

13. En résumé

Un profil associé à un rôle est endossé en utilisant la commande `su` pour se rendre dans le rôle. C'est l'un des shells spéciaux `pfsh`, `pfcsh`, `pfksh` obligatoirement associé à un compte rôle qui permet sa prise en compte. Un profil directement associé à un utilisateur est endossé par l'intermédiaire de la commande `pfexec`.

Une autorisation est acquise sans mesure particulière (soit par le rôle, soit par l'utilisateur). La figure 1 montre des exemples de relations entre utilisateur, rôle et profil.

La figure 2 montre les relations entre utilisateurs et profil.



14. Les privilèges

Jusqu'à Solaris 9, RBAC est implanté au niveau « *userland* » et il offre des fonctionnalités sensiblement identiques à celles autorisées par le célèbre logiciel `sudo`. Avec Solaris 10, apparaît la notion de privilèges implantés au niveau « *kernel* » et associés à RBAC. Ces privilèges au nombre de 68 dans Solaris 10 sont 71 dans OpenSolaris. Leur implantation dans le noyau permet d'outrepasser par exemple le schéma traditionnel uid/gid/permissions et d'accéder à des fichiers par le biais des privilèges, même si les permissions ne le permettent pas.

L'ensemble des privilèges disponibles seront listés avec la commande `ppriv`.

```
$ ppriv -l | pr -4 -t
contract_event    graphics_access   proc_owner        sys_res_config
contract_observer graphics_map      proc_priocntl     sys_resource
cpc_cpu           ipc_dac_read      proc_session      sys_suser_compat
dtrace_kernel     ipc_dac_write     proc_setid        sys_time
dtrace_proc       ipc_owner         proc_taskid       sys_trans_label
dtrace_user       net_bindmlp       proc_zone         win_colormap
file_chown        net_icmpaccess    sys_acct          win_config
file_chown_self   net_mac_aware     sys_admin         win_dac_read
file_dac_execute  net_privaddr      sys_audit         win_dac_write
file_dac_read     net_rawaccess     sys_config        win_devices
file_dac_search   proc_audit        sys_devices       win_dga
file_dac_write    proc_chroot       sys_ipc_config    win_downgrade_sl
file_downgrade_sl proc_clock_highre sys_linkdir       win_fontpath
file_link_any     proc_exec         sys_mount         win_mac_read
file_owner        proc_fork         sys_ip_config     win_mac_write
file_setid        proc_info         sys_net_config    win_selection
file_upgrade_sl   proc_lock_memory  sys_nfs           win_upgrade_sl
```

L'option `-v` permet d'obtenir une description précise des privilèges :

```
$ ppriv -lv file_dac_read
file_dac_read
        Autorise un processus à lire un fichier ou un répertoire alors
        que les bits d'autorisation ou les ACL de ce dernier le lui
        interdisent.
```

Cette liste de privilèges est complétée par 3 privilèges particuliers appelés `all`, `zone` et `basic`. La valeur `all` désigne tous les privilèges et elle ne s'applique que dans la zone globale de Solaris. Si on se trouve dans une zone autre que la zone globale, `zone` désigne également tous les privilèges s'appliquant à cette zone en particulier. La valeur `basic` correspond aux privilèges accordés par défaut et assignés à tous les processus.

La commande `ppriv` possède une option de mise au point permettant de lister les privilèges nécessaires pour effectuer une opération qu'on ne peut pas faire normalement :

```
$  ppriv -e -D cat /etc/shadow
cat[6789]: missing privilege "file_dac_read" (euid = 7543, syscall = 225)
needed at ufs_iaccess+0xd2
cat : impossible d'ouvrir /etc/shadow
```

Si on ajoute le privilège `file_dac_read` à un compte normal ou à un rôle, il pourra alors lire tous les fichiers.

```
$ ppriv $$
4350:   -ksh93
flags = <none>
        E: basic
        I: basic
        P: basic
        L: all
$ su -
...
# usermod -K defaultpriv=basic,file_dac_read paulo
UX: usermod: paulo is currently logged in, some changes may not take effect
until next login.
```

Cela se traduit bien évidemment par l'ajout du privilège dans le fichier `/etc/user_attr` et, après ouverture d'une nouvelle session, on a :

```
$ ppriv $$
4380:   -ksh93
flags = <none>
        E: basic,file_dac_read
        I: basic,file_dac_read
        P: basic,file_dac_read
        L: all
```

Le retour à la normale sera effectué par exemple par :

```
# usermod -K defaultpriv="" paulo
```

Pour faciliter les choses, les privilèges sont groupés selon 4 ensembles appelés :

- **E** pour effectif ;
- **P** pour permis ;
- **I** pour hérités ;
- **L** pour limité.

L'ensemble E correspond aux privilèges courants en usage. L'ensemble P correspond aux privilèges maximum que pourra obtenir le processus. L'ensemble I indique les privilèges hérités des processus fils (un privilège absent de I ne peut être ni dans E, ni dans P). L'ensemble L indique les privilèges pouvant être obtenus par héritage par les processus fils.

15. Applications

RBAC permet de créer assez facilement des rôles ou d'attribuer des profils d'exécution qui permettront de déléguer les tâches administratives liées aux diverses applications. On pourra, moyennant un petit effort, créer des profils d'exécution tels que `Oracle Manager`, `Web Manager`, `Mail Manager`, etc. et séparer de manière étanche l'aspect administration système, réseau, et sécurité des applications.

Conclusion

Avec Solaris 8, a commencé un processus permettant de s'affranchir progressivement du modèle super-user Unix du tout ou rien. Avec l'introduction des privilèges dans Solaris 10, on abandonne ce modèle tout en maintenant la compatibilité ascendante. L'attribution de profil(s) permet de définir des utilisateurs privilégiés sur mesure avec un degré de finesse adapté à des exigences de sécurité variées.

On prendra garde à définir les rôles et les profils avec le plus grand soin et au fait que RBAC n'est pas d'un point de vue fonctionnel totalement stabilisé et qu'il est encore l'objet de modifications significatives. L'attribution directe de profils à un utilisateur sera réservée aux administrateurs système confirmés, car elle exige une analyse détaillée des implications possibles en termes de sécurité. L'utilisation de RBAC dans le monde Solaris n'est pas encore très répandue et si cet article facilite son utilisation et son adoption, il aura atteint son objectif.

Références

- *Solaris 10 System Administration Guide : Security Services Part III : Roles, Rights Profiles, and Privileges*
- Pages du manuel Solaris des commandes RBAC citées dans cet article.
- BRUNETTE (Gleen), « *Restricting Service Administration in the Solaris 10 Operating System* », Sun *BluePrints Online*, juin 2005.
- BRUNETTE (Gleen) & MOFFAT (Darren), « *Privilege Debugging in the Solaris 10 Operating System* », *BluePrints Online*, février 2006.

nidhal.ben-aloui@dcnsgroup.com

LA BIOMÉTRIE : SOLUTION OU ILLUSION ?

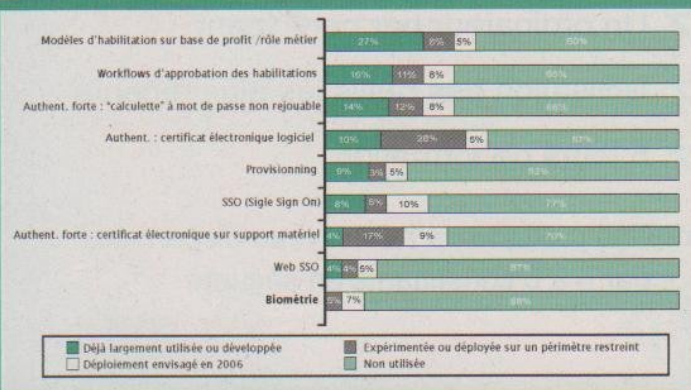
mots clés : *contrôle / identité / authentification*

Cet article présente un état de l'art succinct des systèmes biométriques existants, ainsi que les enjeux qui résultent de tels systèmes de contrôle d'identité. Parmi les problématiques que nous pouvons citer : la révocabilité et la protection de la vie privée.

1. Introduction

La Sécurité des Systèmes d'Information (SSI) est devenue une priorité incontournable au sein des entreprises et des organisations de l'État. La SSI adresse en effet aussi bien la protection des secrets (aspect Confidentialité) de Défense ou industriels, que la protection contre la modification illicite (aspect Intégrité), ainsi que la continuité de service (aspect Disponibilité). Les enjeux sont primordiaux pour un grand nombre d'acteurs et la menace de plus en plus probante (cyberterrorisme, hacking, intelligence économique, etc.).

La politique de sécurité à mettre en place pour contrer les menaces est en général composée de deux facteurs :



Utilisation des techniques d'authentification (source CLUSIF 2007)

- les contre-mesures non techniques : composées des aspects physiques (zones réservées, sas d'accès, etc.), des aspects organisationnels (procédures de sécurité) et des aspects humains (enquête sur le personnel, etc.) ;
- les contre-mesures techniques : composées de multiples aspects dont l'authentification, le contrôle d'accès, le chiffrement, l'audit de sécurité,...

La reconnaissance[1] des utilisateurs dans un système d'information (que ce soit l'authentification d'accès à une zone ou une identification locale ou distante sur une machine) est la clé de voûte de toute politique de sécurité. Il existe trois façons de prouver son identité :

- ce que l'on possède : une carte, un badge, un *dongle* ;
- ce que l'on sait : un mot de passe, code par question/réponse ;
- ce que l'on est : la **biométrie** (empreinte, rétine, ADN, etc.).

Le schéma suivant résume les différentes techniques existantes pour reconnaître un utilisateur : voir figure 1.

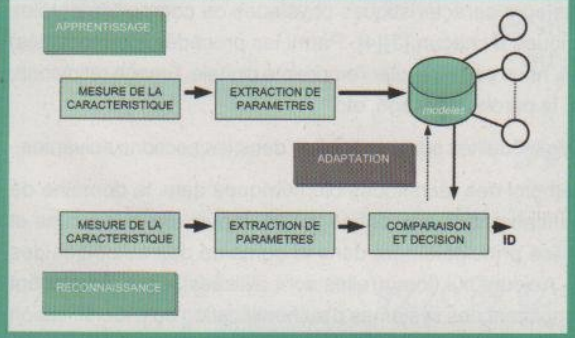
Nous présentons dans un premier temps les notions et terminologie associées à la biométrie. Ensuite, nous dressons un état de l'art des techniques biométriques existantes. Elles se divisent en deux grandes failles : invasives et non invasives. Enfin, nous concluons par les limitations et les perspectives que peuvent avoir de tels systèmes.

2. Notions et terminologie

Voici quelques terminologies utiles pour comprendre la suite de l'article :

- **Enrôlement** : désigne la phase d'enregistrement d'une donnée biométrique en phase d'apprentissage.
- **Gabarit** : désigne le fichier signature contenant l'empreinte biométrique.
- **Matching** : terme anglais pour désigner la tâche de reconnaissance entre deux empreintes digitales.
- **Vérification** : désigne la phase de capture de la donnée biométrique pour une reconnaissance d'un individu.
- **Modalité** : représente chacune des techniques biométriques : l'empreinte digitale, l'iris, etc.

Quelle que soit la technologie biométrique employée, le principe général de fonctionnement reste toujours le même :



2 *Architecture générale d'un système biométrique* **[1]**

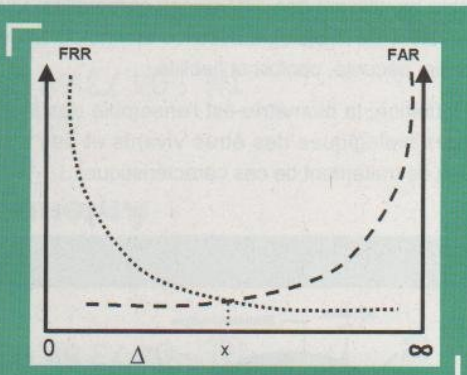
1. Capture de l'information à analyser (une image, un son ou une action) : c'est l'APPRENTISSAGE (phase d'enrôlement).
2. Traitement de l'information et création d'un fichier « signature » (éléments caractéristiques de l'image), puis mise en mémoire de ce fichier de référence appelé « modèle » (c'est le *gabarit*) sur un support (disque dur, carte à puce, code barre) : sauvegarde du MODELE.
3. Dans la phase de vérification, on procède comme pour la création du fichier « signature » de référence. Ensuite, on compare les deux fichiers pour déterminer leur taux de similitude et prendre la décision la plus pertinente : RECONNAISSANCE.
4. Il est parfois intéressant de réévaluer le modèle pour l'adapter à la variabilité des caractéristiques biométriques liées au temps (apparition de rides, vieillissement, etc.) : ADAPTATION, cette étape est facultative.

Il est difficile d'obtenir une coïncidence absolue (100% de similitude) entre le fichier signature créé lors de l'enrôlement et le fichier « signature » créé lors de la vérification.

Pour mesurer les performances d'un système biométrique, la communauté internationale s'est accordée sur les mesures suivantes :

- **TFR** (Taux de Faux Rejets) ou encore FRR[2] : représente le pourcentage de personnes rejetées par erreur par le système.
- **TFA** (Taux de Fausses Acceptations), également FAR[3] : représente le pourcentage d'acceptations qui n'auraient pas dû être retenues.
- **TEE** (Taux d'erreurs égales) ou encore FEE[4] : représente le pourcentage d'intersections entre le TFR et le TFA, (cf. Fig. 3 valeur x)
- **TEEr** (Taux d'erreur à l'enrôlement) ou encore FTE[5] : représente le pourcentage de personnes dont l'empreinte biométrique n'est pas capturable.

Si la reconnaissance d'une personne à partir de son propre modèle échoue, la personne est faussement rejetée. La probabilité que cet événement se produise est appelée « TFR » ou « FRR ». Plus le FRR est grand, plus le nombre de faux rejets augmente.



3 *Courbe de performances FAR et FRR*

Sur ce schéma, delta représente la marge d'erreurs autorisée par le système, variant de 0 à l'infini. Très succinctement, on voit que plus la marge d'erreurs autorisée est importante, plus le FAR augmente, c'est-à-dire que l'on va accepter de plus en plus de personnes qui ne sont pas autorisées (et donc la sécurité du système diminue).

En revanche, on voit que le taux de rejets des personnes autorisées diminue également, ce qui rend le système plus fonctionnel et répond mieux aux attentes des utilisateurs.

À l'autre extrémité, si l'on diminue la marge d'erreurs acceptée par le procédé de mesure biométrique, les tendances des 2 taux sont inversées.

On va de moins en moins accepter des individus essayant de frauder, mais on va aussi, par la même occasion, avoir un taux de rejets sur des personnes autorisées qui sera trop important pour être toléré dans la plupart des cas. Le compromis habituel est de prendre la jonction des courbes, c'est-à-dire le point x où les deux valeurs FAR et FRR sont minimales.

Enfin, lorsqu'une nouvelle personne doit être enrôlée dans un système biométrique et que cette opération n'est pas possible, on parle d'échec d'enrôlement (« *failure to enroll* ») ou FTE. Le FTE indique généralement la probabilité que quelqu'un ne puisse pas être enrôlé dans un système. Par exemple, brûlure au visage, amputation de doigts, iridocyclite sont des cas extrêmement rares.

Pour tester la robustesse des systèmes biométriques, il existe de nombreuses campagnes d'évaluations :

- La campagne ESTER[6] : pour la reconnaissance du locuteur et de la parole en France.
- La campagne du NIST[7] : établissement américain pour l'évaluation des performances des systèmes biométriques uni et multimodaux.
- Biosecure : réseau d'excellence et d'évaluation européen.
- etc.

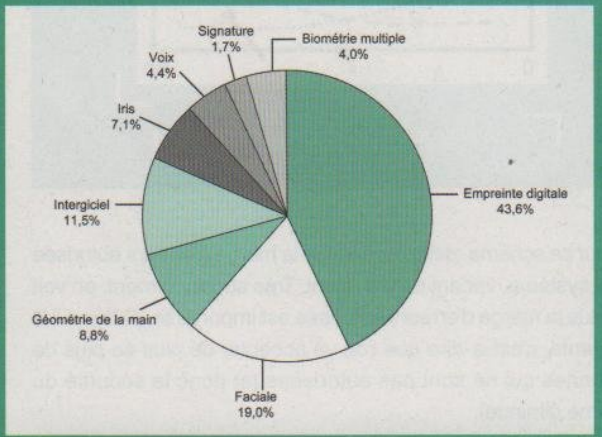
Passons au vif du sujet.

3. État de l'art technologique

Au XIXe siècle, vers 1880, Alphonse Bertillon invente la police scientifique qui répond à la nécessité de s'assurer de la manière la plus irréfutable possible de l'identité des criminels pour les confondre. Il utilise alors le relevé métrique de certains caractères anatomiques pour décrire les criminels afin de les retrouver en cas de récidive.

La biométrie est une technique très moderne qui répond à la préoccupation très ancienne de prouver son identité de manière indiscutable en utilisant des différences corporelles. Elle marie les découvertes de la biologie avec les technologies de pointe pour concilier sécurité, confort et fiabilité.

Par définition, la biométrie est l'ensemble des techniques de mesures biologiques des êtres vivants et des méthodes statistiques de traitement de ces caractéristiques.



4 *Marché de la biométrie par technologie en %, année 2006*

Dans le domaine de l'identification des personnes, la biométrie utilise l'informatique pour identifier ou authentifier la mesure d'une ou plusieurs caractéristiques physiques ou comportementales spécifiques à chacun [3][4]. Parmi les procédés (ou modalités) utilisés, nous pouvons citer l'empreinte digitale, l'image rétinienne, l'ADN, la parole, le visage, etc.

Ces modalités sont expliquées dans les sections suivantes.

L'emploi des techniques biométriques dans le domaine de l'identification des personnes existe depuis des décennies et est utilisé principalement dans le domaine des autopsies des corps. Aujourd'hui (lorsqu'elles sont utilisées), elles remplacent ou complètent des systèmes d'authentification ou d'identification classiques. Par exemple : protection par mot de passe, par carte à puce, ou contrôle d'accès à des zones sensibles. Certaines de ces techniques, via des capteurs électroniques, protégent l'accès à des fichiers informatiques ou à des bâtiments. Il suffit en général de quelques millisecondes au maximum pour mesurer une caractéristique corporelle, telle qu'une empreinte digitale, la voix d'un individu ou encore le morphisme de l'iris de l'œil, et s'assurer qu'elle appartient bien à la personne qui demande l'accès aux zones ou aux documents protégés. Ces systèmes biométriques prennent tout leur sens lorsqu'ils sont couplés avec une politique de sécurité cohérente et robuste.

On distingue deux grandes familles de techniques biométriques : les méthodes dites « invasives » et les méthodes « non invasives ».

Techniques biométriques invasives

L'ADN, l'iris et la rétine sont dites des « modalités biométriques invasives », car l'acquisition de la signature numérique d'un individu nécessite un capteur pénétrant l'anatomie du corps humain (exemple : un faisceau laser pour la rétine). Ce genre de techniques est souvent mal accepté par les usagers, car il n'existe pas assez d'études faites sur le sujet.

Techniques biométriques non invasives

L'empreinte digitale, la reconnaissance faciale, la géométrie de la main, la reconnaissance vocale etc. sont dites « non invasives ». Le capteur se contente de relever une caractéristique prélevée à la surface d'un organe du corps (l'empreinte du doigt) ou dans un voisinage très proche (la voix) (voir figure 4).

Nous présentons ci-après les modalités biométriques les plus utilisées du commerce, ainsi que les plus exotiques.

3.1 La reconnaissance d'empreintes digitales

L'utilisation d'empreintes digitales comme caractère biométrique est à la fois le plus vieux mode de reconnaissance assisté par ordinateur et le plus utilisé actuellement. Un ensemble de facteurs favorisent la démocratisation des empreintes digitales sur le marché de l'authentification/identification des personnes.

Ces facteurs sont :

- la petite taille et le faible coût des dispositifs de capture ;
- la grande capacité de calcul des matériels informatiques ;
- le taux et la vitesse d'identification satisfaisant les besoins des applications ;
- la croissance explosive des réseaux et des transactions sur Internet ;
- la prise de conscience du besoin de facilité d'utilisation ;
- la bonne acceptation par les utilisateurs.

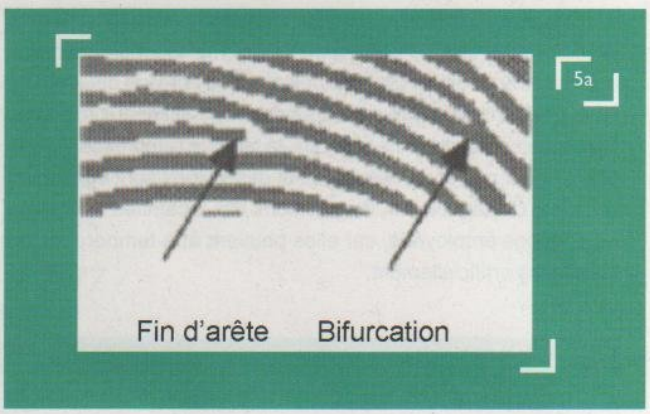
Au milieu du 17ème siècle des études scientifiques ont établi deux caractéristiques sur les empreintes digitales qui sont toujours vraies de nos jours :

- deux empreintes digitales de doigts différents n'auront jamais le même schéma d'arêtes[8] ;
- les schémas d'arêtes d'une empreinte digitale restent inchangés à vie.

3.1.1 Types de caractères

Les lignes qui décrivent différents schémas sur les empreintes digitales sont appelées « arêtes » et les espaces entre les arêtes sont les « vallées ». Ce sont les arêtes qui sont comparées entre une empreinte digitale et une autre lors de la recherche de correspondance. Les empreintes digitales sont généralement mises en correspondance via une ou deux approches. L'approche la plus microscopique est la recherche de minuties[9].

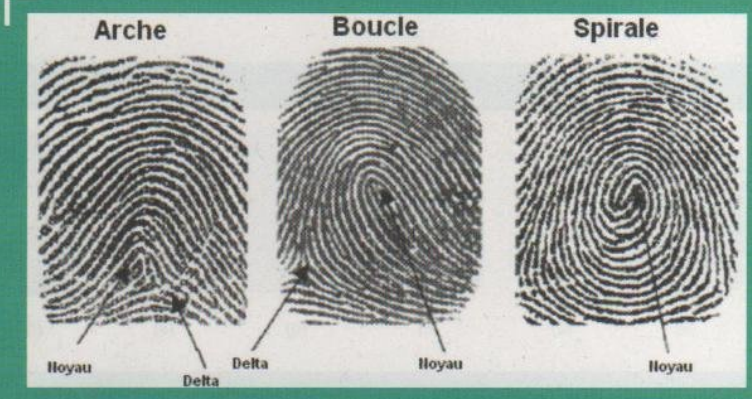
Les deux types de minuties montrées sur l'image ci-dessous sont la fin d'une arête et la bifurcation. Une fin d'arête est l'endroit où l'arête se termine.



Une bifurcation est l'endroit où une arête se divise en deux arêtes à une jonction en forme de Y. Dans le but de rechercher des correspondances, une minutie est associée à d'autres caractères comme la position (x, y) et la direction (d'autres approches utilisent des caractères supplémentaires) (voir figure 5a).

L'approche la plus macroscopique est la recherche de schémas. Dans cette approche, le chemin décrit par les arêtes est comparé à chaque endroit entre deux images d'empreintes digitales. Le dessin des arêtes constitue le schéma global de l'empreinte digitale. L'image ci-dessous présente les trois schémas de références d'empreinte digitale les plus utilisés (on utilise jusqu'à 10 schémas différents).

Deux autres caractéristiques sont parfois utilisées pour la recherche de correspondance : le noyau et le delta (cf. Figure 5b). Le noyau peut être vu comme le centre du schéma de l'empreinte digitale [11][12]. Le delta est le point particulier à partir duquel deux schémas dérivent. Les emplacements de noyaux et de deltas sont utilisés comme points de repère grâce auxquels on peut orienter deux empreintes digitales pour une recherche de correspondance. Cependant, ces caractéristiques ne sont pas présentes sur toutes les empreintes digitales (voir figure 5b).



5b *Différentes minuties sur une empreinte*

D'autres caractéristiques d'empreintes digitales sont utilisées pour la recherche de correspondance. Par exemple, certains capteurs d'empreintes digitales détectent les pores et déterminent leurs positions pour une correspondance similaire aux minuties. Bien qu'elles varient dans le temps, la taille de l'empreinte digitale et la largeur moyenne des arêtes et des vallées sont également utilisées. Généralement, les positions des cicatrices et des plis ne sont pas employées, car elles peuvent être temporaires ou introduites artificiellement.

3.1.2 Traitement de l'image

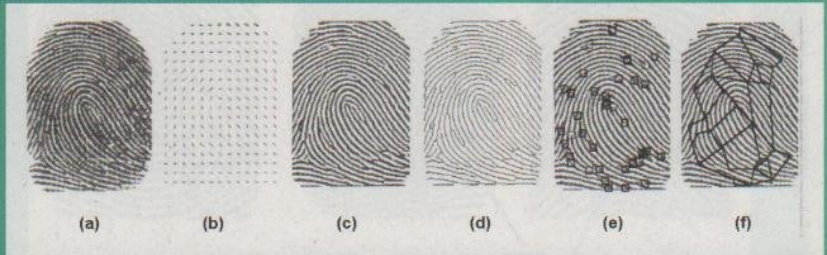
Après la capture, on obtient une image de l'empreinte digitale, que l'on traite. L'objectif final du traitement de l'image est d'obtenir la meilleure image possible grâce à laquelle la bonne correspondance est trouvée. Les étapes du traitement de l'image sont la réduction du bruit et l'amélioration de la qualité, la détection de caractéristiques et l'élimination de fausses correspondances.

3.1.2.1 Amélioration de la qualité de l'image

Une image d'empreinte digitale est un des types d'images les plus bruités. Cela est dû au fait que les doigts sont très sollicités dans la plupart des tâches manuelles que nous effectuons. Les doigts deviennent sales, coupés, marqués, plissés, secs, humides, etc. L'étape d'amélioration de la qualité de l'image a pour but de réduire ce bruit et d'améliorer la définition des arêtes par rapport aux vallées. Cette étape est souvent réalisée par l'utilisation d'un filtre de Gabor. Ce filtre retire les césures des arêtes avec une certaine fiabilité.

3.1.2.2 Extraction de caractéristiques

Les minuties de l'empreinte digitale sont détectées à l'étape d'extraction des caractéristiques. En travaillant sur une image où les lignes sont amincies, les minuties sont plus franches et donc plus facilement détectables. Les fins d'arêtes sont trouvées aux points de terminaison des lignes. Les bifurcations sont trouvées à la jonction de trois lignes.



6 *De l'empreinte digitale au gabarit en passant par les minuties*

Étapes du traitement d'une empreinte digitale :

À partir de l'image originale (a), on définit son orientation (b) [13]. On procède ensuite à sa binarisation (c) [14], puis à un amincissement (d) de l'image. À l'issue de cette étape, on extrait les minuties (e) [15], puis on joint les minuties entre elles, pour obtenir un graphe des minuties (f) (voir figure 6).

Le bruit présent dans l'image originale entraîne systématiquement la détection de minuties étrangères. Elles sont réduites en utilisant des seuils déterminés empiriquement. Par exemple, une bifurcation ayant une branche qui est plus courte que le seuil de longueur est écartée, car il y a de fortes chances qu'elle ne soit pas valide. Deux fins d'arêtes sur une ligne très courte et isolée sont éliminées, car cette ligne est sûrement due au bruit. Deux fins d'arêtes qui sont très proches et qui s'opposent sont éliminées, car elles devaient sûrement être sur la même ligne qui a été brisée à cause d'une cicatrice ou du bruit. Les fins d'arêtes situées aux extrémités de l'empreinte digitale sont éliminées, car ce ne sont pas de vraies fins d'arêtes, mais plutôt la délimitation de l'endroit où le doigt n'est plus en contact avec le dispositif de capture.

Des attributs sont déterminés pour chaque minutie valide détectée : le type de fin d'arête ou de bifurcation, la position (x y) et la direction. Le résultat de l'étape d'extraction des caractéristiques est appelé « modèle de minuties ». C'est une liste de minuties accompagnées des valeurs de leurs attributs. Un intervalle approximatif du nombre de minuties trouvé à ce stade est entre 10 et 100. Si chaque minutie est stockée avec son type (1 bit), sa position (x et y ont 9 bits chacun) et sa direction (8 bits), alors chaque minutie nécessiterait 27 bits – disons 4 octets – et le modèle nécessiterait jusqu'à 400 octets. Il n'est pas rare de voir des longueurs de modèles de 1024 octets.

3.1.2.3 Vérification

À l'étape de vérification, le modèle de l'empreinte digitale de la requête est comparé à toutes les empreintes précédemment stockées [6]. Cela se fait généralement en comparant les voisinages de minuties proches pour trouver des similarités. Un voisinage est composé de trois minuties proches ou plus. Chacune d'entre elles se trouve à une certaine distance et à une orientation relative par rapport aux autres. De plus, chaque minutie a ses propres attributs et sa direction, qui sont également comparés. Si la comparaison n'indique que de petites différences entre les voisinages de l'empreinte enrôlée et de l'empreinte à authentifier, on peut dire qu'elles correspondent.

Le résultat à l'étape de vérification est un score de correspondance, généralement entre 0 et 1. Ce score est soumis à un seuil choisi par l'administrateur du système. Si le score est supérieur au seuil, la correspondance est

juste, sinon la correspondance est fausse. Si le seuil est élevé, on pourra avoir une plus grande confiance dans le résultat, mais le prix à payer est un plus grand nombre de faux rejets[10]. Inversement, si le seuil est trop bas, le nombre de faux rejets est réduit, mais le nombre de fausses acceptations augmente.

La biométrie par empreinte digitale est la technologie la plus employée à travers le monde, et on voit fleurir des solutions de plus en plus abordables et performantes. D'ici à quelques années, les lecteurs d'empreintes digitales n'étonneront plus personne et seront entrés dans les mœurs au même titre que le téléphone portable.

3.2 La reconnaissance de visage

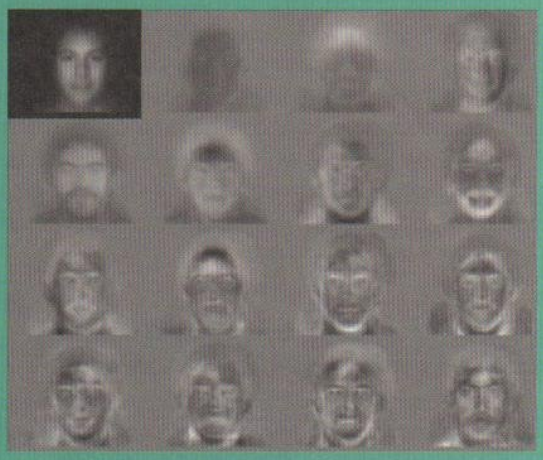
La reconnaissance faciale est utilisée par tout le monde, tous les jours. Le visage est le premier caractère physique utilisé pour identifier quelqu'un. C'est du visage dont on se souvient lorsqu'on essaie de se rappeler ce à quoi ressemble une personne. Nous avons sur nos cartes d'identité des photos qui nous authentifient.

Le visage est fait de diverses caractéristiques microscopiques et macroscopiques distinctes. Les caractéristiques macroscopiques incluent la bouche, le nez, les yeux, les pommettes, le menton, les lèvres et les oreilles. Les caractéristiques microscopiques sont les distances entre les caractéristiques macroscopiques, et leurs tailles.

3.2.1 Algorithmes d'interprétation faciale

3.2.1.1 Eigenface

Eigenface repose sur une technologie brevetée par le MIT. Eigenface, traduit littéralement, signifie « le propre visage de quelqu'un ». L'algorithme fonctionne à partir d'images en niveaux de gris, à deux dimensions. À partir d'une image en niveaux de gris, un Eigenface est extrait. Le visage est ensuite transformé en une série de vecteurs qui lui sont propres, qui sont les propriétés mathématiques décrivant la géométrie unique du visage, formant ainsi le modèle biométrique. Le modèle est ensuite comparé aux Eigenfaces précédemment enrôlées. Le degré de différence entre le modèle et les Eigenfaces de référence détermine la correspondance. Plus la différence est petite, plus il y aura correspondance (voir figure 7).



7 *Exemple de visage traité avec Eigenface*

3.2.1.2 L'analyse de caractéristiques locales

L'analyse de caractéristiques locales a été développée par les docteurs Joseph Atick, Paul Griffin, et Norman Redlich de Visionics Corporation. L'analyse de caractéristiques locales utilise les traits macroscopiques du visage comme points de référence [7].

L'algorithme commence par isoler le visage de son environnement. Les points de référence sont ensuite localisés en utilisant les variations d'ombre autour de chaque caractéristique. Une fois que la variation d'ombre est trouvée, elle est utilisée comme point d'ancrage. À partir de chaque point d'ancrage, les angles des triangles sont mesurés, et un modèle de 672 bits est généré. Un changement d'intensité de la lumière ou de l'orientation peut faire changer les ombres du visage.

Ce changement d'ombres entraînerait la création d'un modèle différent. En pratique, lorsqu'un visage est scanné, un nouveau modèle est créé en utilisant l'analyse de caractéristiques locales ; ce nouveau modèle est comparé aux modèles de référence. Plus le pourcentage de la ressemblance est élevé, plus les deux modèles correspondent.

La figure ci-dessous représente un visage sur lequel une analyse de caractéristiques locales a été appliquée. Tout d'abord le visage est distingué de l'arrière-plan, puis l'analyse de caractéristiques locales est exécutée. La dernière image contient un agrandissement de l'analyse de caractéristiques (la différence d'ombrage est apparente).

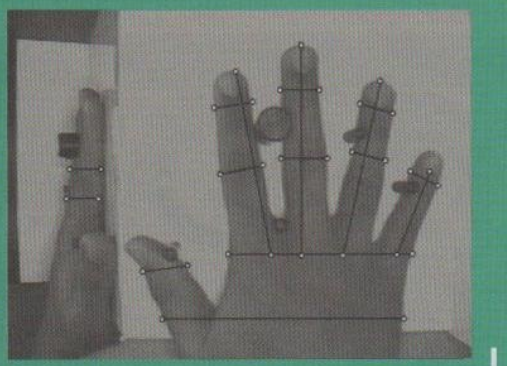
8 *Segmentation pour reconnaissance faciale*

La recherche en reconnaissance faciale a été très active et a fait d'énormes progrès durant les dix dernières années. Bien que les systèmes actuels de reconnaissance faciale obtiennent de très bons résultats pour des visages capturés dans un environnement contrôlé, ils sont bien moins performants dans des situations non contrôlées. Les humains savent différencier le visage de son environnement, mais les systèmes existants ne sont pas suffisamment performants pour en faire de même. Une révolution fondamentale des méthodes employées est nécessaire pour faire un grand pas en avant.

3.3 La géométrie de la main

Chaque main humaine est unique. La longueur des doigts, la largeur, l'épaisseur, la courbure et la position relative de ses caractéristiques permet de distinguer n'importe quelle personne d'une autre. Le scanner de géométrie de la main utilise une caméra à charge couplée, des diodes émettant de la lumière infrarouge avec des miroirs et des réflecteurs pour capturer des images en noir et blanc de la silhouette de la main humaine dans une matrice de 32000 pixels. Ce scanner n'enregistre pas les détails de surface, ignore les empreintes digitales, les lignes, les cicatrices et les couleurs. Cette méthode [8] est proche du fait de placer sa main sur un rétroprojecteur. Le scanner lit la forme de la main en enregistrant la silhouette. En combinaison avec un miroir sur le côté et un réflecteur, le dispositif optique produit deux images distinctes, une de dessus et une de côté. Cette méthode est connue sous le nom de « scan orthographique » (voir figure 9).

Le scanner prend 96 mesures de la main de l'utilisateur. Le microprocesseur et un logiciel interne convertissent les mesures en un modèle de 9 octets qui est stocké pour une comparaison ultérieure. Pendant la session d'enrôlement, le scanner invite l'utilisateur à placer sa main sur le plateau du scanner trois fois consécutives. Le plateau est une surface très réfléchissante qui projette l'image de la silhouette de la main. Des picots disposés sur la surface du plateau permettent à l'utilisateur de bien positionner ses doigts pour améliorer la capture d'image. Le scanner fait la moyenne des trois modèles et génère un modèle précis qui est stocké en mémoire.

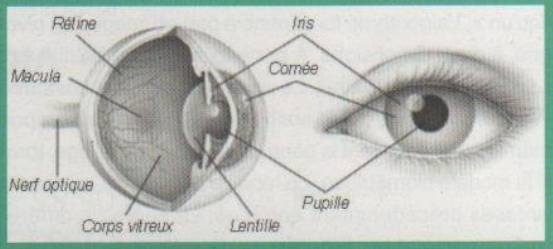


9 *Scanner de géométrie de la main*

La biométrie de la forme de la main est simple à mettre en œuvre. Elle est très bien acceptée par les utilisateurs aussi bien pour le contrôle d'accès que pour le pointage horaire. Elle s'utilise en authentification et a prouvé sa fiabilité dans le temps. Elle s'emploie très bien avec des utilisateurs qui manipulent des produits corrosifs par exemple. Pour ces cas, les empreintes digitales risquent fort d'être inutilisables. On compte de nombreuses applications à travers le monde, par exemple pour l'aéroport de San Francisco.

3.4 La reconnaissance de l'iris

Les technologies biométriques de l'iris semblent être le Saint Graal de la biométrie. Un trait biométrique fort et fiable est mesuré, générant un modèle qui est simple à comparer et qui ne génère quasiment pas de FAR (taux de fausse acceptation). De même, le taux de FRR (taux de faux rejet) est extrêmement bas, de l'ordre de 0.2% en trois tentatives. Avec ces caractéristiques, la biométrie de l'iris fonctionne aussi bien pour l'identification que pour l'authentification [9]. L'iris est le seul organe interne visible du corps humain. Il est situé dans l'œil, derrière la cornée et l'humeur aqueuse, et c'est un caractère physique idéal pour la mesure. Il est protégé par la paupière et la cornée et n'est donc pas exposé à de rudes conditions extérieures qui pourraient rendre sa capture difficile. Il est extrêmement discriminant et ne sera pas le même pour deux jumeaux génétiquement identiques. C'est donc une excellente caractéristique biométrique (voir figure 10).



10 *Image de l'œil en coupe : rétine, iris*

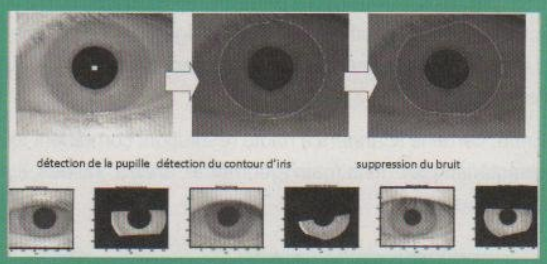
3.4.1 Comment est capturé l'iris ?

L'iris est visible à l'œil nu comme une mosaïque de textures. C'est ce qui est vu quand le spectre visible de la lumière est utilisé pour éclairer l'iris. Quand une lumière proche des infrarouges est utilisée, d'autres caractéristiques sont visibles. Ce sont ces caractéristiques qui sont capturées jusqu'à un mètre de distance avec la technologie appropriée. Généralement, cette technologie

inclut une caméra monochrome CCD d'une résolution de 480x640. Elle est utilisée pour extraire une image d'approximativement 100 à 140 pixels. Pour qu'un utilisateur se fasse scanner l'iris, il doit regarder une caméra et ajuster sa position en fonction d'informations qui lui sont données en retour.

3.4.2 Description de l'algorithme utilisé

Une fois que l'iris est capturé, il est converti en un modèle d'une taille de 2048 bits. Pour comparer un modèle de test avec un modèle de référence, un simple OU exclusif (XOR) est appliqué sur les deux valeurs. Les vecteurs de bits correspondants sont utilisés dans une opération ET pour vérifier qu'il n'y a pas d'artefacts affectant la comparaison. Les résultats sont utilisés pour calculer une distance de Hamming. La distance de Hamming est une mesure de non similarité entre deux modèles d'iris. La distance est ensuite utilisée pour déterminer une correspondance ou non. La simplicité de l'algorithme permet de chercher très rapidement des correspondances, de l'ordre de 10^6 essais par seconde sur une machine possédant un microprocesseur cadencé à 300 MHz (voir figure 11).



11 *Exemples de détection d'iris sous l'effet du clignement des cils*

La biométrie de l'iris est rapide, robuste et résiste à l'usurpation d'identité, mieux que n'importe quel autre trait physique. On pourrait donc penser que c'est la technologie biométrique idéale pour le contrôle d'accès. Cependant, cette technologie n'est pas largement répandue, et ce, pour des raisons simples :

- Le coût du matériel : des caméras spécifiques coûteuses sont toujours nécessaires. Elles ont besoin d'avoir leur propre source de lumière.
- La perception par l'utilisateur : malgré le fait que la lumière infrarouge utilisée soit inoffensive, il reste une sensation de danger.
- Le positionnement : pour que l'iris soit bien placé, un certain nombre d'ajustements sont nécessaires. De ce fait, certaines personnes ne seront jamais capables d'utiliser ce produit, et d'autres auront besoin de beaucoup de tentatives pour être complètement habituées à son usage. Certaines caméras utilisent des techniques de reconnaissance de l'œil pour s'ajuster automatiquement. Ces solutions, bien que meilleures, augmentent le coût et nécessitent encore des coordinations avec l'utilisateur.
- La taille : bien que la taille actuelle des caméras ait été réduite, elle reste relativement grande. Avec la diminution de la taille, il sera plus facile de déployer cette technologie dans un environnement de bureau.

Tous ces problèmes finiront par être résolus avec du temps, de l'argent et des avancées technologiques. Quand cela arrivera et que la perception des utilisateurs changera, la technologie de l'iris sera un sérieux concurrent pour la biométrie des empreintes digitales dans le domaine du contrôle d'accès.

3.5 La reconnaissance vocale

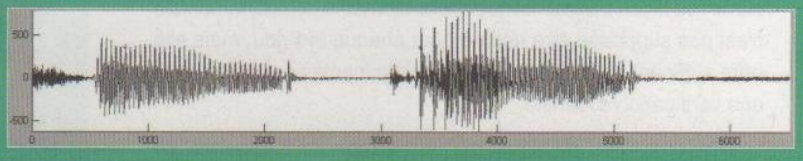
La voix présente un grand nombre de variations suivant les individus, qui constituent autant de caractéristiques d'identification. Ces différences sont également mélangées à d'autres types de variabilités :

- variabilité due au contenu linguistique ;
- variabilité intra-locuteur (qui fait que la voix dépend aussi de l'état physique et émotionnel d'un individu) ;
- variabilité due aux conditions d'enregistrement du signal de parole (bruit ambiant, microphone utilisé, lignes de transmission, distorsion).

Cette méthode est un moyen biométrique intéressant à exploiter. La croissance de l'utilisation des téléphones mobiles et la diversification des applications proposées par les opérateurs trouvent dans l'authentification biométrique à distance [2] une valeur sûre. La reconnaissance du locuteur devient possible, et ce, sans apporter de modifications à appareil téléphonique.

Chaque personne possède une voix propre que l'on peut analyser à l'aide d'un micro. La reconnaissance vocale étudie ces caractéristiques :

- la fréquence ;
- la tonalité ;
- l'intensité...



12 *Enregistrement d'une séquence audio en bande de fréquence*

Toutefois, la fatigue, le stress ou un rhume peuvent provoquer des variations de la voix et générer des perturbations. La fraude est également possible en enregistrant, à son insu, la voix d'une personne autorisée.

La reconnaissance du locuteur se divise en deux grandes familles :

- Les « *text independent* » : le locuteur peut prononcer n'importe quelle phrase pour être reconnu.
- Les « *text dependent* » : le texte à prononcer par le locuteur est imposé par le système, et peut être différent entre deux identifications.

Les systèmes dépendant du texte donnent généralement de meilleures performances d'authentification que les systèmes indépendants du texte, car la variabilité due au contenu linguistique de la phrase prononcée est alors neutralisée. De plus, il devient difficile pour un fraudeur de prévoir le texte à enregistrer pour tromper le micro.

3.6 Les biométries exotiques

3.6.1 La démarche

La démarche, qui est la façon particulière de marcher propre à un individu, est une technologie biométrique spatio-temporelle complexe. La démarche n'est pas censée être très discriminante, mais elle l'est suffisamment pour permettre la vérification d'identité dans certaines applications à faible sécurité.

La démarche est une technologie biométrique comportementale. Sur une longue période de temps, la démarche change à cause des variations de poids du corps humain, des blessures majeures aux articulations ou au cerveau, et de l'état d'ébriété. L'acquisition de la démarche est similaire à l'acquisition de l'image d'un visage et pourrait être, par conséquent, une technologie biométrique acceptable.

Puisque les systèmes fondés sur la reconnaissance de la démarche utilisent les séquences vidéo d'une personne marchant pour mesurer les nombreux mouvements de chaque articulation, ils nécessitent une grande capacité de calcul.

3.6.2 La dynamique de frappe

On part de l'hypothèse que chaque personne tape sur un clavier de façon caractéristique. Cette biométrie comportementale n'est pas supposée être unique pour chaque individu, mais elle offre suffisamment d'informations discriminantes pour permettre une vérification d'identité.

Pour certains individus, on peut s'attendre à observer de grandes variations dans la façon de taper. De plus, les frappes d'une personne pourraient être observées à son insu quand cette personne saisit des informations.

3.6.3 L'odeur

On sait que chaque objet émet une odeur qui est caractéristique de sa composition chimique et qui pourrait être utilisée pour distinguer des objets variés. Un échantillon d'air entourant un objet est soufflé au-dessus d'une rangée de capteurs chimiques, chacun étant sensible à un certain groupe de composés aromatiques.

Un composant de l'odeur émise par un corps humain est propre à un individu en particulier. Il n'est pas encore clairement établi que la constante dans l'odeur corporelle puisse être détectée malgré le parfum des déodorants, et la variation de la composition chimique de l'environnement alentour.

3.6.4 L'empreinte de la paume

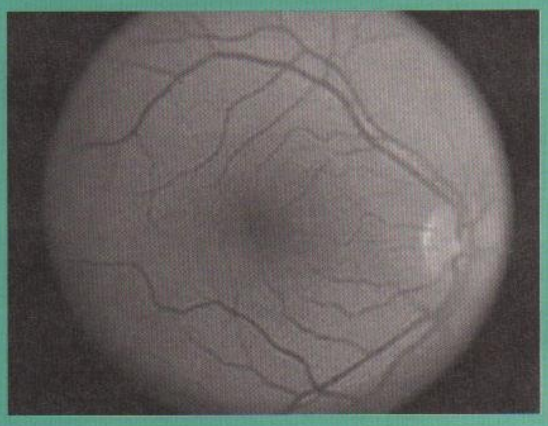
Les paumes des mains contiennent des schémas d'arêtes et de vallées comme les empreintes digitales. La zone de la paume est bien plus grande que celle du doigt, ce qui fait que les empreintes de paumes sont censées être bien plus discriminantes. Puisque les scanners d'empreintes de paumes nécessitent la capture d'une grande surface, ils sont plus encombrants et coûtent plus cher que les capteurs d'empreintes digitales.

Les paumes humaines contiennent également d'autres caractéristiques distinctives comme les lignes principales et les rides que l'on capture même avec un scanner à basse résolution moins coûteux.

Enfin, certains scanners à haute résolution, combinent toutes les caractéristiques de la main (géométrie, arêtes, vallées, lignes principales, et rides).

3.6.5 La rétine ≠ Iris

Le réseau des veines de la rétine est une structure riche et est supposé être particulier à chaque individu et à chaque œil. Il est reconnu comme étant le caractère biométrique le plus sûr, car



13 *Image d'une rétine de l'œil*

il n'est pas facile à modifier ou à répliquer. L'acquisition d'images nécessite que l'individu présente son œil à un capteur et qu'il fixe un spot lumineux spécifique dans son champ de vision pour qu'une région prédéterminée de la rétine soit scannée.

L'acquisition d'images implique la coopération du sujet dont l'œil est en contact avec le capteur. Tous ces facteurs affectent défavorablement l'acceptation de cette technologie. La rétine peut révéler des informations sur l'état de santé, par exemple l'hypertension, ce qui ne va pas dans le sens de l'acceptation de ce type de biométrie (voir figure 13).

3.6.6 La signature manuscrite

La manière de signer son nom est connue pour être une caractéristique individuelle. Bien que les signatures nécessitent un contact avec l'instrument d'écriture et un effort de la part de l'utilisateur, elles ont été acceptées par le gouvernement, par la loi, et dans les transactions commerciales comme méthode de vérification.

Les signatures représentent un caractère biométrique comportemental qui change sur une longue période de temps et qui est influencé par l'état physique et émotionnel du signataire. Les signatures de certaines personnes varient de manière substantielle : même des signatures successives sont significativement différentes. De plus, les faussaires professionnels sont capables de reproduire des signatures qui trompent le système.

3.7 Les systèmes biométriques multimodaux

En utilisant de multiples modalités biométriques (comme le visage et les empreintes digitales d'une personne ou plusieurs doigts d'une personne), on peut dépasser certaines des limites inhérentes à la biométrie unimodale[11]. De tels systèmes, connus sous le nom de systèmes biométriques multimodaux, sont plus fiables du fait de la présence de multiples preuves indépendantes.

Ces systèmes sont également capables de répondre aux besoins rigoureux en termes de performances imposées par des applications variées. Ils s'attaquent aux problèmes de la non-universalité, puisque de multiples caractères garantissent une couverture suffisante de la population.

De plus, la biométrie multimodale fournit une contre-mesure à l'usurpation d'identité compliquant la tâche d'un intrus qui doit imiter les nombreux caractères d'un utilisateur légitime simultanément. En demandant à l'utilisateur de fournir une série aléatoire de caractères biométriques (par exemple index et majeur droits, dans cet ordre), le système s'assure que l'utilisateur présent au point d'acquisition des données est bel et bien vivant. Ainsi, une authentification de type défi-réponse peut être facilitée.

Il existe également ce que l'on pourrait appeler les « systèmes hybrides ». Ces systèmes sont une combinatoire de systèmes classiques (carte à puce, dongle, etc.) avec une solution biométrique uni ou multimodale.

3.7.1 Modes opératoires

Un système biométrique multimodal peut opérer dans l'un des trois modes suivants : mode en série, mode en parallèle ou mode hiérarchique. Dans le mode en série, la sortie d'un caractère biométrique est utilisée pour réduire le nombre d'identités possibles avant que le caractère suivant ne soit utilisé.

Par exemple, un système multimodal opérant avec le visage et les empreintes digitales peut d'abord utiliser l'information faciale pour retrouver les deux meilleures correspondances, et ensuite utiliser les empreintes digitales pour converger vers une seule

identité. Ceci est en contraste avec un mode d'opération en parallèle où l'information de multiples caractères est utilisée simultanément pour procéder à la reconnaissance. Cette différence est cruciale.

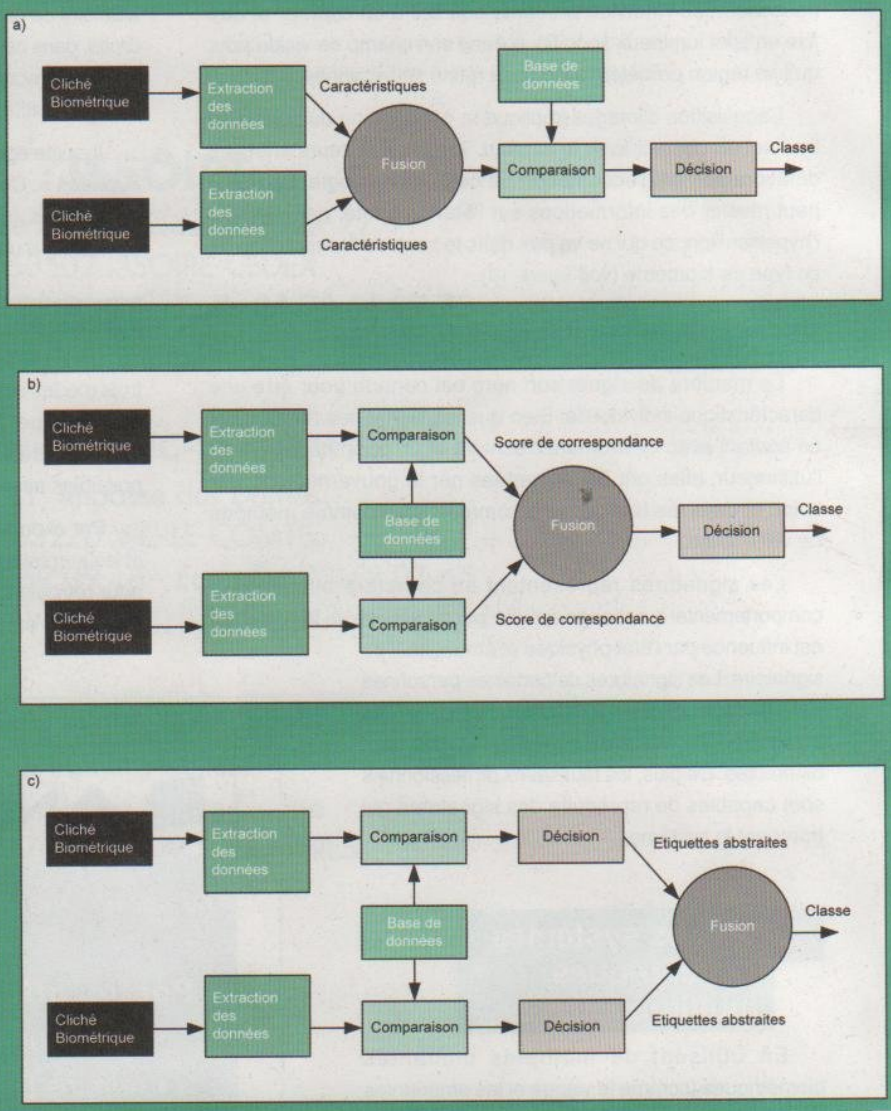
Dans le mode d'opération en série, les divers caractères biométriques n'ont pas besoin d'être acquis simultanément. De plus, une décision peut être prise sans avoir acquis tous les caractères. Cela réduit le temps global de reconnaissance. Dans le schéma hiérarchique, les technologies biométriques sont combinées dans une structure en forme d'arbre.

3.7.2 Les niveaux de fusion

Il ne faut surtout pas confondre *combinatoire* et *fusion*. La combinatoire peut être une simple juxtaposition des scores de systèmes experts (comme des décisions par vote). Alors que la fusion (précoce ou tardive) unit, via des procédés mathématiques, les paramètres ou solveurs des différents systèmes. Ces procédés donnent un sens à cette fusion. Lors d'une combinatoire, le sens est donné au résultat final interprété.

Les systèmes de biométrie multimodaux intègrent des informations présentées par plusieurs indicateurs biométriques. L'information peut être consolidée à différents niveaux. On distingue trois niveaux de fusion lorsqu'on combine deux (ou plus) systèmes biométriques.

- (a) Fusion au niveau de l'extraction des caractéristiques : l'information obtenue à partir de chaque modalité biométrique est utilisée pour calculer un vecteur de caractéristiques. Si les données extraites d'un système sont indépendantes de celles extraites de l'autre, il est raisonnable de concaténer les deux vecteurs en un seul nouveau vecteur. Le nouveau vecteur de caractéristiques a une plus grande dimension et représente l'identité d'une personne dans un espace de caractéristiques différent et plus discriminant. On emploie des techniques de réduction de caractéristiques pour extraire les caractéristiques les plus représentatives de ce grand ensemble de caractéristiques.
- (b) Fusion au niveau du score de correspondance : chaque caractère biométrique fournit un score de similarité indiquant la proximité entre le vecteur de caractéristiques en entrée et le vecteur modèle de caractéristiques. Ces scores sont combinés pour affirmer la véracité de l'identité à vérifier. On utilise des techniques telles que des moyennes pondérées pour combiner les scores.
- (c) Fusion au niveau de la décision (niveau abstrait) : chaque système biométrique prend sa propre décision concernant la reconnaissance, utilisant sur son propre vecteur de caractéristiques. Un vote à la majorité peut être utilisé pour prendre la décision finale.



14 *Différents niveaux de fusion de l'information*

L'intégration au niveau de l'extraction des caractéristiques suppose une forte interaction entre les données d'entrée ; de tels arrangements sont appelés des intégrations étroitement couplées. À l'opposé, l'intégration lointainement couplée s'applique à la sortie de deux agents relativement autonomes, chaque agent évaluant l'entrée indépendamment, dans sa propre perspective.

Une combinaison appliquée le plus tôt possible dans le système de reconnaissance est plus efficace. Par exemple, une intégration au niveau de l'extraction des caractéristiques donne de meilleurs résultats qu'au niveau du score de correspondance. C'est parce que la représentation de caractéristiques transporte une information plus riche comparée au score de correspondance, alors que les étiquettes abstraites contiennent le moins d'informations à propos de la décision qui est prise.

Cependant, il est plus difficile de réaliser une fusion au niveau des caractéristiques, car la relation entre les espaces de caractéristiques des différents systèmes biométriques peut ne pas être connue et les représentations des caractéristiques pas compatibles.

Après voir étudié les principaux systèmes biométriques, regardons quelles sont leurs limites.

4. Limitations des systèmes biométriques

Tout système a ses limites, la biométrie ne fait pas exception malgré l'usage de l'informatique. Ce n'est pas parce qu'on utilise un système biométrique que le niveau de sécurité est plus élevé : la biométrie n'est qu'une petite brique dans un système de sécurité.

Le système biométrique parfait, sans faille, n'existe pas encore et n'existera **peut-être (probablement ?)** jamais. Les limites d'un système sont souvent liées à ses performances [10], par exemple la difficulté pour un ordinateur de reconnaître une chose aussi changeante qu'un visage ou à reconnaître la voix d'une personne dans un milieu fortement bruité. Il faut aussi compter avec le désir de mettre le système en échec, c'est l'éternel jeu du gendarme et du voleur.

L'empreinte biologique, en phase de devenir un titre d'identité universel, induit forcément l'instauration de débats éthiques inédits. Ceci s'ajoute donc à la longue liste des reproches faits à la biométrie.

D'un point de vue scientifique, le passage obligatoire par les deux phases distinctes d'enrôlement et de vérification implique inévitablement l'emploi de probabilités d'ordre statistique. Si le degré de reconnaissance est insuffisant (*probabilistiquement* parlant), la personne concernée sera « rejetée » par le système. Les systèmes biométriques sont donc intrinsèquement faillibles [16].

Prenons le cas de la reconnaissance du locuteur. Les imitateurs essayent habituellement de reproduire les caractéristiques vocales qui sont les plus évidentes au système auditif humain et ne recréent pas les caractéristiques moins accessibles (fricative, formant, etc.). Il n'est donc, théoriquement, pas possible d'imiter la voix d'une personne inscrite dans une base de données et donc de se substituer à elle.

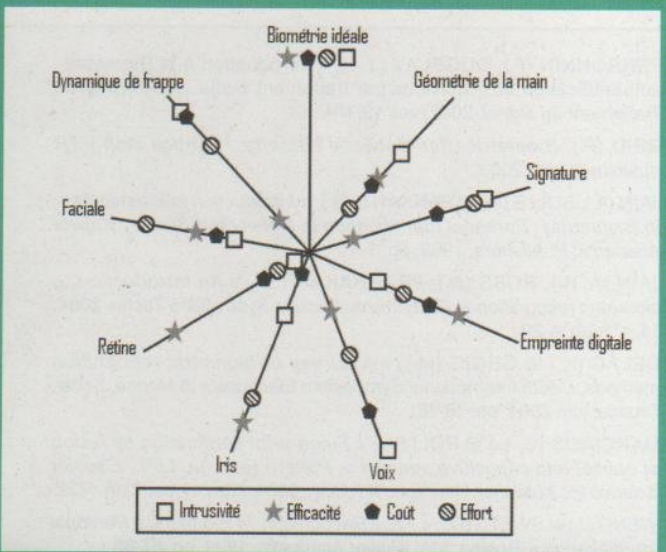
Le système biométrique idéal n'existe pas. Il varie selon la nature de l'application et du public concerné.

Le schéma ci-contre représente les performances des systèmes biométriques les plus répandus.

Légende :

- **Effort** : effort requis pour l'utilisateur lors de la mesure.
- **Intrusivité** : décrit dans quelle mesure l'utilisateur perçoit le test comme intrusif.
- **Coût** : coût de la technologie (lecteurs, capteur, etc.).
- **Efficacité** : efficacité de la méthode (capacité à identifier quelqu'un).

Je vous laisse comprendre et interpréter cette figure.



15 *Études des perceptions par modalités biométriques*

Conclusion

Pour conclure, nous dirons que les systèmes biométriques dans des contextes bien ciblés et bien paramétrés sont bien acceptés par les utilisateurs. Ils simplifient les tâches d'administration des systèmes conventionnels (exemple : mot de passe, code PIN, clé de serrure, etc.) tout en augmentant le niveau de sécurité existant et son ergonomie.

Il faut tout de même développer une approche formelle de sécurité de ces systèmes pour une éventuelle certification. Et donner un niveau de sécurité des techniques biométriques à la manière des notions développées dans la « cryptographie prouvée » pour apporter la preuve de la fiabilité de fonctions de sécurité des systèmes biométriques.

Cette certification doit s'accompagner d'une évaluation des méthodes de leurres de ces dispositifs et mesurer de manière objective la fiabilité de ces techniques pour les comparer entre elles.

L'objectif est donc bien de limiter les risques liés à l'utilisation de la biométrie, et non de la rendre parfaitement sûre, ce qui serait voué à l'échec.

Notes

[1] Nous utilisons volontairement le mot reconnaissance pour parler des deux différentes notions : identification et authentification.

[2] FRR : terme anglais pour *False Rejection Rate*

[3] FAR : terme anglais pour *False Acceptation Rate*

[4] FEE : terme anglais pour *False Error Rate*

[5] FTE : terme anglais pour *Failure To Enroll*

[6] ESTER : évaluation des Systèmes de Transcription Enrichie d'Émissions Radiophoniques

[7] NIST : *National Institute of Standards and Technology*

[8] Arête : une ligne de l'empreinte du doigt

[9] Minutie : une forme d'arête définie par une position (x,y)

[10] Voir le paragraphe « 4.Limitations des systèmes biométriques »

[11] Unimodal : qui repose sur une seule modalité biométrique, l'empreinte seule, l'iris seul, etc.

Références

[1] PERRONNIN (F.), DUGELAY (J. l.), « Introduction à la Biométrie : authentification des Individus par traitement audio-vidéo », *Revue Traitement du signal*, 2002, vol. 19, n°4.

[2] REID (P.), *Biometrics for Network Security, Prentice Hall PTR publishers*, déc 2003.

[3] JAIN (A.), BOLLE (R.) et PANKANTI (S.), « *Introduction to Biometrics* », *in Biometrics. Personal Identification in Networked Society Kluwer Academic Publishers*, 1999, pp. 1-41.

[4] JAIN (A. K.), ROSS (A.), PRABHAKAR (S.), « *An introduction to biometric recognition* », *IEEE Trans. Circuits Syst. Video Techn*, 2004, 14, n°1, pp. 4-20.

[5] DELAC (K.) et GRGIC (M.), « *A survey of biometric recognition methods* », *46th International Symposium Electronics in Marine*, Zadar, Croatia, juin 2004, pp. 16-18.

[6] MARCIALIS (G. L.) et ROLI (F.), « *Fingerprint verification by fusion of optical and capacitive sensors* », *Pattern Recogn. Lett., Elsevier Science Inc.publisher,* New York, NY, USA, 2004, 25, n°11, pp. 1315-1322.

[7] WENG (J.) et SWETS (D.), « *Face Recognition, in Biometrics: Personal Identification* », Boston, MA: Kluwer Academic, 1999, pp. 67-86.

[8] ZUNKEL (R.), *Hand Geometry Based Authentication, in Biometrics: Personal Identication in Networked Society,* A. Jain, R. Bolle et S. Pankanti (Eds.), *Kluwer Academic Publishers*, 1998.

[9] DAUGMAN (J.), *Recognizing persons by their Iris patterns, Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers*, 1999.

[10] WAYMAN (J.), JAIN (A. K.), MALTONI (D.) et MAIO (D.), *Biometric Systems: Technology, Design and Performance Evaluation*, Springer, 2005.

[11] JAIN (A. K.), PRABHAKAR (S), HONG (L.) et PANKATI (S.), *Filterbank-based fingerprint matching, IEEE Transaction on Images Processing*, mai 2000, 9, n°5.

[12] CHAN (K. C.), MOON (Y. S.) et CHENG (P. S.), « *Fast Fingerprint Verification Using Sub-region of Fingerprint Images* », *IEEE Trans. On Circuit and Systems for Video Technology*, janv. 2004, 14, n°1, pp. 95-101.

[13] RAO (A. R.), *A Taxonomy for Texture Description and Identification*, Springer-Verlag, New York, New York, 1990.

[14] MAIO (D.) and MALTONI (D.), « *Direct gray-scale minutiae detection in fingerprints* », *IEEE Transactions on Pattern Analysis and Machine Intelligence*, janv. 1997, 19, n°1, pp. 27-40.

[15] MALTONI (D.), MAIO (D.), JAIN (A. K.) et PRABHAKAR (S.), *Handbook of Fingerprint Recognition, Springer-Verlag*, juin 2003.

[16] DIRECTION GÉNÉRALE DES AFFAIRES JURIDIQUES, *Rapport d'étape sur l'application des principes de la convention 108 à la collecte et au traitement des données biométriques*, Conseil de l'Europe, Strasbourg, fév. 2005.