



MYTHES ET LEGENDES DES TIC

30 novembre 2010

Collection ATENA

Une réalisation de Forum ATENA avec la collaboration de *(par ordre alphabétique)* :

[Jean-Pierre Cabanel](#), [Franck Franchin](#), David Grout, [Daniel Hagimont](#), Gérard Peliks, Sadry Porlon,
Nicolas Ruff, Philippe Vacheyrout

Livre collectif sous la direction de Gérard Peliks

Copyright forum ATENA – Voir en dernière page les droits de reproduction

SOMMAIRE

| | |
|--|-----------|
| MYTHES ET LEGENDES DES TIC..... | 1 |
| MYTHES ET LEGENDES DE L'INTERNET | 5 |
| LES FAUSSES CERTITUDES..... | 5 |
| MYTHE N° 1 : L'INTERNET BENEFICIE LARGEMENT DE L'INNOVATION | 5 |
| MYTHE N° 2 : L'INTERNET EST UN RESEAU QUI APPARTIENT A TOUT LE MONDE | 5 |
| MYTHE N° 3 : L'INTERNET EST ISSU DU RESEAU ARPANET..... | 6 |
| MYTHE N° 4 : LE ROUTAGE DE L'INTERNET EST DECENTRALISE..... | 6 |
| MYTHE N° 5 : L'ADRESSE IP IDENTIFIE UN ORDINATEUR..... | 7 |
| MYTHE N° 6 : L'IPv6 VA RESOUDRE TOUS LES PROBLEMES EVOQUES | 7 |
| LE POST-IP..... | 8 |
| MYTHES ET LEGENDES DE LA SECURITE DE L'INFORMATION..... | 9 |
| LES AGRESSIONS, ÇA N'ARRIVE PAS QU'AUX AUTRES | 9 |
| MYTHE N° 1 : IL EXISTE DES HAVRES DE PAIX SUR L'INTERNET | 9 |
| MYTHE N° 2 : LES EXECUTABLES EN ".EXE", VOILA LE DANGER ! | 10 |
| MYTHE N° 3 : LES CYBERCRIMINELS VEULENT DETRUIRE VOTRE SYSTEME D'INFORMATION | 11 |
| MYTHE N° 4 : LA SECURITE DE L'INFORMATION EST UN CENTRE DE COUT | 11 |
| MYTHE N° 5 : LES ATTAQUES VIENNENT DE L'EXTERIEUR..... | 12 |
| MYTHE N° 6 : LE CYBERMONDE EST UN ESPACE DE NON DROIT..... | 12 |
| MYTHES ET LEGENDES DES RISQUES DE CYBERGUERRE SUR LES INFRASTRUCTURES VITALES | 14 |
| INTRO..... | 14 |
| MYTHE N° 1 : LES SYSTEMES CRITIQUES SONT PROTEGES DES ATTAQUES GRACE A LEUR REDONDANCE | 14 |
| MYTHE N° 2 : INTERNET EST UNE INFRASTRUCTURE CRITIQUE PRIMORDIALE | 15 |
| MYTHE N° 3 : NOUS AURONS UN PEARL-HABOR DIGITAL DANS LES DIX PROCHAINES ANNEES | 15 |
| MYTHE N° 4 : LE CYBER-TERRORISME EST UNE MENACE IMPORTANTE | 15 |
| MYTHE N° 5 : LA GUERRE DE TROIE N'AURA PAS LIEU..... | 15 |
| MYTHES ET LEGENDES DES VULNERABILITES LOGICIELLES | 16 |
| MYTHE N° 1 : TROUVER DES VULNERABILITES , C'EST COMPLIQUE (RESERVE AUX EXPERTS)..... | 16 |
| MYTHE N° 2 : MAINTENANT QUE LA SECURITE EST DEVENUE UN ENJEU IMPORTANT POUR LES EDETEURS, LE NOMBRE DE VULNERABILITES VA DIMINUER..... | 16 |
| MYTHE N° 3 : TOUT LE MONDE EST TRES CONCERNE PAR LA DECOUVERTE DE VULNERABILITES CRITIQUES | 17 |
| MYTHE N° 4 : CORRIGER LES VULNERABILITES AMELIORE LA SECURITE DES SYSTEMES..... | 17 |
| MYTHE N° 5 : IL EXISTERA UN JOUR DES LOGICIELS GRAND PUBLIC INVULNERABLES | 17 |
| MYTHES ET LEGENDES DES VERS, VIRUS ET TROJANS..... | 19 |
| MYTHE N° 1 : LES EDETEURS D'ANTIVIRUS ECRIVENT EUX-MEMES LES CODES MALVEILLANTS: | 19 |
| MYTHE N° 2 : LES CODES MALVEILLANTS SONT ENFANTINS A GENERER :..... | 19 |
| MYTHE N° 3 : C'EST SUR LES PC SOUS WINDOWS QUE LES VIRUS ATTAQUENT | 20 |
| MYTHE N° 4 : UNE MISE A JOUR DE LA BASE ANTIVIRALE PAR SEMAINE ET JE SUIS TRANQUILLE | 20 |
| MYTHE N° 5 : IL NE SE PASSE RIEN DE SPECIAL SUR MA MACHINE C'EST DONC QUE TOUT VA BIEN..... | 21 |
| MYTHES ET LEGENDES DU CHIFFREMENT..... | 22 |
| QUELQUES MOTS A MAITRISER QUAND ON PARLE DE CRYPTOLOGIE | 22 |
| MYTHE N°1 : LE SECRET DU CHIFFREMENT EST DANS L'ALGORITHME | 22 |
| MYTHE N° 2 : ON CHIFFRE AVEC SA CLE PRIVEE..... | 23 |
| MYTHE N° 3 : ON CHIFFRE AVEC UNE CLE PUBLIQUE | 24 |
| MYTHE N° 4 : LE CHIFFREMENT QUANTIQUE, ARME ABSOLUE, DES AUJOURD'HUI | 24 |
| MYTHE N° 5 : LE CHIFFREMENT SEUL MOYEN D'ASSURER LA CONFIDENTIALITE | 25 |
| LES MECANISMES DU CHIFFREMENT | 26 |

| | |
|--|-----------|
| MYTHES ET LEGENDES DE LA SIGNATURE ELECTRONIQUE | 28 |
| LA SIGNATURE ELECTRONIQUE, CE QU'ELLE N'EST PAS..... | 28 |
| MYTHE N° 1 : ON SIGNE PAR SON CERTIFICAT ELECTRONIQUE | 28 |
| MYTHE N° 2 : LE CERTIFICAT EST CONFIDENTIEL ET IL FAUT LE PROTEGER..... | 29 |
| MYTHE N° 3 : UNE SIGNATURE ELECTRONIQUE EN VAUT UNE AUTRE | 30 |
| MYTHE N° 4 : SIGNER, C'EST CHIFFRER ET CHIFFRER C'EST SIGNER..... | 31 |
| MYTHE N° 5 : UNE SIGNATURE ELECTRONIQUE, C'EST POUR LA VIE | 31 |
| LES MECANISMES DE LA SIGNATURE ELECTRONIQUE | 31 |
| MYTHES ET LEGENDES DE L'IDENTITE NUMERIQUE | 33 |
| MYTHE N° 1 : L'IDENTITE NUMERIQUE EST UNIQUE :..... | 33 |
| MYTHE N° 2 : L'IDENTITE NUMERIQUE RELEVE DE L'AUTORITE REGALIEENNE. | 34 |
| MYTHE N° 3 : IDENTIFICATION ET AUTHENTIFICATION C'EST PAREIL. | 34 |
| MYTHE N° 4 : LA SECURITE EST GARANTIE PAR LES REFERENTIELS DE SECURISATION ET D'INTEROPERABILITE (RGS - RGI)..... | 34 |
| MYTHE N° 5 : LA GOUVERNANCE DE L'INTERNET RELEVE D'UNE ORGANISATION CENTRALISEE..... | 35 |
| EN CONCLUSION : INTERNET EST LA PIRE ET LA MEILLEURE DES CHOSES | 35 |
| MYTHES ET LEGENDES DES SYSTEMES DE CLOUD | 36 |
| MYTHE N° 1 : LE CLOUD EST JUSTE CE QU'ON APPELAIT AVANT LE "TIME SHARING" : LES APPLICATIONS NE SONT PLUS HEBERGEES CHEZ SOI ET ON NE PAYE QUE CE QUE L'ON CONSOMME | 36 |
| MYTHE N° 2 : LE CLOUD COMPUTING EST UNE REVOLUTION TECHNOLOGIQUE..... | 37 |
| MYTHE N° 3 : LE CLOUD PRIVE D'UN GRAND COMPTE EST COMPLETEMENT SECURISE | 39 |
| MYTHE N° 4 : LES INFORMATIONS STOCKEES SUR UN CLOUD PARTAGE SONT PROTEGEES, PAR CONTRAT, DES VIRUS, VERS ET AUTRES ATTAQUES | 39 |
| MYTHE N° 5 : SI VOUS QUITTEZ VOTRE FOURNISSEUR, VOTRE CONTRAT GARANTIT LA CONFIDENTIALITE ET LA RESTITUTION DE VOS INFORMATIONS ET LEUR DESTRUCTION..... | 40 |
| MYTHE N° 6 : AVEC UN SERVICE DE CLOUD, JE N'AI PLUS BESOIN DE ME PREOCCUPER DE MA SECURITE ET DE LA DISPONIBILITE DES SERVICES, ET MON CONTRAT COUVRAIT LES RISQUES INFORMATIQUES ENGENDRES | 41 |
| QUELQUES PLATEFORMES EXISTANTES | 41 |
| MYTHES ET LEGENDES DE LA CERTIFICATION CRITERES COMMUNS..... | 43 |
| LA CONFIANCE OBJECTIVE EN UNE SOLUTION DE SECURITE | 43 |
| MYTHE N° 1 : MA SOCIETE EST CERTIFIEE "CRITERES COMMUNS" | 43 |
| MYTHE N° 2 : LA CERTIFICATION CRITERES COMMUNS PORTE SUR L'ENSEMBLE D'UN PRODUIT..... | 44 |
| MYTHE N° 3 : DEUX PRODUITS DE MEME TYPE, CERTIFIES CRITERES COMMUNS, SONT COMPARABLES | 44 |
| MYTHE N° 4 : DANS EALx+, LE "+" EST LE PRINCIPAL FACTEUR DE QUALITE | 45 |
| MYTHE N° 5 : UN CERTIFICAT CRITERES COMMUNS A UNE DATE DE PEREMPTION | 45 |
| MYTHE N° 6 : UNE CERTIFICATION CRITERES COMMUNS OBTENUE DANS UN DES PAYS CERTIFICATEURS EST AUTOMATIQUEMENT RECONNUE DANS TOUS LES PAYS | 46 |
| MYTHE N° 7 : UN NIVEAU DE CERTIFICATION EVALUE LES FONCTIONNALITES DE SECURITE D'UN PRODUIT | 46 |
| MYTHE N° 8 : UNE SOLUTION DE SECURITE DOIT ETRE CERTIFIEE CRITERES COMMUNS POUR ENTRER DANS LE CATALOGUE DE L'ADMINISTRATION FRANÇAISE | 47 |
| MYTHE N° 9 : EN FRANCE, C'EST L'ANSSI QUI CONDUIT LES TESTS D'EVALUATION..... | 47 |
| POUR EN SAVOIR PLUS : | 48 |
| MYTHES ET LEGENDES DU DROIT DE LA COMMUNICATION SUR L'INTERNET | 49 |
| MYTHE N° 1 : UNE INJURE OU UNE DIFFAMATION DONT ON EST VICTIME SUR INTERNET EST SUSCEPTIBLE D'UNE ACTION DEVANT LES TRIBUNAUX TANT QUE LE MESSAGE EST VISIBLE SUR LE SITE LITIGIEUX..... | 49 |
| MYTHE N° 2 : IL FAUT AVOIR ETE INJURIE, DIFFAME OU DENIGRE POUR POUVOIR OBTENIR UN DROIT DE REPONSE AUPRES DU SITE INTERNET A L'ORIGINE DE L'INFRACTION | 50 |
| MYTHE N° 3 : IL FAUT AVOIR ETE INJURIE, DIFFAME OU DENIGRE POUR POUVOIR OBTENIR UN DROIT DE REPONSE AUPRES DE LA TELEVISION OU DE LA RADIO A L'ORIGINE DE L'INFRACTION | 50 |
| MYTHE N° 4 : DEMANDER UN DROIT DE REPONSE A L'EDITEUR D'UN SITE INTERNET ET L'OBTENIR EMPECHE TOUTE ACTION DEVANT LES TRIBUNAUX CONTRE L'AUTEUR DES PROPOS. | 51 |

| | |
|--|-----------|
| MYTHE N° 5 : LE FAIT QUE L'AUTEUR D'UN MESSAGE DIFFAMATOIRE OU INJURIEUX SE SOIT EXCUSE PUBLIQUEMENT SUITE A LA DIFFUSION DU PROPOS LUI PERMETTRA D'ÉCHAPPER A UNE SANCTION EN CAS D'ACTION DEVANT LES TRIBUNAUX..... | 51 |
| MYTHE N° 6 : LE FAIT POUR L'ÉDITEUR D'UN SITE INTERNET DE NE PAS AVOIR MIS A DISPOSITION DES INTERNAUTES UN CERTAIN NOMBRE D'ÉLÉMENTS D'IDENTIFICATION COMME, POUR LES PERSONNES PHYSIQUES, (SON NOM, SON PRENOM, SON DOMICILE) OU POUR LES PERSONNES MORALES (SA DENOMINATION, SA RAISON SOCIALE OU ENCORE SON SIEGE SOCIAL) NE PEUT PAS LUI VALOIR UNE CONDAMNATION DEVANT LES TRIBUNAUX. | 51 |
| MYTHE N° 7 : IL EST POSSIBLE DE REPRODUIRE INTEGRALEMENT L'ARTICLE D'UN AUTEUR SUR SON SITE A CONDITION DE CITER SON NOM ET LA SOURCE DE L'ARTICLE. | 52 |
| MYTHE N° 8 : LE FAIT DE REPRODUIRE UNE ŒUVRE OU UN CONTENU SUR UN SITE INTERNET A VOCATION NON COMMERCIALE PERMET D'ÉCHAPPER A UNE CONDAMNATION POUR CONTREFAÇON. | 52 |
| CONCLUSION | 52 |
| MYTHES ET LEGENDES DES TELECHARGEMENT ILLEGAUX | 53 |
| MYTHE N°1 : L'EXCEPTION POUR COPIE PRIVEE PERMET A CELUI QUI TELECHARGE UNE ŒUVRE SUR INTERNET SANS AUTORISATION DE NE PAS ETRE CONDAMNE DEVANT LES TRIBUNAUX S'IL DEMONTE QUE LADITE COPIE A FAIT L'OBJET D'UNE UTILISATION STRICTEMENT PRIVEE | 53 |
| MYTHE N°2 : DEPUIS LES LOIS HADOPI, LE TELECHARGEMENT ILLEGAL D'UNE ŒUVRE SUR INTERNET NE PEUT PLUS ETRE SANCTIONNE « QUE » PAR UNE SUSPENSION D'INTERNET PENDANT UN MOIS MAXIMUM ET D'UNE AMENDE NE DEPASSANT PAS 1500 EUROS. | 54 |
| MYTHE N°3 : SI MON ACCES A INTERNET EST SUSPENDU SUITE A UNE DECISION DU JUGE, IL ME SUFFIT DE SOUSCRIRE IMMEDIATEMENT UN NOUVEL ABONNEMENT..... | 55 |
| MYTHE N°4 : SI LE JUGE DECIDE D'UNE SUSPENSION DE MON ABONNEMENT, JE NE VAIS QUAND MEME PAS ETRE CONTRAINT DE CONTINUER A PAYER CET ABONNEMENT PENDANT LA DUREE DE CETTE SUSPENSION | 55 |
| MYTHE N°5 : L'ABONNE QUI REÇOIT DES RECOMMANDATIONS DE LA PART DE LA HADOPI DEVRA ATTENDRE D'ETRE POURSUIVI DEVANT LES TRIBUNAUX POUR FAIRE VALOIR SES DROITS..... | 56 |
| MYTHE N°6: EN PRESENCE D'UN TELECHARGEMENT ILLEGAL AVERE, LE JUGE A UNE MARGE DE MANŒUVRE ASSEZ FAIBLE DANS LA FIXATION DE LA DUREE DE LA SUSPENSION DE L'ACCES A INTERNET | 56 |
| MYTHE N°7 : C'EST LA HAUTE AUTORITE POUR LA DIFFUSION DES ŒUVRES ET LA PROTECTION DES ŒUVRES QUI COLLECTE, ELLE-MEME, LES ADRESSES IP DES ABONNES DONT L'ACCES A SERVI A TELECHARGER DES ŒUVRES | 57 |
| CONCLUSION | 58 |
| GLOSSAIRE | 59 |
| BIBLIOGRAPHIE | 60 |
| A PROPOS DES AUTEURS | 61 |

MYTHES ET LEGENDES DE L'INTERNET

*Gérard Peliks, CASSIDIAN
an EADS Company*

LES FAUSSES CERTITUDES

L'Internet est tellement ancré dans notre vécu quotidien que comme pour toute chose qui s'est rapidement imposée, il s'est bâti autour de ce phénomène, des croyances devenues certitudes qu'il n'est même pas envisageable de remettre en question sans passer pour quelqu'un qui n'a rien compris à ce qui semble évident à l'homo vulgaris.

Mais ces certitudes ont parfois leur part d'erreurs et peuvent figer le développement de ce moyen irremplaçable de communication qui a bien besoin d'évoluer, peut-être même en changeant de base.

Mieux comprendre l'Internet d'aujourd'hui, en particulier dans ses couches basses est indispensable pour appréhender les travaux qui sont menés actuellement dans des centres de recherche, et qui pourraient bien changer les bases de l'Internet du futur.

MYTHE N° 1 :

L'INTERNET BENEFICIE LARGEMENT DE L'INNOVATION

En fait très peu d'innovations ont été réalisées depuis la fin des années 70 dans les couches basses de l'Internet. Comme le système fonctionne, porté par l'augmentation des performances prévue dans les lois de Moore, comme les protocoles sont entérinés par des organismes de standardisation, l'IETF en particulier, ceux qui avaient le pouvoir de faire évoluer l'Internet ont préféré se servir de l'existant pour asseoir leur business. Notons que la standardisation de l'Internet n'est pas le fait d'organismes internationaux de normalisation comme l'ISO, l'UIT ou l'ETSI, et que l'IETF est un organisme essentiellement sous contrôle des Américains.

La recherche et le développement des couches basses de l'Internet ont été laissés à l'abandon car les retombées en revenus immédiats n'ont jamais été perçues de manière évidente et l'aspect économique a primé et écarté l'innovation. Il fallait que l'Internet rapporte de l'argent. Pour cela, il ne fallait surtout pas toucher aux couches basses qui devaient rester stables.

Certes, côté applicatif, il y a eu de grandes innovations, comme bien sûr le Web, aujourd'hui participatif et demain sémantique, comme les nouveaux usages : musique, vidéo, films, P2P, ToIP, forums. Il y en aura de nombreux autres à peine croyables aujourd'hui, comme la 3D et la réalité augmentée... Mais justement, ces avancées peuvent difficilement reposer sur des couches basses qui n'ont pas évolué en rapport avec ce que réclament les nouvelles applications, en sécurité, en mobilité, en sans-fils, en multihoming (connexion à plusieurs réseaux).

MYTHE N° 2 :

L'INTERNET EST UN RESEAU QUI APPARTIENT A TOUT LE MONDE

Ça c'est un mythe tellement répandu que l'accès à la toile, l'envoi des courriels, les forums de discussion sont devenus aussi naturels que l'air qu'on respire et qui appartient à tous, comme semble l'être l'Internet, abonnement à un fournisseur de services mis à part. Et pourtant

L'Internet est loin d'être neutre. Il "appartient" à l'ICANN (Internet Corporation for Assigned Names and Numbers). En effet, l'ICANN gère l'espace d'adressage du sommet de la hiérarchie des noms de domaines de l'Internet, et ses serveurs de noms de domaines racines, ce qui en fait de facto son véritable propriétaire car qui détient le nommage détient le pouvoir.

Créé en 1998, l'ICANN est une organisation de droit privé, plus précisément de droit californien. Vinton Cerf, un des intervenants de notre grand événement sur le futur de l'Internet du mois de janvier en avait été le président durant près d'une dizaine d'années. Il est vrai que ces derniers temps, la gouvernance de l'ICANN est devenue un peu moins américaine, mais à peine moins. On dit que le président des Etats-Unis dispose (ou disposera) d'un gros bouton rouge, pour désactiver l'Internet mondial en cas de cyber attaque grave sur son pays. D'ailleurs les Etats-Unis avaient déconnecté pendant un certain temps le domaine de l'Irak du reste de l'Internet. Aucun autre pays ne pourrait en faire autant.

Les Chinois ont déjà pris leurs distances par rapport à ce qu'on appelle encore communément "l'Internet" (au singulier), en constituant leur propre Internet indépendant de celui du reste du monde. Les Iraniens penseraient sérieusement à faire de même. Ces dissidences pourraient faire effet domino, ne serait-ce que pour prendre en compte des alphabets non latins, des lettres accentuées ou une philologie non américaine. On parlera alors non pas de l'Internet mais "des" internets, tout ceci pour une question d'adressage et de gestion des noms de domaines !

MYTHE N° 3 :

L'INTERNET EST ISSU DU RESEAU ARPANET

Ce n'est pas faux. L'Internet a beaucoup bénéficié des travaux réalisés pour le réseau ARPANET et en particulier du développement des protocoles IP et des protocoles au dessus (TCP, UDP, ICMP, FTP, SMTP, HTTP ...).

Toutefois si on mène une recherche en paternité de l'Internet, on peut remonter plus loin, jusqu'aux travaux autour du projet CYCLADES de l'IRIA (qui allait devenir l'INRIA) et de l'idée du datagramme, objet logiciel qui permet de travailler en mode sans connexion. A la tête du projet CYCLADES, il y avait le Français Louis Pouzin, à qui revient le titre d'inventeur de l'Internet. Mais dans la France des années 70, sous la présidence de Giscard, les PTT avaient imposé le circuit virtuel (mode avec connexion) qui allait donner X25 puis ATM.

Et c'est ainsi qu'une idée française, un mode sans connexion, ne s'est pas concrétisée en France et que les Etats-Unis sont devenus les maîtres incontestés de l'Internet.

MYTHE N° 4 :

LE ROUTAGE DE L'INTERNET EST DECENTRALISE

Décentralisé comme le routage du téléphone ou du GSM ? On voudrait bien que ce soit vrai mais c'est loin d'être le cas. Si on prenait une image, utiliser le routage de l'Internet, c'est comme si on demandait à un facteur de distribuer le courrier, mettons rue de Vaugirard. Mais le premier immeuble de cette rue ne serait pas le "1 rue de Vaugirard", mais le "232 boulevard Eisenhower", en face ce ne serait pas le "2 rue de Vaugirard" mais le 12 avenue Mao Tse Toung, et ainsi de suite.

Vous voyez le surcroît de travail pour le pauvre facteur obligé de consulter un répertoire qui fait la liaison entre l'implantation de l'immeuble dans la rue et son adresse ? Et pour les

employés du centre de tri postal, quel cauchemar pour classer le courrier ! Il faut donc des répertoires (serveurs DNS).

Tout ceci suite à de mauvaises options dans l'attribution des adresses IP, dans le nommage des domaines et dans la répartition des tâches entre les couches IP et TCP. Mais c'est ainsi que fonctionne le routage sur l'Internet car la plupart des routes sont statiques.

Chaque message, chaque fichier est découpé en datagrammes et chaque datagramme qui connaît son adresse de destination (contenue dans le champ IP) est acheminé de proche en proche, via des routeurs, dans les réseaux connectés. Et chaque routeur doit connaître vers quel routeur de proximité transmettre le datagramme qui ne lui est pas destiné, en fonction des routes qu'il connaît et de celles qu'on lui fait connaître.

Ceci entraîne une explosion en taille des tables de routage, des performances dégradées car les routeurs arrivent à la limite de leur capacité de calcul et le problème va vite devenir insoluble.

MYTHE N° 5 :

L'ADRESSE IP IDENTIFIE UN ORDINATEUR

Ça vous semble évident ? Et bien non, l'adresse IP identifie le contrôleur réseau par lequel votre ordinateur se connecte à l'Internet ou à un Intranet. On aurait bien voulu qu'une adresse IP indique qui en est le possesseur, ou au moins l'ordinateur qui possède cette adresse si ce n'est qui est l'utilisateur de cet ordinateur, à quel endroit se trouve cet ordinateur et quelle est sa fonction. On est loin du compte.

Tous ces renseignements (qui, où, quoi), ne peuvent être donnés qu'en rajoutant constamment des rustines au dessus de la couche IP de l'Internet.

Comme l'a fait remarquer le professeur Kavé Salamatian de l'Université du Jura, l'Internet bien conçu il y a quarante ans pour un nombre très petit de nœuds, à ses début dans le projet ARPANET, avait une couche IP fine et élégante, mais elle s'est très vite engraisée et présente aujourd'hui de grosses poignées d'amour qui sont IPsec, NAT, Diffserv, Mcast...

Un poids trop élevé et un corps trop potelé, tous les nutritionnistes vous le diront, ce n'est pas bon pour la santé.

MYTHE N° 6 :

L'IPv6 VA RESOUDRE TOUS LES PROBLEMES EVOQUES

L'IPv6, nouveau protocole de l'Internet, résout le problème du nombre d'adresses IP devenu très insuffisant, avec l'IPv4, pour satisfaire aux exigences de la demande pour les objets communicants, pour les voitures électriques, pour la grille électrique et d'une manière générale pour l'explosion du nombre d'utilisateurs. Un utilisateur, en particulier pour la mobilité a besoin aujourd'hui de nombreuses adresses IP. Et les objets intelligents communicants, les étiquettes RFID vont encore faire exploser ce nombre d'adresses nécessaires.

L'IPv6 ajoute également des solutions pour assurer la sécurité, la qualité de service, la mobilité et la diffusion en multicast (un émetteur et plusieurs récepteurs).

Mais l'IPv6 conserve la philosophie de l'IPv4, en particulier celle du mode sans connexion et la notion de "best effort".

Si l'IPv6 n'est pas la solution, faut-il faire table rase de l'existant et repartir à zéro, et non de protocoles couverts de rustines, et de protocoles qui s'empilent et parfois coexistent mal entre eux, comme le préconisent plusieurs chercheurs, tels John Day et Louis Pouzin qui ont été à la base de l'Internet ?

LE POST-IP

En conclusion de ces mythes et des réponses qu'on peut apporter pour démystifier le phénomène, John Day propose, par exemple, un nouveau socle pour l'Internet, non plus bâti sur les couches IP mais sur un modèle de communication interprocessus (Inter Process Communications : IPC) récursif : les protocoles RINA qu'il décrit dans son livre "Patterns in Network Architecture, a return to fundamentals"

Dans ce nouveau principe, qui est une technologie de rupture par rapport à l'existant, le réseau n'est plus un moyen de transporter les données mais un mécanisme d'échange entre processus qui transportent les données. Seuls les processus accèdent aux données qu'ils transportent. L'extérieur n'a pas accès aux adresses internes, ce qui rend difficiles les attaques classiques, basées sur la connaissance des adresses IP vulnérables, pour compromettre les données et renforce la sécurité.

Si le mode avec connexion et le mode sans connexion se rencontrent pour assurer un transport de l'information sûr et performant, dans une architecture où les IPC remplaceront le modèle en couches, et se dupliqueront de manière récursive pour s'adapter aux réseaux physiques, il est certain que l'Internet du futur pourra reposer sur un socle plus solide que celui sur lequel repose l'Internet d'aujourd'hui.

MYTHES ET LEGENDES DE LA SECURITE DE L'INFORMATION

*Gérard Peliks, CASSIDIAN
an EADS Company*

LES AGRESSIONS, ÇA N'ARRIVE PAS QU'AUX AUTRES

Bien calé dans votre fauteuil, vous lisez votre messagerie, parfois vous participez aux forums sur les vulnérabilités et les menaces pouvant peser sur votre système d'information, et de temps en temps vous prenez connaissance des dernières alertes des CERT.

Oui, bien des gens n'ont pas de chance de se faire ainsi agresser. Mais pas vous ! Parmi les dizaines de milliers de logiciels malveillants qui tournent en permanence sur les réseaux, guettant la moindre faille autour de votre PC, comment faites-vous pour toujours passer au travers ? Qu'il est merveilleux, ce sentiment de sécurité qui entoure votre Information ! Sentiment de bien-être encore accru par l'assurance que les contre-mesures que vous avez mises en œuvre, en particulier votre antivirus et votre firewall personnel vous garantissent de ne jamais être concernés par les horreurs qui se passent chez les autres !

Mais la réalité est que la sécurité de l'Information, avec laquelle vous vivez en apparence, est un mythe ! L'insécurité est l'état normal et, comme vos voisins, vous subissez aussi des agressions et parfois celles-ci passent et font des dégâts.

Le véritable danger d'ailleurs n'est pas tellement au niveau des menaces qui vous environnent mais se situe entre votre chaise et votre clavier. Le véritable danger, pesant sur votre information, c'est vous, si vous ne mesurez pas combien est dangereux le monde qui vous entoure.

MYTHE N° 1 :

IL EXISTE DES HAVRES DE PAIX SUR L'INTERNET

Les virus, les vers, les chevaux de Troie, concernent les utilisateurs des PC sous Windows. Votre PC tourne sur une distribution de Linux (Ubuntu, Mandriva ?) et donc les virus ne sont pas dirigés contre vous, puisque sous Linux il n'y en a pas ? Erreur, il existe des logiciels malveillants sous Linux aussi.

Alors, tournons nous vers les MAC puisque là au moins nous sommes tranquilles ? Erreur, il existe aussi des logiciels malveillants dédiés aux MAC. Mais votre Smartphone n'est pas sous Windows et ce n'est pas un MAC ? Vous avez raison sur ce point mais c'est aussi un mythe qu'il n'y a pas de logiciels malveillants pour Smartphones, et plus il y aura de PC sous Linux, plus il y aura de MAC, plus il y aura de smartphones et de eBooks, plus il y aura de virus qui les prendront pour cible. Et ce n'est pas tout.

L'imprimante de votre entreprise n'est pas plus à l'abri que le sont vos postes de travail. Une imprimante en réseau est, comme tout serveur, un nœud sur l'Intranet et comme tout nœud d'un réseau, elle est menacée dans son fonctionnement tout d'abord. Que diriez-vous si votre imprimante, dès qu'elle est alimentée, imprimait à longueur de journée, rame après rame, parce qu'elle serait victime d'une campagne de spam que vous ne pouvez arrêter qu'en payant une rançon ? Le chantage visant une entreprise est un marché qui commence à devenir florissant, et qui pourrait bien un jour se généraliser.

Votre imprimante pose de plus un problème côté confidentialité des informations qu'elle a imprimées. Non ce n'est pas parce qu'une main inavouable récupère systématiquement, avant vous, sur votre imprimante, les informations confidentielles que vous venez d'imprimer, encore que ça peut arriver. Ce n'est pas non plus que vous ne vous méfiez pas assez du spool. Votre imprimante a un disque dur dans lequel les impressions sont stockées. Et quand vous restituez votre imprimante à la société qui vous l'a louée, pour vous équiper d'une imprimante plus moderne ou mieux adaptée, vos informations résident toujours sur son disque dur. Et voilà comment, des informations confidentielles depuis longtemps stockées sur une imprimante, alors que ses utilisateurs n'en avaient pas conscience, changent de main.

On a aussi beaucoup parlé des dangers que font courir les documents de la suite Office de Microsoft, suite aux macrovirus qui présentent effectivement un réel danger. Heureusement, la transmission de documents au format PDF est la solution ? Elle ne l'est plus. Les fichiers PDF, qui peuvent être aussi contaminés, représentent aujourd'hui un des trois principaux vecteurs d'infection.

Alors vers quoi vous tourner ? Sur 360 degrés, vous êtes menacés. Il faut apprendre à vivre dangereusement et comme il n'est pas possible d'éliminer tout danger, il faut chercher à le réduire à un niveau acceptable. C'est ce qu'on appelle le risque résiduel, qu'il faut savoir accepter et gérer.

MYTHE N° 2 :

LES EXECUTABLES EN ".EXE", VOILA LE DANGER !

Au début, il y avait les virus, constitués d'instructions qui s'accrochent à un programme exécutable. Le virus libère sa charge létale quand le programme, auquel il est accolé, s'exécute. Si vous ne lancez pas l'exécutable contaminé, le virus reste inactif. Et comme le virus modifie la taille de l'exécutable, en fonction du contenu et de la taille de ses instructions, la modification qui est la signature du virus, une fois connue, peut être éradiquée de l'exécutable pour le faire revenir à son état sain. C'est ainsi que procèdent les anti-virus. Contrairement à ce qu'on croit généralement, les virus ne se dupliquent pas. L'infection ne peut se répandre que si on transmet l'exécutable contaminé, par exemple en attachement à un e-mail.

Mais Il existe une autre famille de logiciels malfaisants, les vers (worms en anglais) qui eux ne sont pas attachés à un exécutable. Ils sont eux-mêmes des exécutables autonomes et ils investissent votre PC en passant, à travers le réseau, par une faille non couverte affectant un des logiciels que vous utilisez. Une fois installés chez vous, ils se dupliquent et, toujours par le réseau, se répandent un peu partout chez les autres utilisateurs. On pourrait juste vous reprocher d'être connectés !

Les vers forment une famille bien plus nombreuse et bien plus dangereuse que les virus, et c'est pourquoi, croire que n'exécuter que des fichiers ".exe", ".zip" ou autres fichiers avec du code exécutable de confiance, pour ne pas être infecté, est un mythe.

Croire que la messagerie est le seul vecteur d'infection avec les fichiers exécutables attachés aux messages que vous recevez est aussi un mythe. Le vecteur principal d'infection aujourd'hui est le Web.

Il suffit de naviguer sur des pages Web contaminées et vous récoltez des programmes malfaisants contenus dans des pages que votre navigateur télécharge avant de les interpréter. Une page Web, apparemment anodine, peut contenir beaucoup d'éléments exécutables, comme des applets Java, des ActiveX, des codes JavaScript, des Flashes ... Les cybercriminels piègent des sites, même les plus honnêtes, surtout les plus lus. C'est ce qu'on appelle l'infection "drive by download" très répandue. Aujourd'hui le Web devance la messagerie

comme premier vecteur d'infection et. Les fichiers PDF viennent juste après la messagerie dans le classement des éléments dangereux.

MYTHE N° 3 :

LES CYBERCRIMINELS VEULENT DETRUIRE VOTRE SYSTEME D'INFORMATION

Attaquer les systèmes d'information pour éprouver la délicieuse poussée d'adrénaline qui vient avec l'agression du système d'information d'une entreprise, si possible grande et connue, pour le détruire et en entendre ensuite parler; attaquer les réseaux pour prouver qu'après tout on n'est pas incompetent, et les plaintes que poussera l'entreprise en seront une preuve éclatante, c'est du passé et ce type d'attaques ludiques est devenu un mythe, sauf si une cyberguerre se déclenche ou si le cyberterrorisme frappe, ce qui est un autre problème.

Aujourd'hui les cybercriminels attaquent le réseau pour un motif tout aussi inavouable que pour le détruire et leurs attaques sont plus feutrées. Ils mènent leurs attaques pour gagner de l'argent facilement et sans prendre trop de risques. Il est moins périlleux en effet d'attaquer les coffres virtuels d'une banque située à 10 000 km de distance, par l'Internet, depuis un pays où la législation concernant le cybercrime est quasi inexistante, en utilisant un PC et une connexion haut débit, que d'utiliser un camion bélier, un fusil à pompe et un chalumeau, sur place.

Attaquer pour des raisons pécuniaires change les attaquants, les attaques et les cibles. Les attaquants sont souvent des groupes de cybercriminels, parfois sans compétence informatique particulière, mais utilisant des outils conviviaux qu'on trouve dans l'underground de l'Internet, les "kiddies tools". Vous y trouvez même des kits "prêts à l'emploi".

Ces attaques sont silencieuses et les vecteurs d'infection, comme chevaux de Troie et bots spécialisés s'insèrent sans dégâts visibles dans les systèmes d'information des victimes ciblées. Aux virus dévastateurs succèdent les familles de chevaux de Troie, qui sont des bots, pour relayer les attaques, et des vers qui ne veulent surtout aucun mal à votre outil de travail et à vos informations, seulement à vos comptes bancaires. Bien au contraire, ils ont intérêt à ce que tout marche parfaitement chez vous. Mais tapis au fond de votre disque dur, ils observent. Les logiciels malfaisants attendent leur heure...

Et quand vous saisissez l'adresse Web de votre établissement bancaire, alors ils se réveillent et captent l'information que vous entrez : login, mot de passe, numéro de compte, date d'expiration de votre carte de crédit, tout est intercepté et envoyé au cybercriminel. Et ainsi le marché du renseignement sur les victimes potentielles est alimenté et rapporte gros. Il existe des keyloggers qui vont chercher l'information au niveau des touches du clavier que vous utilisez.

Vous pouvez certes chiffrer votre information sur votre PC, mais ce que vous tapez sur les touches de votre clavier, c'est de l'information en clair. La question hélas ne sera pas, avec la généralisation de la cybercriminalité, de savoir si vous avez ou pas un cheval de Troie dans votre système d'information, mais plutôt combien vous en avez, qui se battent en duel pour être peu nombreux à bénéficier de vos ressources informatiques.

MYTHE N° 4 :

LA SECURITE DE L'INFORMATION EST UN CENTRE DE COUT

Bien entendu s'équiper des matériels et logiciels indispensables, s'entourer d'experts sécurité compétents a un coût. Maintenir et bien gérer le système, établir des tableaux de bord conformément à sa politique de sécurité, et aux standards, exploiter les résultats des

événements, des vulnérabilités, des non-conformités n'est pas une tâche anodine et mobilise des ressources humaines et pécuniaires.

Le coût de la sécurité pèse en général sur le budget informatique, et constitue parfois, hélas pour les victimes futures, une variable d'ajustement des budgets, surtout en temps de crise.

Mais l'insécurité a-t-elle un coût ? Si une entreprise victime d'une agression qui lui a fait perdre son fichier clients, l'historique de ses commandes, ses secrets de fabrication, son image de marque, et entaché la moralité de ses dirigeants, est appelée à disparaître à court terme après une attaque réussie, le coût de l'insécurité sera supporté par l'ensemble de l'entreprise, quand celle-ci devra fermer ses portes.

Mais si vous croyez que la sécurité est trop chère... essayez l'insécurité" ☺

MYTHE N° 5 :

LES ATTAQUES VIENNENT DE L'EXTERIEUR

Le côté obscur de la force qui pèse sur votre information peut certes venir de l'extérieur où une cohorte d'individus malfaisants menace vos finances et vos ressources. Ca ce n'est pas un mythe. Mais le mythe serait de croire que les méchants sont toujours à l'extérieur.

Le firewall qui isole votre réseau en bâtissant un périmètre de sécurité autour de votre système d'information et filtre tout ce qui sort et ce qui entre conformément à votre politique de sécurité est indispensable. Mais il ne sait pas ce qui se passe dans votre Intranet.

Les systèmes d'information aujourd'hui ne sont plus des places fortes qui doivent être entourées d'un rempart imprenable. Ils se rapprochent plus de pays avec des frontières, des ports mais aussi des aéroports d'où l'on peut pénétrer sans passer par les frontières. Sans compter, pour le criminel, la possibilité d'être parachuté près d'un endroit sensible. Il faut donc sécuriser plus que le périmètre de sécurité extérieur de votre entreprise. C'est d'autant plus vrai avec les technologies sans fils, le Peer to Peer, le Cloud Computing, qui, s'ils rendent des services indiscutables, n'en ouvrent pas moins des brèches dans le périmètre de sécurité d'une entreprise. Il faut aussi mettre des contre-mesures à l'intérieur de votre réseau d'entreprise.

Les employés sont-ils des méchants quand l'occasion fait le larron ? Pas tous, bien sûr, mais il faut garder à l'esprit qu'au moins 60% des attaques qui réunissent, ont pour origine l'intérieur de l'entreprise, ou au moins des complicités dans l'entreprise.

MYTHE N° 6 :

LE CYBERMONDE EST UN ESPACE DE NON DROIT

La multiplication des attaques, largement plus médiatisée que les peines qui pourtant frappent les attaquants qui se font prendre, peut laisser penser que le cyber monde est un espace de non-droit où les malveillants, les maîtres chanteurs, les indéclicats peuvent œuvrer en toute impunité et leurs victimes se faire agresser ou plumer sans recours. Il n'en est rien.

Mais comme l'Internet ne connaît pas de frontières, il n'est pas toujours évident de déterminer quelle juridiction s'applique. Droit du sol où le serveur Web malveillant réside ? Nationalités des agresseurs ? Nationalités des victimes ? Pays où se passe l'agression ? En France, l'article 113-2 du nouveau code pénal répond en partie à ces questions. Il s'appuie sur le principe de territorialité, établit que « *l'infraction est supposée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire* ».

Nous allons évoquer ici seulement des lois qui s'appliquent en France. N'étant pas juriste, je n'entrerai pas dans les détails. Chaque pays a ses propres lois et ses accords croisés avec d'autres pays ou communautés de pays et bien sûr les agresseurs avertis lancent de

préférence leurs attaques à partir de pays où la législation est très floue et l'extradition difficile. C'est bien sûr aussi dans ces mêmes pays que sont hébergés souvent les serveurs délictueux et les maîtres des Botnets.

En France, contrairement à ce qu'on peut croire, le cybercrime est encadré. Des lois existent et la jurisprudence commence à s'étoffer. D'ailleurs, plusieurs lois datant d'avant même la généralisation de l'utilisation de l'Internet sont applicables, telles les lois dites Godfrain, du 5 janvier 1985, articles L.323-1 et suivants du Nouveau Code pénal qui punissent les *atteintes au système de traitement automatisé de données* et prévoient des amendes et des peines de prison même si aucune incidence directe n'a perturbé le système pénétré.

Mais le système judiciaire ne peut intervenir que si la victime ne tait pas le délit commis par l'attaquant et le préjudice subi et que si elle porte plainte.

Avec la volatilité des preuves, la difficulté de les tracer, l'anonymat facile, l'absence de frontières et une présence policière limitée, le cybermonde réunit tous les ingrédients pour être le théâtre d'un crime parfait, à moins que les victimes ne réagissent efficacement.

Si vous vous apercevez que vous avez été attaqués et avez subi des préjudices mais si vous ne portez pas plainte, l'agresseur ne sera sûrement pas inquiété. Si par contre vous portez plainte auprès de l'autorité compétente, il reste une petite chance pour que l'agresseur soit inquiété et cesse de s'attaquer à vous et aux autres. Comme avec l'Internet nous sommes tous liés, améliorer sa sécurité, c'est aussi améliorer la sécurité des autres.

Un web de signalement des infractions a été mis en place par le Ministère de l'intérieur, n'hésitez pas à l'utiliser, c'est ainsi que la vie peut devenir plus dure pour les cybercriminels :

www.internet-signalement.gouv.fr

MYTHES ET LEGENDES DES RISQUES DE CYBERGUERRE SUR LES INFRASTRUCTURES VITALES

Franck Franchin, FRANCE TELECOM

INTRO

A faire

MYTHE N° 1 :

LES SYSTEMES CRITIQUES SONT PROTEGES DES ATTAQUES GRACE A LEUR REDONDANCE

Dans de nombreux secteurs d'activité industrielle, 2 ou 3 fournisseurs se partagent désormais le marché des systèmes de commande et de contrôle, sous forme d'un duopole ou d'un oligopole. Cela entraîne que la redondance des systèmes à caractère critique est souvent assurée par le même logiciel ou le même matériel, simplement dupliqués, afin de permettre une redondance à froid ou à chaud.

Que se passe-t-il donc si un système est attaqué ? On peut scénariser une attaque en cinq phases :

- Phase préparatoire de reconnaissance, infiltration et renseignement – ouverture des accès nécessaires à l'attaque
- Phase d'attaque
- Découverte de l'attaque par la victime
- Mesure de défense
- Forensique et post-mortem

Lorsque l'attaque est découverte, la victime peut adopter plusieurs stratégies : arrêter totalement le système et/ou le processus concerné ou basculer sur le système de secours. Grande question : est-ce que le système de secours a été compromis ?

Dans un avion, les commandes vols vitales sont doublées, via des technologies différentes : câbles électriques, fibres optiques, hydraulique et passent par des chemins physiques différents. Il existe aussi des modes dégradés lorsque la redondance des systèmes est trop complexe ou trop coûteuse à implémenter.

Avec un système informatique, comment s'assurer d'une vraie redondance quand le système d'exploitation est du même fournisseur, voire de la même version, sans même parler du même logiciel métier. Comment être sûr que le système de secours est à la fois 'isofonctionnel' (et donc mis à jour comme le système 'en production') ?

Si on prend comme référence la fameuse affaire Stuxnet/SCADA, la préconisation de Siemens une fois l'attaque connue fut... de ne surtout toucher à rien et surtout de ne pas changer le mot de passe qui était pourtant codé en dur dans les programmes ! Le remède risquait d'être plus grave que la maladie. On parle pourtant de systèmes à plusieurs millions d'euros qui régulent et pilotent des centrales nucléaires, des usines chimiques et autres activités à risque.

Il y a donc redondance et redondance. Quand on implémente la redondance de deux baies de disques durs amenées à stocker des données très sensibles, on utilise des processus logiques et physiques de redondance à froid et à chaud (les fameux disques durs hot plug ou les modes de type RAID) mais on s'assure aussi que les disques durs eux-mêmes ne

proviennent pas du même fabricant pour chaque baie. Et si ce n'est pas possible, on prend des lots fabriqués à des dates différentes pour ne pas risquer un même défaut de fabrication.

Il est beaucoup plus difficile d'appliquer cette saine philosophie dans le monde informatique des logiciels.

Un exemple très simple : imaginez que vous soyez journaliste, que votre outil critique soit votre traitement de texte et que vos missions nécessitent une disponibilité de votre outil à 100%. La solution pour s'affranchir des attaques informatiques consisterait à avoir un ordinateur PC sous Windows et un autre ordinateur Apple sous MacOS. Au niveau logiciel vous pourriez avoir un OpenOffice d'un côté et un Microsoft Word de l'autre. Cela fonctionnerait très bien tant que le journal pour lequel vous travaillez n'ait pas choisi d'implémenter des macros spécifiques Word qui n'existent pas sous OpenOffice. La solution serait alors d'être iso-outil et d'avoir Word sur les deux machines. Sauf que Word sous Windows et Word sous MacOS ne sont pas totalement iso-fonctionnels, voire compatibles (selon l'éditeur, cela serait corrigé dans la version 2012). La seule solution définitive serait alors d'avoir deux ordinateurs PC avec Word sous Windows, l'un sous Windows Seven, l'autre sous Windows XP, par exemple. En espérant que les macros se comportent exactement de la même manière sous les deux systèmes exploitation.

Hélas, le choix est encore plus limité pour les systèmes de commande et de contrôle en milieu industriel. Le système de redondance est donc très souvent une copie synchronisée du système en production, avec bascule des données, voire des données de session. La meilleure façon d'avoir deux systèmes aux vulnérabilités strictement identiques.

Cela signifie que la meilleure redondance reste souvent la décision et l'arbitrage humain. Encore faut-il que l'attaque ait été décelée à temps. Dans l'exemple précédent de Stuxnet, l'attaque modifiait certains paramètres bien particuliers de processus industriels très complexes. Seules les victimes savent réellement le temps qu'a duré l'attaque avant qu'elles ne s'en aperçoivent. Certaines centrifugeuses iraniennes ont eu des baisses de rendement inexplicables bien avant qu'on évoque du bout des lèvres l'éventualité de Stuxnet...

MYTHE N° 2 :

INTERNET EST UNE INFRASTRUCTURE CRITIQUE PRIMORDIALE

A faire

MYTHE N° 3 :

NOUS AURONS UN PEARL-HABOR DIGITAL DANS LES DIX PROCHAINES ANNEES

Cette phrase est extraite d'une audition d'expert devant le Sénat américain en 1998 (retrouver la référence). Que s'est-il passé depuis ? Des événements bien plus graves qu'un Pearl Harbor digital : l'affaire Madoff, la crise des surprimes, le dépôt de bilan virtuel des PIGs, la Corée du Nord qui joue avec le feu. Qu'en penser ?

Suite...

MYTHE N° 4 :

LE CYBER-TERRORISME EST UNE MENACE IMPORTANTE

A faire

MYTHE N° 5 :

LA GUERRE DE TROIE N'AURA PAS LIEU

A faire

MYTHES ET LEGENDES DES VULNERABILITES LOGICIELLES

Nicolas Ruff, EADS Innovation Works

MYTHE N° 1 :

TROUVER DES VULNERABILITES , C'EST COMPLIQUE (RESERVE AUX EXPERTS)

Dans le domaine des failles de sécurité, il y a bien deux compétences disjointes (souvent détenues par des personnes différentes d'ailleurs): la découverte des failles, et la transformation des failles en attaques (appelée *exploitation* ou simplement *exploit* dans le jargon).

Si la deuxième compétence reste et restera réservée aux experts techniques, il est au contraire à la portée de n'importe qui de découvrir des failles.

Vous avez reçu un document endommagé qui fait "planter" Word ? Vous avez peut-être entre les mains une bombe !

Vous avez rempli un formulaire en ligne et le serveur vous a retourné un message incompréhensible car vous avez un guillemet simple (') dans votre nom de famille ou dans votre mot de passe ? Vous avez peut-être trouvé un moyen de compromettre à distance le serveur !

En pratique, quiconque a pratiqué l'audit de sécurité pendant quelques années a forcément découvert des vulnérabilités dans des dizaines de logiciels pourtant largement utilisés. Il y a un fossé entre le sentiment de sécurité des utilisateurs (souvent béats devant la technologie), et la sécurité effective de leurs applications.

COROLAIRE: UN LOGICIEL QUI N'A AUCUNE VULNERABILITE CONNUE EST "SUR"

Archifaux ! Un logiciel qui n'a aucune vulnérabilité connue n'a jamais été audité sérieusement et/ou son éditeur n'a pas de processus sérieux de gestion des vulnérabilités (ce qui inclut correction et communication).

MYTHE N° 2 :

MAINTENANT QUE LA SECURITE EST DEVENUE UN ENJEU IMPORTANT POUR LES EDITEURS, LE NOMBRE DE VULNERABILITES VA DIMINUER

Il est certain que la sécurité informatique n'a jamais bénéficié d'autant de couverture médiatique (n'allons pas jusqu'à dire de moyens :). Pourtant le nombre de nouvelles vulnérabilités ne baisse pas - il a même plutôt tendance à augmenter !

La raison ? C'est que la plupart des "gros" logiciels que nous utilisons actuellement a été développée il y a fort longtemps, dans un monde très différent du nôtre. Un monde où les quelques personnes interconnectées l'étaient via RNIS, et où la principale menace était la disquette. Pour des raisons de coût et de compatibilité, ces logiciels ne sont pas prêts d'être réécrits.

Et en ce qui concerne les nouveaux logiciels qui sont développés actuellement ? Ils le sont par des stagiaires ou des sous-traitants *offshore*, qui reproduisent exactement les mêmes erreurs qu'il y a 30 ans !

MYTHE N° 3 :

TOUT LE MONDE EST TRES CONCERNE PAR LA DECOUVERTE DE VULNERABILITES CRITIQUES

On pourrait penser que la découverte d'une vulnérabilité critique dans un logiciel est un évènement sérieux qui va impliquer toutes les parties prenantes.

Pourtant l'utilisateur (ou le client, s'il ne s'agit pas d'un logiciel gratuit) ne peut pour ainsi dire rien faire : il doit attendre le correctif de l'éditeur.

L'éditeur quant à lui dispose de ressources et de connaissances en sécurité limitées (c'est pour cela que ses produits sont vulnérables ;). Il va donc au choix : minimiser la portée de la découverte, intégrer le correctif dans une future maintenance, ou proposer un correctif spécifique (parfois payant) au client.

Quant aux autres utilisateurs du logiciel, ils sont rarement prévenus : les éditeurs n'aiment pas trop qu'on parle de leurs failles sur la place publique.

Et ceci dans le meilleur des cas, car parfois l'auditeur (ou son client) sont poursuivis en justice par l'éditeur du logiciel pour violation de licence !

MYTHE N° 4 :

CORRIGER LES VULNERABILITES AMELIORE LA SECURITE DES SYSTEMES

Cela pourrait être vrai dans un monde où tous les systèmes sont mis à jour en temps réel. Malheureusement la plupart des systèmes du monde "réel" sont mis à jour entre 24h et ... jamais !

Ceci est particulièrement vrai dans le domaine des systèmes embarqués (sans parler de SCADA). On peut considérer par exemple que l'énorme majorité des téléphones portables n'est pas mise à jour après sa commercialisation. Un téléphone sous Android restera donc vulnérable à toute faille affectant le noyau Linux et/ou le navigateur Chrome après sa sortie.

A contrario, il faut souvent moins de 24h à un attaquant motivé pour produire une attaque à partir d'un correctif de sécurité. Sans parler de l'auteur initial de la découverte, qui est libre de l'exploiter à loisir tant que le correctif n'est pas disponible, ce qui prend parfois des années !

Ce problème a déjà été retourné dans tous les sens - et il n'admet pas de solution satisfaisante pour toutes les parties. Il est impossible de ne pas mettre au courant les clients des failles sans en informer également les pirates.

MYTHE N° 5 :

IL EXISTERA UN JOUR DES LOGICIELS GRAND PUBLIC INVULNERABLES

Est-ce que nos enfants (ou nos petits-enfants) pourront utiliser un jour un "système de traitement automatisé de données" (quel qu'il soit) en toute fiabilité ? Probablement pas. D'ailleurs c'est plutôt l'inverse qui est en train de se produire: aujourd'hui, la "panne informatique" est invoquée pour justifier à peu près toutes les erreurs et tous les dysfonctionnements.

La réduction des coûts à outrance, la déqualification des métiers techniques comme l'ingénierie logicielle, la course à l'immédiateté (et la culture du "patch" qui l'accompagne) ont tendance à diminuer la qualité de la production logicielle.

A titre anecdotique, on peut citer l'exemple des jeux vidéo dont la version vendue en magasin est non fonctionnelle - les éditeurs ayant mis à profit le temps de pressage et de distribution des CD-ROM pour finir le développement du logiciel, et fournir le tout sous forme d'un patch à télécharger.

Sans parler évidemment des vulnérabilités qui sont introduites volontairement par l'éditeur (aussi appelées backdoors), souvent dans le but de faciliter le support client ... Vous avez oublié votre mot de passe de 30 caractères ? Pas de problème, le technicien saura vous dépanner !

On peut donc conclure sur une note positive en affirmant que la recherche de vulnérabilités logicielles a de beaux jours devant elle !

MYTHES ET LEGENDES DES VERS, VIRUS ET TROJANS

David Grout, McAfee

MYTHE N° 1 :

LES EDITIONS D'ANTIVIRUS ECRIVENT EUX-MEMES LES CODES MALVEILLANTS:

Dès que je suis arrivé dans ce domaine en 2003 ce fut la première remarque de l'un de mes clients... « Mais c'est vous qui générez tous ces codes pour vous mettre en valeur à travers vos protections et nous vendre vos solutions ». Vaste question, que d'interrogations, serait-ce possible ?... Une investigation devenait alors nécessaire. Après quelques recherches sur l'Internet je me rendis compte que les vers les plus répandus de cette époque l'étaient en fait à travers des codes générés par des scripts Kiddies (nous en reparlerons dans un prochain mythe). 7 années plus tard en 2010 l'ensemble de mes interrogations sur le sujet est levé et sans ambiguïtés, en effet les laboratoires d'un éditeur de sécurité reçoivent en moyenne 1000 nouveaux codes malveillants par heure.

On comprend aisément deux choses, les éditeurs de sécurité n'ont pas besoin de se faire de la publicité, le mal est réel, et de plus le volume est si considérable que les entreprises d'aujourd'hui n'auraient même pas la capacité humaine de générer tous ces codes.

Pour conclure, il est sur qu'aujourd'hui l'écriture de codes de malveillants n'est pas fait par les éditeurs de sécurité, ils ont déjà un travail herculéen à les contrecarrer.

MYTHE N° 2 :

LES CODES MALVEILLANTS SONT ENFANTINS A GENERER :

Cette phrase est la citation préférée de tous les « geeks » en élaboration de codes malveillants, autrefois appelés les scripts kiddies terme qui était au départ plutôt péjoratif dans la communauté mais que j'emploierai plus pour englober les personnes et les utilitaires permettant à n'importe quelle personne de générer par lui-même un code malveillant.

Malheureusement nous sommes passés depuis quelques années dans une autre dimension de la sécurité et de la malveillance, car aujourd'hui l'argent est le vecteur premier de reconnaissance. Finie l'époque où l'on souhaitait juste défigurer un site Internet et y mettre son nom pour, comme disent les enfants, montrer que « l'on est capable de le faire ». Aujourd'hui même si ce type d'attaque existe toujours, il est aisément contré par des dispositifs de sécurité de « base » comme les antivirus, firewall.

Depuis quelques années la génération de codes malveillants se complexifie et est le fruit d'équipes complètes de personnes présentant des compétences multiples et très pointues dans différents domaines. Il existe même à ce jour des entreprises dédiées à l'écriture de codes malveillants (avec un SAV oui oui !!!), nous sommes passés de la reconnaissance d'un nom à la reconnaissance financière.

Les dernières attaques en dates appelées aussi APT (Advanced Persistent Threats) telles que Aurora ; Stuxnet le démontrent. Le code malveillant est devenu aujourd'hui une chose extrêmement complexe motivée par le plus vieux moteur du monde : l'Argent. Il ne faut pas oublier aussi l'utilisation de cette menace, ou de cette arme qu'est le code malveillant à un niveau étatique. Aujourd'hui la démobilisation d'un pays par un malware serait-elle possible : Die Hard 4 est-il si loin de nous ?....

MYTHE N° 3 : **C'EST SUR LES PC SOUS WINDOWS QUE LES VIRUS ATTAQUENT**

Un mythe qui nous tient, je dirais même qui nous colle ... Et oui les virus attaquent Windows mais pas seulement. Le concept aujourd'hui d'une attaque malware est de gagner de l'argent, alors pourquoi Windows ? Tout simplement parce que la part de marché de cet OS est la plus conséquente donc potentiellement les cibles offertes par Windows sont les plus nombreuses.

Mais aujourd'hui avec l'évolution et l'ouverture des plateformes on voit des virus sur MAC, sur Linux et encore plus aujourd'hui sur IOS (Apple OS). Une chose est sûre : la seule motivation et le seul vecteur est l'argent, alors plus un OS est utilisé par des populations sensibles en entreprises plus ces OS seront visés. Il y a fort à parier que 2011 sera l'année du mobile et ce dans tous les sens du terme.

Dernier élément qui casse définitivement ce mythe, parmi les attaques ciblées à des fins financières mais aussi politiques, les malwares visent aussi des OS inconnus du grand public : SCADA avec l'attaque Stuxnet en est un.

Donc pour conclure, aucun OS n'est à l'abri et au vu du peu de couverture que les entreprises consacrent à des environnements « non standards » comme Linux ou MAC, il est sûr qu'en tant que si j'étais un hacker, mon choix de cible primaire serait vite fait ...

MYTHE N° 4 : **UNE MISE A JOUR DE LA BASE ANTIVIRALE PAR SEMAINE ET JE SUIS TRANQUILLE**

Commençons par quelques chiffres : En 2003 l'éditeur pour lequel je travaille annonçait que nous franchissions la barre mythique des 200 000 souches virales couvertes par les signatures antivirales. Aujourd'hui ce chiffre est atteint tous les 4 jours... Oui, oui vous lisez bien, aujourd'hui une base de signatures couvre 42 millions de souches et augmente en moyenne de 50 000 échantillons par jour.

Alors oui, on peut se mettre à jour toute les semaines le risque n'est que de 350 000 infections potentielles. Aujourd'hui il est clair que le niveau de mise à jour se doit d'être continu. Cependant les éditeurs sont confrontés à une problématique que n'ont pas les hackers, le risque de "faux positif". En effet, un faux positif, ou une détection erronée d'un fichier sain, peut avoir des conséquences désastreuses, c'est pour cela que les firmes antivirus sont contraintes à des tests de qualifications et qualités multiples avant la publication de leurs signatures.

La solution aujourd'hui est complexe mais le marché va vers la sécurité à travers des signatures pour une base validée et testée à laquelle s'ajoute une approche « In the Cloud » ou en temps réel en cas de suspicion forte sur un fichier, même si celui-ci n'est pas détecté par la signature classique. Mais il faut retenir que même si ce type de protection tend vers une couverture complète, elle ne reste néanmoins qu'une protection réactive. L'avenir de la protection se situe aujourd'hui dans la pro activité et surtout la prédictibilité, un énorme challenge ...

En attendant mettez vous à jour antivirale le plus souvent possible, voici un mythe qui n'en n'est pas un !

MYTHE N° 5 :

IL NE SE PASSE RIEN DE SPECIAL SUR MA MACHINE C'EST DONC QUE TOUT VA BIEN

Une vieille croyance du monde de l'informatique est que si rien ne se passe d'étrange c'est que tout va bien ... Je dirais que cela n'est pas faux dans 95% des cas, mais que se passe t'il dans les 5% restant ?

Vous allez vous dire, mais il est parano celui là ? Il voit des malwares partout ! Vous n'avez pas tort, mais aujourd'hui il existe une catégorie de malware encore mal perçue par les utilisateurs, les Trojans (ou chevaux de Troie) qui veulent récupérer de l'argent de manière silencieuse.

Le concept n'est plus comme dans le cas de virus massif, de faire tomber une machine (ex : conficker) ou de créer un réseau de robots qui ciblera des sites web pour les faire tomber, mais un concept vraiment différent. L'idée globale est pour l'assaillant de venir s'inviter sur le poste de sa cible sans que celle-ci s'en aperçoive, à travers l'utilisation de rootkits par exemple.

Ensuite le jeu est de faire évoluer son code de manière sensible afin de ne jamais alerter les outils de protections locaux, puis une fois le virus installé et actif , d'ouvrir une porte entre la machine attaquée et l'Internet (Backdoor). Lorsque ces étapes sont réalisées alors l'assaillant commence à lancer des commandes et à récupérer de l'information : captures d'écran, fichiers sensibles ... et ceci en petits morceaux afin de ne jamais éveiller le doute...

Si vous venez de lancer votre gestionnaire de tâches, votre "regedit" et que vous recherchez des traces c'est que vous aussi vous êtes devenu paranoïaque...

Mais si il ne se passe rien sur votre machine, alors peut-être qu'il ne se passe réellement rien ?...

MYTHES ET LEGENDES DU CHIFFREMENT

*Gérard Peliks, CASSIDIAN
an EADS Company*

QUELQUES MOTS A MAITRISER QUAND ON PARLE DE CRYPTOLOGIE

La cryptologie, science des messages cachés, se divise en deux disciplines antagonistes, la cryptographie et la cryptanalyse.

La cryptographie est l'art de transformer un message en clair, en un message incompréhensible. Pour cela le message en clair est traité par un algorithme (un programme) et une clé de chiffrement (un ensemble de bits). La cryptographie est aussi l'art, connaissant l'algorithme et une clé, de retrouver le message en clair à partir du message caché. On parle de "chiffrer" et de "déchiffrer" le message. C'est le chiffre de défense : on cache l'information sauf à celui qui est en droit d'en prendre connaissance.

Mais si on connaît le message chiffré sans connaître la clé pour déchiffrer le message, il est parfois, par calcul, quand même possible d'obtenir le message en clair. C'est la cryptanalyse. On parle alors de "décrypter" le message chiffré. C'est le chiffre d'attaque : on essaie de récupérer un message chiffré alors qu'on n'en est pas le destinataire.

Ceci étant posé, que signifie "crypter" un message ? Cela ne signifie rien et le mot crypter est à bannir du vocabulaire de la cryptologie.

La cryptologie à l'ère numérique est un combat entre les cryptographes qui élaborent des algorithmes toujours plus difficilement cassables, et qui se basent sur des clés toujours plus longues, et les cryptanalystes qui élaborent des méthodes toujours plus efficaces pour retrouver le message en clair sans utiliser la clé.

Par exemple, à l'ère pré-numérique, Scherbius qui avait conçu la première machine Enigma dans les années 1920 était un cryptographe. Les Anglais du Bletchley Parc, durant la seconde guerre mondiale, qui décryptaient les messages, que les Allemands chiffrèrent avec cette machine, étaient des cryptanalystes.

MYTHE N°1 :

LE SECRET DU CHIFFREMENT EST DANS L'ALGORITHME

Non, contrairement à ce qu'on pense généralement, le programme de traitement (l'algorithme) qui transforme, en utilisant une clé de chiffrement, un fichier en clair en un fichier chiffré, n'est ni confidentiel défense, ni même un secret industriel, tout du moins dans un contexte où ce principe a été compris.

Le secret réside dans une clé qui sert à chiffrer un fichier, cas de la signature électronique ou du chiffrement symétrique, ou à déchiffrer ce fichier, cas du chiffrement asymétrique.

Kerckhoffs, à la fin du 19ème siècle avait déjà énoncé ce principe : "le secret du chiffrement ne doit résider que sur le secret de la clé". L'algorithme peut être public.

Et mieux, si l'algorithme est un standard comme par exemple l'AES ou le RSA, une communauté importante d'experts peut essayer de le casser, signale ses failles qui sont alors corrigées, et avec le temps, le code d'implémentation de cet algorithme ne présente plus de vulnérabilité évidente, connue.

Si le code d'implémentation de l'algorithme de chiffrement est jalousement gardé, alors seuls ceux qui ont le droit d'en connaître, donc un nombre infime d'experts par rapport à ceux qui

composent la communauté sur le net, peuvent corriger d'éventuelles erreurs. De plus, quand les experts qui connaissent les méandres d'un algorithme confidentiel ne sont plus disponibles, la connaissance a disparue et la maintenance ne peut plus se faire.

Avec un algorithme public, c'est au niveau de la clé que le secret réside. L'algorithme utilise diverses parties de la clé pour effectuer les transformations qui aboutissent au chiffrement ou au déchiffrement du message. Sans la connaissance de la clé, il est difficile de savoir comment se comporte l'algorithme, donc il est difficile, à partir du message chiffré, de reconstituer le message en clair.

Il existe néanmoins des chiffrements qui reposent sur le secret de l'algorithme. Mais ni Kerckhoffs, ni les cryptologues d'aujourd'hui ne trouvent que c'est une bonne idée et conseillent d'utiliser plutôt les algorithmes standards et éprouvés, et de plus soutenus par la communauté du chiffre.

MYTHE N° 2 :

ON CHIFFRE AVEC SA CLE PRIVEE

Mythe ou réalité, cela dépend.

Pour comprendre ce qui suit et pourquoi le chiffrement qui utilise une clé privée est un mythe, cela nécessite des explications sur les deux méthodes de chiffrement. Le chiffrement symétrique et le chiffrement asymétrique.

Dans le chiffrement symétrique, on chiffre une information en utilisant une clé et un algorithme de chiffrement symétrique tels que le 3DES ou l'AES. On déchiffre avec le même algorithme et la même clé. La clé de chiffrement, dite "clé secrète", est la même que la clé de déchiffrement, c'est pourquoi ce type de chiffrement est dit symétrique. En utilisant la même clé, un coup on chiffre, un coup on déchiffre.

Mais un problème se pose. Celui qui chiffre génère la clé de chiffrement symétrique (la clé secrète), mais comment celui qui va déchiffrer, si ce n'est pas la même personne que celui qui a chiffré, va-t-il entrer en possession de cette clé, qui doit bien sûr rester secrète pendant le transfert ? L'autre gros problème est la multiplication des clés secrètes si on se met à chiffrer et déchiffrer entre un nombre élevé de destinataires. Le chiffrement symétrique est pratique et de plus très rapide, mais suite à la difficulté de transmettre la clé et suite à la multiplication des clés qu'il impose, il est difficilement utilisable en l'état.

Le chiffrement asymétrique met en jeu deux clés mathématiquement liées. Une clé privée qui est un secret et une clé publique dont tout le monde peut prendre connaissance. Quand on chiffre avec un algorithme de chiffrement asymétrique comme le RSA, et avec une des deux clés, on déchiffre avec le même algorithme et avec l'autre clé. Dernier postulat : connaissant la clé publique, il est évidemment très difficile de retrouver la clé privée correspondante.

Vous conservez votre clé privée, de manière idéale sur un token USB ou une carte à puce protégée par un code PIN, et vous donnez à tous ceux qui en ont besoin votre clé publique correspondante, ou alors vous dites où aller la chercher.

Avec quoi chiffrez-vous votre information pour la garder confidentielle ? Avec votre clé privée ? Non bien sûr, réfléchissez. Si vous chiffrez avec votre clé privée, tous ceux qui ont votre clé publique pourront déchiffrer votre information, donc il aura été inutile de la chiffrer et la confidentialité espérée ne sera qu'illusoire.

MYTHE N° 3 :

ON CHIFFRE AVEC UNE CLE PUBLIQUE

Nous avons vu que ce n'est pas avec votre clé privée que vous chiffrez votre information, sinon tout le monde pourrait la déchiffrer.

Alors si ce n'est pas avec votre clé privée, c'est forcément avec l'autre clé, votre clé publique ? Et bien non ! Si vous chiffriez avec votre clé publique, comme personne d'autre que vous n'est censé posséder votre clé privée, pour déchiffrer, à moins que vous chiffrez vos informations pour, seulement vous-même les déchiffrer, ce ne peut être avec votre clé publique. Alors si ce n'est avec votre clé publique, ce pourrait être avec la clé publique de celui à qui vous voulez envoyer votre information chiffrée ?

En effet, comme vous trouvez cette clé publique dans le certificat de celui à qui vous voulez envoyer l'information chiffrée, et comme ce certificat est signé par une autorité de confiance, vous êtes sûr que c'est vraiment la clé publique de votre correspondant, car lui seul possède la clé privée correspondante avec laquelle il va déchiffrer l'information que vous avez chiffrée. Donc tout va bien et c'est comme ça qu'il faut faire ?

Et bien non !

Le chiffrement asymétrique présente un gros handicap : il est cent à mille fois plus lent que le chiffrement symétrique. Cela est dû à ses algorithmes qui sont plus complexes. Si déchiffrer une vidéo prend 5 minutes en chiffrement symétrique et plusieurs heures en chiffrement asymétrique, vous aurez vite choisi quel chiffrement vous désirez utiliser.

Ce n'est donc pas non plus avec la clé publique de votre destinataire que vous allez chiffrer votre information, mais avec une clé secrète symétrique que vous générez. Et cette clé secrète, vous la chiffrez avec la clé publique de votre destinataire. Vous lui envoyez cette clé de chiffrement symétrique ainsi chiffrée. La clé de chiffrement symétrique reste confidentielle durant le transfert puisqu'elle ne peut être déchiffrée que par le destinataire qui seul possède sa clé privée. Avec sa clé privée le destinataire déchiffre la clé secrète, et avec cette clé secrète, il déchiffre l'information qui avait été chiffrée avec cette même clé secrète, par chiffrement symétrique.

En résumé, ce n'est pas avec une clé publique qu'on chiffre une information, mais avec une clé secrète symétrique. La clé publique ne servant ici qu'à chiffrer la clé secrète, par chiffrement asymétrique, et la clé secrète sera ensuite déchiffrée par la clé privée du destinataire.

MYTHE N° 4 :

LE CHIFFREMENT QUANTIQUE, ARME ABSOLUE, DES AUJOURD'HUI

Basé non plus sur des calculs mathématiques mais sur la physique des particules, le chiffrement quantique causera une rupture technologique, dans le monde des cryptographes et des cryptanalystes, c'est dire que leur combat va prendre une dimension nouvelle.

Le calcul quantique permet d'effectuer en parallèle une énorme quantité d'opérations qui s'opérait en série avec les calculateurs classiques. Les ordinateurs vont pouvoir résoudre rapidement les problèmes quasiment insurmontables avec les moyens conventionnels tels que la décomposition d'un grand nombre en facteurs premiers, base du RSA, ou le problème du logarithme discret, base du chiffrement par courbes elliptiques.

Nous n'entrons pas ici dans les détails, mais retenez que le cassage de clés par force brute, c'est-à-dire la recherche de toutes les combinaisons possibles de clés pour arriver à retrouver un message en clair à partir d'un message chiffré, deviendra possible, dans un temps acceptable.

Mais aujourd'hui les ordinateurs quantiques ont un gros défaut : ils n'existent pas, sauf dans les romans de science fiction ou alors à titre expérimental, ils en sont à leurs premiers balbutiements dans des laboratoires de recherche.

Les cryptographes ont ainsi encore des années de tranquillité devant eux. De plus, ils peuvent utiliser la mécanique quantique, et nous ne parlons plus d'ordinateurs quantiques, pour échanger une clé de chiffrement de manière sûre, ce qui était jusque là le gros problème à résoudre pour le chiffrement symétrique.

La mécanique quantique dit qu'un photon tourne autour d'un axe qui est orienté dans une direction qu'on peut lui imposer en jouant sur un champ magnétique. On connaît d'autre part la probabilité que ce photon traverse ou pas un filtre à particules, en fonction de l'angle que fait ce filtre par rapport à l'orientation de l'axe du spin du photon qui essaie de le traverser.

Et merveille des merveilles, pour un cryptographe, si une tierce personne observe le spin d'un photon, son orientation est modifiée. Celui qui reçoit la clé s'aperçoit d'une incohérence avec ce que devait être l'état du photon quand celui-ci a été envoyé.

Cette propriété est utilisée pour échanger la clé de chiffrement de manière sûre, car si un espion entre dans la boucle et observe, la clé envoyée est invalidée et on en essaie une autre.

Le calculateur quantique qui résout les problèmes difficilement traités par les ordinateurs actuels et qui cassent les clés dont la taille rendait jusqu'ici ce passage impossible ou trop coûteux en temps et en ressources est encore un mythe qui va durer quelque temps avant de devenir réalité.

Par contre l'échange sécurisé de clés de chiffrement, qui utilise la mécanique quantique, a dès aujourd'hui des applications, en particulier dans le domaine des télécoms.

MYTHE N° 5 :

LE CHIFFREMENT SEUL MOYEN D'ASSURER LA CONFIDENTIALITE

Une façon d'assurer la confidentialité d'une information est de la chiffrer. Mais il existe un autre moyen, plus pernicieux : cacher cette information, qui reste en clair, dans son contenant. C'est la science de la stéganographie, aussi vieille que la cryptologie, sinon plus.

Avec la stéganographie, l'information à cacher est en clair, mais on ne se doute pas de sa présence. Un exemple physique simple est l'utilisation de l'encre sympathique qui rend invisible un message, sauf quand on chauffe son support. Plus technique, des micropoints peuvent dissimuler une information en la rendant microscopique.

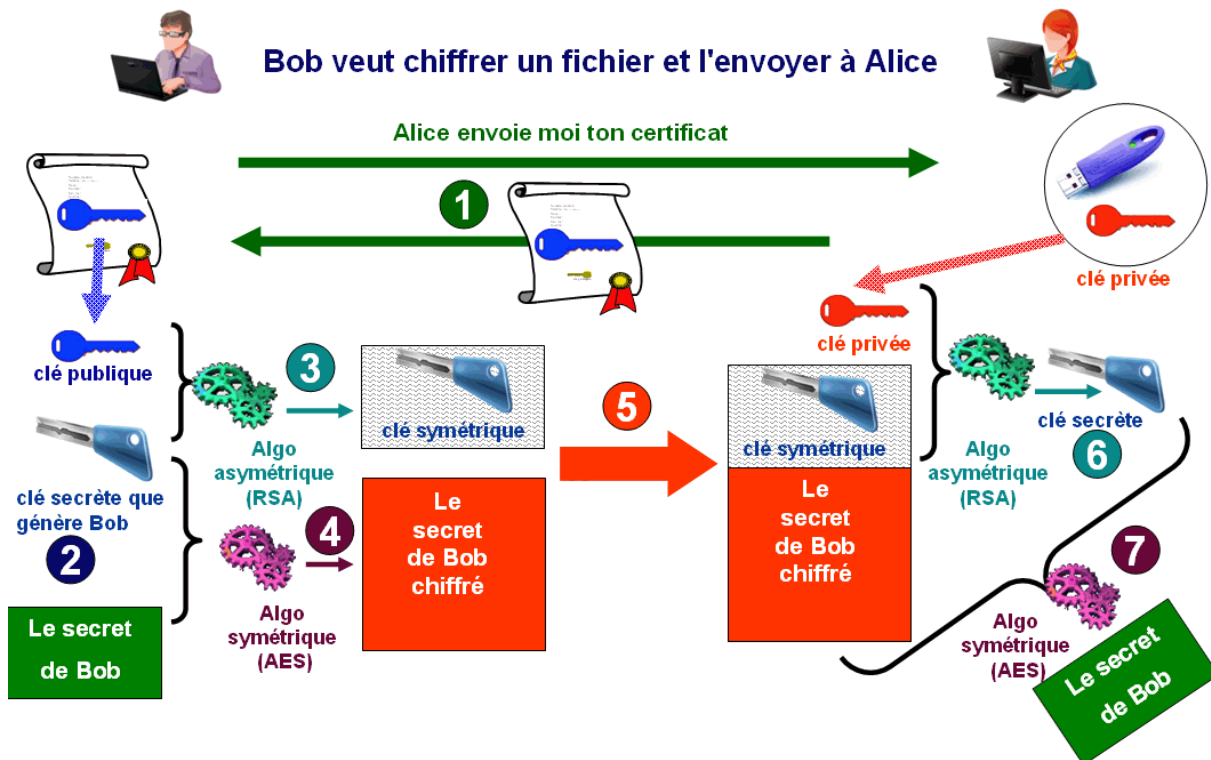
Autre exemple, dans une vidéo de vacances, suivant que vous portiez un chapeau de paille ou un béret basque, ça peut signifier quelque chose à quelqu'un que vous avez mis au parfum de la vraie signification de votre couvre-chef, mais pas pour le commun des mortels.

Une application numérique de la stéganographie est de jouer sur le dernier bit de chaque pixel d'une image, pour cacher un message dans l'ensemble de ces bits. L'œil ne remarque pas les modifications de teintes ou de niveaux de gris de l'image, mais avec le programme approprié, l'image révèle ses messages cachés.

Face à un message chiffré, le cryptanalyste pensera que le message dissimule un secret et a donc de la valeur et il tentera de le décrypter. L'avantage de la stéganographie est que si le message est simplement invisible dans son support visible, personne n'aura l'idée d'aller le chercher sauf son destinataire qui saura que, dans un fichier anodin, se trouve le message secret.

LES MECANISMES DU CHIFFREMENT

Principe ¹ :



Bob chiffre un fichier et l'envoie à Alice. Les exemples sur le chiffrement font toujours intervenir Bob et Alice. Dans la réalité, se sont-ils connus vraiment et échangés des informations chiffrées ? Peut-être est-ce aussi un mythe ☺ ?

Comme l'a dit Albert Einstein « il faut rendre les choses complexes aussi simples que possible mais il ne faut pas les rendre plus simples que possible ». Il est sûr que la crypto est complexe, ça ce n'est pas un mythe.

Allons y ensemble, je vous guide dans l'utilisation des diverses clés et algorithmes divers qui interviennent dans l'échange d'un fichier chiffré.

Bob demande à Alice son certificat. Alice le lui envoie. Bob vérifie le certificat d'Alice, qui est l'autorité qui l'a signé, ses dates de validité, et s'il l'accepte en tire la clé publique d'Alice, pour l'utiliser dans un algorithme asymétrique, comme le RSA.

Bob génère une clé secrète avec laquelle il chiffrera son message confidentiel par un algorithme de chiffrement symétrique, comme l'AES.

Avec la clé publique d'Alice, Bob chiffre sa clé secrète qu'il vient de générer, en utilisant un chiffrement asymétrique, comme le RSA.

Avec sa clé secrète, Bob chiffre son message, en utilisant un chiffrement symétrique, comme l'AES.

Bob envoie à Alice, le message qui a été chiffré par sa clé secrète et un algorithme symétrique comme l'AES, et joint sa clé secrète qui a été chiffrée par la clé publique d'Alice et un algorithme asymétrique comme le RSA.

¹ Crédit Pictogrammes Aastra

Avec sa clé privée contenue dans son token USB, Alice déchiffre la clé secrète, générée par Bob et chiffrée avec la clé publique d'Alice.

Et avec cette clé secrète et un algorithme symétrique, comme l'AES, Alice déchiffre le message envoyé par Bob.

La clé secrète intervenant dans le chiffrement symétrique utilisée pour chiffrer et déchiffrer le message secret a ainsi été envoyée par Bob à Alice en toute sécurité.

MYTHES ET LEGENDES DE LA SIGNATURE ELECTRONIQUE

*Gérard Peliks, CASSIDIAN
an EADS Company*

LA SIGNATURE ELECTRONIQUE, CE QU'ELLE N'EST PAS

Avec la généralisation des accès par l'Internet et la dématérialisation des documents, un jour viendra où la signature électronique va reléguer la signature papier au rang de curiosité du passé.

Aujourd'hui cette technologie, qui authentifie un document et en prouve l'intégrité, est mal connue, et dans le vécu quotidien, on utilise la signature électronique sans trop se poser de questions ou si on s'en pose, on apporte souvent de mauvaises réponses. C'est en particulier le cas sur l'utilité du certificat, objet de bien d'interprétations erronées.

Comme la signature manuscrite, la signature électronique permet à celui qui consulte un document signé d'authentifier le signataire. Mais la signature électronique, c'est encore autre chose.

Non, la signature électronique n'est pas la copie d'une petite partie d'un écran contenant une signature manuscrite, qu'on aurait coupée puis collée au bas d'un document Word. Cette manipulation s'appelle simplement du traitement d'image et n'a aucune valeur car on peut après tout placer ainsi n'importe quelle signature sur n'importe quel document. Il est alors trompeur d'établir une relation entre le document et la signature, même si celle-ci était, en toute honnêteté, déjà dans le document initial scanné.

La signature électronique n'est pas d'avantage ce que vous saisissez en apposant votre paraphe sur une tablette digitale et qui ajoute directement votre signature manuscrite au document que vous signez, comme un contrat de location de voiture, par exemple. Cela s'appelle la signature numérique et fait l'objet de lois spécifiques.

La signature électronique consiste en un petit fichier chiffré, accolé à un document, qui prouve en faisant appel à divers algorithmes et clés de chiffrement que le document a bien pour origine celui qui l'a signé (authenticité) et n'a pas été modifié depuis sa signature (intégrité). Le destinataire, par son logiciel de traitement du document signé, ou manuellement, peut en vérifier l'authenticité et l'intégrité. De plus, le signataire ne pourra pas prétendre ne pas avoir eu connaissance de son document signé (non répudiation).

Nous évoquons dans ce document les mythes et les légendes qui tournent autour de la signature électronique, et nous apportons des réponses. A la fin du document, vous trouverez des explications techniques plus détaillées sur les mécanismes qui interviennent dans l'établissement d'une signature électronique et sur la vérification du document signé.

MYTHE N° 1 :

ON SIGNE PAR SON CERTIFICAT ELECTRONIQUE

Un certificat électronique ne sert en aucun cas à signer un document qu'on émet. Il intervient dans la vérification de la signature d'un document qu'on reçoit ou qu'on consulte.

Votre certificat personnel ne vous est d'aucune utilité pour signer un document ou pour vérifier la signature d'un document que vous recevez. Pour effectuer cette vérification, vous avez besoin, non pas de votre certificat mais du certificat de celui qui a signé le document.

En annexe, vous trouverez des explications techniques qui vous permettront de mieux saisir les mécanismes.

Un certificat prouve que quelqu'un, qui en est le propriétaire, possède aussi une clé de chiffrement privée qui lui est propre et qu'il a utilisée pour signer son document. Grâce à ce certificat le destinataire du document pourra vérifier que ce document a bien été signé par celui dont il a le certificat.

Un certificat contient une clé, dite "clé publique", mathématiquement liée à une deuxième clé, dite "clé privée".

Si vous chiffrez un élément du document avec votre clé privée, cet élément ne pourra être déchiffré qu'avec votre clé publique correspondante, qui se trouve dans votre certificat que vous remettez au destinataire du document. Inutile de prendre des précautions pour transférer votre certificat, celui-ci ne contient aucune donnée confidentielle.

Votre certificat est lui-même signé par une autorité de confiance, qui utilise bien sûr le même mécanisme, pour prouver que la clé publique trouvée dans le certificat est bien la vôtre, c'est-à-dire correspond bien à la clé privée que vous possédez et avec laquelle vous avez signé le document.

Vous signez votre document avec votre clé privée, le destinataire de votre document signé vérifie votre signature avec votre clé publique.

L'élément chiffré puis déchiffré qui a servi à établir qui a signé le document est une "empreinte", ou anglais un "hash" et en bon français un "condensat".

On ne signe donc pas avec un certificat électronique, ni avec la clé publique qu'on trouve dans le certificat, mais avec sa clé privée.

MYTHE N° 2 :

LE CERTIFICAT EST CONFIDENTIEL ET IL FAUT LE PROTEGER

Non, un certificat n'est pas confidentiel, c'est un fichier tout à fait visible et public, destiné à être lu et utilisé par n'importe qui. Le certificat ne contient aucune donnée confidentielle, tout son contenu est en clair, mis à part l'élément chiffré dont nous avons parlé au mythe no 1.

Le certificat est par contre, lui-même, signé électroniquement par une autorité de confiance qui en atteste l'authenticité et l'intégrité. Si vous modifiez ne serait-ce qu'une virgule dans le certificat, cette modification apparaîtra au logiciel de traitement du certificat comme n'étant plus signé par l'autorité de confiance que ce certificat indique.

Le certificat contient une clé de chiffrement publique, qui correspond à la clé privée possédée également par le propriétaire du certificat. Comme le nom des clés l'indique, la clé publique trouvée dans le certificat est publique et donc n'est pas confidentielle.

Seule la clé privée correspondant à la clé publique est confidentielle, et son propriétaire ne doit jamais la dévoiler. La clé privée n'est bien évidemment pas dans le certificat mais, dans le cas idéal, sur un support amovible, tel qu'un token USB protégé par un code PIN.

Le certificat est lui-même signé par une autorité de confiance qui a chiffré un élément du certificat (l'empreinte du certificat qui est l'élément dont nous avons parlé au mythe no 1). Vous possédez le certificat de l'autorité de confiance, contenant sa clé publique (attention, c'est un deuxième certificat, celui de l'autorité de confiance).

L'empreinte chiffrée du certificat peut être alors déchiffrée, par vous, à l'aide de la clé publique de l'autorité de confiance et ainsi vous êtes sûr de l'authenticité et de l'intégrité du certificat qui est attestée par l'autorité de confiance.

Mais si ne possédez pas le certificat de l'autorité de confiance ? Alors vous ne pouvez pas vérifier la validité (authenticité et intégrité) du certificat que cette autorité a signé. Rassurez-vous, vos logiciels connaissent déjà les certificats de nombreuses autorités de confiance, et ceux qui vérifient les signatures électroniques, savent vous demander d'ajouter, aux certificats des autorités que vous connaissez déjà, le certificat de telle autorité de confiance, et vous indiquent en général d'où le télécharger.

MYTHE N° 3 :

UNE SIGNATURE ELECTRONIQUE EN VAUT UNE AUTRE

Bien entendu, nous ne parlons pas ici de l'identité de celui qui signe. Il est sûr qu'un document signé par un notaire ou par une autorité officielle a plus de valeur devant la loi qu'un document signé par un inconnu. Nous parlons ici de la validité d'une signature, qui que soit le signataire. En d'autres termes nous parlons de l'adéquation entre le signataire et sa signature.

Il existe différents niveaux de confiance pour les signatures parce qu'il existe différents niveaux de confiance pour les certificats. Tout dépend qui en établit la validité et comment les certificats ont été obtenus.

Il y a également différents niveaux de confiance à accorder aux certificats suivant les algorithmes de chiffrement et de calcul d'empreinte utilisés et la longueur des clés de chiffrement. L'algorithme de calcul d'empreinte recommandé aujourd'hui est le SHA2 et la longueur des clés pour le chiffrement asymétrique RSA est de 2048 bits.

La première chose qu'on regarde dans un certificat est l'autorité de confiance qui l'a signé. Si le destinataire a confiance en cette autorité, le certificat peut être utilisé pour en tirer la clé publique qu'il contient afin de vérifier qui a signé le document. Si le destinataire ne fait pas confiance en l'autorité qui a signé le certificat, il ne fera pas confiance en la signature du document.

Les autorités de confiance n'ont de sens que par la confiance qu'elles inspirent à leurs clients qui achètent leurs certificats (et avec chaque certificat la clé privée qui correspond à la clé publique que le certificat contient).

Cette confiance peut être accordée par exemple aux certificats signés par une autorité de confiance de même nationalité que le destinataire du document signé, ou alors à une autorité de confiance reconnue par beaucoup d'état comme Verisign qui est une autorité américaine.

Et surtout, il est important de connaître comment un certificat a été décerné à son propriétaire. Le certificat et la clé privée ont pu être achetés par courriel, à travers l'Internet, juste en fournissant une adresse et en le payant. A l'autre bout de l'échelle, le certificat, et sa clé privée associée ont pu être décernés par une autorité de confiance qui convoque l'utilisateur et s'assure de son authenticité, avant de lui remettre sa clé privée et le certificat qui contient sa clé publique.

On distingue plusieurs classes de certificats. Un certificat s'il est obtenu sans formalités, pourvu qu'on le paye, est un certificat qui n'est pas de la même classe qu'un certificat obtenu après déplacement et authentification forte de l'utilisateur. En France, seuls les documents signés et vérifiés avec des certificats à partir d'une certaine classe ont même valeur juridique que les documents qui présentent une signature manuscrite.

MYTHE N° 4 :

SIGNER, C'EST CHIFFRER ET CHIFFRER C'EST SIGNER

Non, signer n'est pas chiffrer. Il y a des documents signés et des documents chiffrés. Il y a aussi des documents à la fois signés et chiffrés. En fait la signature et le chiffrement sont deux fonctions différentes avec des buts différents. Le chiffrement assure la confidentialité alors que la signature assure l'authenticité et l'intégrité du document sur laquelle elle porte. Un document peut être signé mais être en clair.

La signature du document, d'un point de vue technique fait appel à un calcul d'empreinte, puis cette empreinte est chiffrée par chiffrement asymétrique. De même la vérification de la signature du document fait appel aussi au chiffrement asymétrique pour déchiffrer l'empreinte avec la clé publique correspondant à la clé privée.

Mais seule l'empreinte du document est chiffrée ou déchiffrée, le document lui peut ne pas être chiffré. La signature électronique n'assure pas la confidentialité du document.

A l'opposé, rien ne prouve qu'un document chiffré l'ait été par son propriétaire et qu'il n'ait pas été modifié par une tierce personne.

MYTHE N° 5 :

UNE SIGNATURE ELECTRONIQUE, C'EST POUR LA VIE

La signature n'est vérifiable que durant la période de validité du certificat.

Outre la clé publique, le certificat contient la date à partir de laquelle il commence à être valable et la date à partir de laquelle il ne sera plus valable. Comme le certificat est lui-même signé par une autorité de confiance, si on falsifie ces dates, cela se remarque. Les logiciels de vérification des signatures tiennent compte de ces dates.

Il existe également des listes de révocation de certificats. Si le certificat du signataire a été révoqué, le logiciel de traitement de signature électronique refusera de considérer la signature du document comme valable, même si le certificat est encore dans ses dates de validité.

Une signature électronique n'est donc vérifiable, par logiciel, que durant la période de validité du certificat qui possède la clé publique avec laquelle on le vérifie.

Mais si le document a été signé alors que le certificat pour vérifier la signature était encore valable ? Bien entendu, même quand le certificat a expiré ou a été révoqué, la signature peut être tout de même recevable par un être humain qui prend de la hauteur par rapport à un logiciel de traitement de signatures électroniques, qui agit mais n'interprète pas.

C'est le même cas qui se pose si un contrat a été signé par un employé qui était dans une entreprise au moment de la signature, et l'a quittée depuis.

LES MECANISMES DE LA SIGNATURE ELECTRONIQUE

Pour comprendre le mécanisme de la signature électronique, il faut connaître deux mécanismes qui sont le calcul d'empreinte et le chiffrement asymétrique.

Le calcul d'empreinte consiste à calculer, à partir d'une chaîne de caractères de longueur quelconque, un ensemble de bits (l'empreinte) dont le nombre fixe est déterminé par l'algorithme de calcul d'empreinte. C'est par exemple 128 bits pour le MD5 et 160 bits pour le SHA1. Si la chaîne de caractère de longueur variable subit la moindre modification, son empreinte produite sera différente. Un document est donc caractérisé par son empreinte.

Le chiffrement asymétrique fait intervenir deux clés. L'une pour chiffrer, l'autre pour déchiffrer. L'une des clés est privée et doit être gardée secrète par son propriétaire, l'autre est publique et son propriétaire peut la donner à tout le monde. Cette clé publique est placée

dans un certificat électronique qui atteste qu'elle correspond bien à la clé privée détenue par le propriétaire des deux clés.

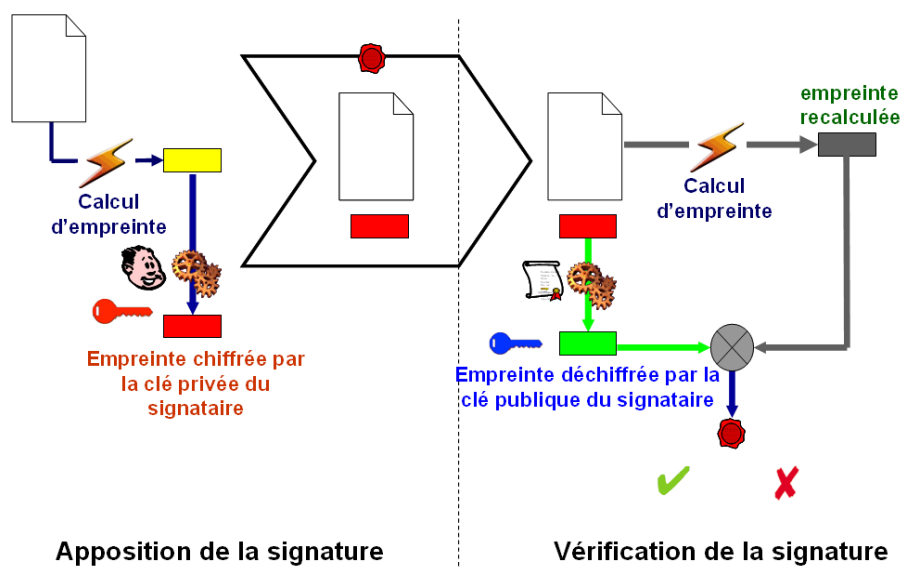
La clé publique est contenue dans un certificat qui est signé par une autorité de confiance. Bien entendu, connaissant la clé publique, il n'est pas possible d'en déduire la clé privée. Quand on chiffre avec l'une des clés, on ne peut déchiffrer qu'avec l'autre. Dans la signature électronique, c'est la clé privée qui est utilisée pour chiffrer et la clé publique pour déchiffrer. Dans le chiffrement asymétrique d'un document, c'est l'inverse.

Le signataire calcule l'empreinte du document à signer et la chiffre avec sa clé privée. Il joint l'empreinte chiffrée au document qui est alors signé.

Ceux qui vérifient la signature du document ont besoin de la clé publique de celui qui l'a signé, donc du certificat qui la contient. Ils déchiffront grâce à la clé publique l'empreinte chiffrée. Ils recalculent, à partir du document reçu, l'empreinte de ce document. Si l'empreinte déchiffrée est la même que l'empreinte recalculée, la signature est prouvée.

Le document est authentique car son empreinte n'a pu être chiffrée que par celui qui détient la clé privée. Le document signé est intègre puisque le calcul de l'empreinte du document signé est identique au calcul d'empreinte du document avant sa signature.

Principe :



Terminons cette exploration en soulignant un arrêt de la Cour de Cassation qui par un arrêt du 30 septembre 2010 rappelle les formes impératives que doit revêtir un échange électronique pour acquérir une force probatoire et une valeur juridique donnant ainsi son importance à cette technologie : " Sans signature électronique garantissant identité du signataire et intégrité du message, le courriel n'a pas plus de valeur juridique qu'une lettre anonyme faite de collages de caractères découpés dans les journaux".

MYTHES ET LEGENDES DE L'IDENTITE NUMERIQUE

Philippe Vacheyrou, CAPUCINE

La notion d'identité numérique apparaît dans la loi Informatique fichiers et liberté de 1978 et le concept s'est imposé progressivement au fil des pratiques d'identification et d'authentification, notamment dans le cadre des procédures administratives et de la mise au point de processus de signature numérique.

Par ailleurs, l'utilisation du Web dans une perspective participative, le développement des réseaux sociaux ont permis l'émergence d'autres problématiques qui y sont liées.

On en arrive donc à l'utilisation du même terme dans deux contextes différents :

- L'identité numérique perçue en termes d'image de l'individu au sens social du terme, c'est-à-dire l'e-réputation.
- L'identité numérique en tant que support de procédures légales, recouvrant la notion d'identification et de possibilité d'authentification de documents à valeur probante, reliés à l'identité au sens légal du terme (authenticité). C'est dans ce sens là que nous l'envisagerons sous le terme de Cyber Identité en liaison avec les labels SuisseID, IDéNum et les cartes Nationales d'Identités Electroniques.

Techniquement, l'identité numérique se définit comme un « lien technologique entre une entité réelle et une entité virtuelle ». (voir Wikipedia)

MYTHE N° 1 :

L'IDENTITE NUMERIQUE EST UNIQUE :

Ceci est à la fois vrai et faux.

L'entité réelle en cause étant l'individu, elle est unique malgré la diversité des moyens employés pour l'authentifier. Par contre, l'entité virtuelle, en tant que profil utilisateur (Avatar) : national, familial, professionnel, médical, juridique, consommateur, etc. - est multiple avec les données qui s'y attachent et qui ne sont pas nécessairement toutes les mêmes. Dans les deux cas l'individu doit pouvoir bénéficier de l'application de la loi Informatique et liberté et des recommandations diverses qui l'accompagnent :

- Anonymat
- Droit à l'oubli
- Protection des données personnelles
- Propriété intellectuelle
- Traçabilité des données
- Maîtrise de son Identité Numérique au niveau international

En ce qui concerne les dispositifs, divers processus, méthodes, sont possibles. Plusieurs niveaux de certification existent, les autorités de certifications peuvent être privées ou publiques. Il en résulte une multitude de moyens et même de façons d'en aborder le concept.

En ce sens il est possible de parler de multiplicité des identités virtuelles, du simple pseudonyme à usage ciblé à l'identité certifiée à travers un acte authentique

Il en est de même des procédés, du couple login/ mot de passe au système basé sur des données biométriques dont le plus extrême serait l'ADN, en passant par les systèmes de

certificats. Il convient de protéger cet identifiant par les dispositifs disponibles sur le marché (PKI, IGCP 2.0, OTP, SSO, Token etc.)

MYTHE N° 2 :

L'IDENTITE NUMERIQUE RELEVE DE L'AUTORITE REGALIENNE.

Les gouvernements délèguent à des tiers certificateurs le soin d'établir l'identité nationale par le biais d'une identité numérique (Carte bancaire, clé USB, mot de passe dynamique etc...)

De plus toute identité numérique n'est pas utilisée dans un cadre nécessitant une identification certaine (Cartes prépayées)

Il est possible de mettre en place des «cyber- identités » destinées à retracer une activité tout en permettant un certain anonymat – sous réserve des possibilités d'identification dans un cadre réglementé, par exemple à travers la possibilité d'indiquer simplement l'hébergeur dans le cas de blogs individuels. Cette Cyber Identité permet à l'utilisateur de conserver l'anonymat, assurer la protection de ses données personnelles et de préserver la propriété intellectuelle, mais elle n'est pas dépendante de l'autorité régalienne.

MYTHE N° 3 :

IDENTIFICATION ET AUTHENTIFICATION C'EST PAREIL.

L'identification repose sur les informations associées à un objet ou un humain dans un contexte donné pour le distinguer. Il s'agit de disposer des informations nécessaires pour déterminer que l'individu est bien, selon les données que l'on possède, celui qu'il prétend être. Elle s'applique à l'individu.

L'authentification consiste à s'assurer de l'authenticité, l'intégrité et la non-répudiation des informations fournies. Il peut s'agir des informations fournies pour l'identification ou de tout autre processus ou document. Elle s'applique à l'objet et non à l'individu.

MYTHE N° 4 :

LA SECURITE EST GARANTIE PAR LES REFERENTIELS DE SECURISATION ET D'INTEROPERABILITE (RGS¹ - RGI²)

Selon le Référentiel Général de Sécurité :

« L'objectif du RGS n'est pas d'imposer une technologie, une architecture ou une solution technique, ni même les fonctions de sécurité décrites dans le RGS »

Le socle de sécurisation IAS (Identification, Authentification, Signature) sur lequel s'appuient les rapports de certification³ pour les Carte d'Identité Electronique ne peut pas fonctionner, dans la mesure où les identifiants biométriques sont des données statiques numérisables et reproductibles. Il est donc possible, partant d'une fausse identité authentifiée, d'aboutir à une signature techniquement valide mais fausse.

¹ Le référentiel RGS peut être trouvé sur le site : <http://www.ssi.gouv.fr/IMG/pdf/RGSv1-0.pdf>

² Voir le référentiel sur le site :

https://www.ateliers.modernisation.gouv.fr/ministeres/domaines_d_expertise/architecture_fonction/public/rgi/referentiel_general1617/downloadFile/file/Referentiel%20General%20Interoperabilite%20Volet%20Technique%20V0.90.pdf

³ Voir sur le site du gouvernement : http://www.ssi.gouv.fr/IMG/certificat/anssi-cc_2009-56fr.pdf

En inversant les deux facteurs, le socle AIS permet à l'utilisateur de délivrer son identité dans un environnement authentifié avec une adresse ID (label IDéNum¹ pour la France) constituant un intranet ou réseau de confiance numérique qui rejoint le post-IP et la proposition de John DAY en y associant l'ID (SuisseID, IDéNum, CapucineID etc.). Ce dernier est compatible avec le RGS puisqu'il est précisé :

« En revanche lorsqu'une autorité de certification juge nécessaire, à l'issue d'une analyse de risque, de mettre en œuvre les fonctions de sécurité qui sont prévues dans le RGS, elle doit alors respecter les règles correspondantes ».

MYTHE N° 5 :

LA GOUVERNANCE DE L'INTERNET RELEVE D'UNE ORGANISATION CENTRALISEE

La Gouvernance de l'Internet ne se limite pas à une question d'adressage et la gestion des noms de domaine. L'objet de l'ICANN précise « Les autres questions concernant les internautes, telles que les règles relatives aux transactions financières, les contrôles de contenus sur l'Internet, les messages électroniques à caractère commercial non sollicité (*spam*) et la protection des données n'entrent pas dans le cadre des responsabilités de coordination technique de l'ICANN »

Les autres questions relèvent donc des Internautes, en complément du réseau constitué par la gestion des DNS avec des adresses IP il convient de créer un réseau de fédération d'Identité à l'instar de Shibboleth (qui est un mécanisme de propagation d'identités, développé par le consortium Internet², qui regroupe 207 universités et centres de recherches). Cette notion associée avec des adresses ID, à l'instar d'un réseau OpenID+ sécurisé, associés aux réseaux des Internets, pourrait constituer une gouvernance de l'Internet qui relèverait alors de plusieurs organisations centralisées sur la base de « critères communs » évoqués précédemment, définis dans le Web sémantique.

Il revient donc à chaque usager de s'assurer du bon usage des TIC en réseau sécurisé pour participer à la gouvernance mondiale dans le cadre du Forum pour la Gouvernance de l'Internet³ et construire la Société de l'Information du XXIème siècle, en tirant parti des Technologies du Relationnel notamment avec les environnements 3D, pour partir de la réalité augmentée, vers un futur augmenté.

EN CONCLUSION : INTERNET EST LA PIRE ET LA MEILLEURE DES CHOSES

Cette formule fourre-tout n'est pas un argument mais est largement utilisée par les détracteurs d'Internet. Une formule ne fait pas la réalité et, si nous avons pu observer ce que pouvaient être les pires facettes d'Internet, à l'instar du « Le meilleur des mondes⁴ » de Aldous Huxley. Reste à expérimenter ce que pourrait être un monde meilleur entre le « Big Brother » de George Orwell⁵ et la « Big Society » de David Cameron, le premier ministre britannique, pour mieux responsabiliser les citoyens dans les collectivités locales afin de construire un réseau vertueux d'économie sociale et solidaire avec une démarche d'entrepreneuriat social, pour un développement soutenable.

¹ Voir annonce IDéNum : <http://www.gouvernement.fr/gouvernement/label-idenum-plus-de-securite-et-plus-de-facilite-pour-l-usage-des-services-sur-interne>

² Voir la définition de ce concept sur Wikipédia sur <http://fr.wikipedia.org/wiki/Internet2>

³ Site du Forum : <http://www.intgovforum.org/cms>

⁴ Voir la page de Wikipédia http://fr.wikipedia.org/wiki/Le_Meilleur_des_mondes

⁵ Pour en savoir plus, voir la page de Wikipédia : http://fr.wikipedia.org/wiki/George_Orwell

MYTHES ET LEGENDES DES SYSTEMES DE CLOUD

Professeur Jean-Pierre Cabanel, INP / ENSEEIHT, membre de l'IRIT

Professeur Daniel Hagimont, INP / ENSEEIHT, membre de l'IRIT

Face à l'augmentation continue des coûts de mise en place et de maintenance des systèmes informatiques, les entreprises externalisent de plus en plus leurs services informatiques et confient leur gestion à des entreprises spécialisées (que nous appelons fournisseurs). L'intérêt principal réside dans le fait que le client de ces fournisseurs ne paie que pour les services effectivement consommés, alors qu'une gestion de ces services par le client ne serait pas complètement amortie, en particulier lorsque les besoins du client varient. Le « Cloud Computing » se situe dans cette orientation récente.

Devant le manque de consensus sur la définition de la notion de « Cloud Computing », reprenons celle de CISCO : "Cloud Computing is an IT resources and services that are abstracted from the underlying infrastructure and provided on-demand and at scale in a multitenant environment".

Il s'agit donc de fournir aux clients (des entreprises) des services à la demande, illusion de l'infinité des ressources et enfin d'utiliser les mêmes ressources (mutualisation) pour tous les clients.

Cette stratégie offre plusieurs avantages parmi lesquels :

- Réduction des coûts pour le client. Il n'a plus besoin de gérer sa propre infrastructure et il est facturé en fonction de l'utilisation des services du Cloud.
- Flexibilité pour le client. Il peut augmenter la capacité de son infrastructure sans investissements majeurs, les ressources du Cloud étant allouées dynamiquement à la demande.
- Moins de gaspillage. Les infrastructures gérées chez les clients sont souvent sous-utilisées, alors que l'infrastructure d'un Cloud mutualise un ensemble de ressources pour un grand nombre de clients, ce qui permet d'augmenter le taux moyen d'utilisation des ressources.

Un exemple privilégié de mesure de ce gaspillage est la consommation électrique des infrastructures.

MYTHE N° 1 :

LE CLOUD EST JUSTE CE QU'ON APPELAIT AVANT LE "TIME SHARING" : LES APPLICATIONS NE SONT PLUS HEBERGEES CHEZ SOI ET ON NE PAYE QUE CE QUE L'ON CONSOMME

Le Cloud, c'est un peu plus compliqué. Les utilisateurs potentiels d'un Cloud se regroupent en 3 catégories : administrateur du Cloud, administrateur du client et utilisateur final.

L'administrateur du Cloud est responsable de l'administration des ressources matérielles et logicielles du Cloud. Il est notamment responsable de la gestion de la capacité d'hébergement du Cloud. Le Cloud doit donc fournir à son administrateur des services d'administration lui permettant de gérer les ressources matérielles et logicielles mises à disposition des clients.

Quant à l'administrateur du client, il utilise les ressources fournies par le « Cloud » pour gérer les applications finales du client. Il n'a pas une vue globale de l'environnement du Cloud,

mais seulement des ressources mises à la disposition du client et des applications gérées avec ces ressources.

En fonction du niveau de service fourni par le Cloud, on identifie 3 scénarios d'utilisation du Cloud :

- **Infrastructure as a Service (IaaS)** : Il s'agit du niveau le plus bas. Le Cloud fournit des ressources matérielles à ses clients (capacité de traitement, de stockage ...). Ces ressources matérielles peuvent être fournies directement au client (l'unité d'allocation est alors généralement une machine équipée d'un système d'exploitation) ou être virtualisées (l'unité d'allocation est alors généralement une machine virtuelle, plusieurs machines virtuelles pouvant s'exécuter sur une même machine physique) pour une gestion plus fine des ressources physiques. Pour ce niveau, le Cloud fournit un ensemble d'API permettant à l'administrateur du client d'utiliser un ensemble de ressources. L'administrateur du client a alors la responsabilité d'utiliser ces ressources (machines physiques ou virtuelles) pour y installer et gérer les applications utilisées par le client.
- **Platform as a Service (PaaS)** : Il s'agit d'un niveau intermédiaire dans lequel le Cloud ne fournit pas que des machines et leurs systèmes d'exploitation, mais également des logiciels appelés plateformes applicatives. Ces plateformes sont des environnements d'exécution pour les applications finales comme par exemple : les serveurs d'applications dans une architecture JEE. Ces plateformes applicatives sont maintenues par l'administrateur du Cloud, mais l'administrateur du client a la charge d'administrer les applications finales du client sur ces plateformes applicatives.
- **Software as a Service (SaaS)** : Il s'agit du niveau le plus haut dans lequel le Cloud fournit directement les applications finales à ses clients. L'administrateur du Cloud administre les applications finales et le rôle de l'administrateur du client est quasiment nul. Il est important de souligner qu'un Cloud de niveau SaaS peut être implanté par un acteur en s'appuyant sur un Cloud de niveau PaaS géré par un autre acteur, lui même implanté sur un Cloud IaaS.

MYTHE N° 2 :

LE CLOUD COMPUTING EST UNE REVOLUTION TECHNOLOGIQUE

On peut penser que le « Cloud Computing » est une révolution technologique, mais non, c'est une orientation vers un mode de gestion des infrastructures informatiques des entreprises.

En adoptant cette orientation, on retrouve tout les problèmes classiquement adressés dans les infrastructures actuelles, et notamment :

- **La tolérance aux pannes.** Un service géré dans un Cloud doit tolérer les pannes dans le sens où il faut assurer la cohérence de l'état du service en cas de panne ainsi que sa disponibilité pour les usagers. La disponibilité peut être plus difficile à assurer du fait que les services sont déportés dans le Cloud et qu'une indisponibilité de la connexion entre le client et le Cloud peut lourdement affecter la disponibilité du service.
- **La sécurité.** Un service géré dans un Cloud doit résister à des utilisations malveillantes. La sécurité peut être délicate à assurer du fait que le Cloud peut héberger des applications pour le compte de différents utilisateurs (ce qui n'est pas le cas pour une infrastructure interne à l'entreprise cliente). De plus, l'utilisation d'un service nécessite une communication entre le client et le Cloud, ce qui peut constituer un talon d'Achille pour la sécurité.

- **L'interopérabilité et la portabilité.** Les clients des « Clouds » auront vite envie de pouvoir migrer des services d'un Cloud à un autre, ce qui nécessitera l'établissement de standards permettant de tels échanges.

Un problème apparaît toutefois plus crucial dans le domaine du Cloud Computing. Comme on l'a vu précédemment, l'organisation d'un Cloud implique deux administrateurs : l'administrateur du Cloud et l'administrateur du client. L'administrateur du Cloud doit déployer des logiciels (systèmes d'exploitation, machines virtuelles, plateformes applicatives ou logiciels pour l'utilisateur final) sur des machines physiques et les gérer à l'exécution (migration, répartition de la charge) afin d'assurer la qualité de service à ses clients.

L'administrateur du client doit effectuer les mêmes tâches d'administration dans le cas des scénarios PaaS et IaaS. Ces tâches d'administration ne peuvent être effectuées manuellement et une tendance générale est de fournir des environnements d'administration autonomes visant à automatiser au maximum ces tâches (on parle également plus généralement « d'autonomic computing ». Ces environnements d'administration autonome fournissent des formalismes permettant de décrire les actions à effectuer pour déployer des applications et les reconfigurer dynamiquement pour prendre en compte les conditions à l'exécution.

Il existe principalement trois types de système de Cloud et les problèmes de sécurité sont différents suivant la structure utilisée.

1. **Les systèmes privés** propres à un grand compte, avec si nécessaire quelques sous-traitants
2. **Les systèmes partagés** par plusieurs grands comptes
3. **Les systèmes publics**, ouverts à tout le monde

Un système de type Cloud se décompose en plusieurs parties :

- Des postes clients indépendants
- Un système de communication entre le poste client et le système.
- Des bâtiments qui abritent les ordinateurs Cloud
- Des ordinateurs, systèmes d'exploitation et logiciels du Cloud

Chacun de ces éléments est un des maillons de la chaîne sécuritaire du système et impacte sur les paramètres suivants :

- Confidentialité
- Authentification
- Dénier de service
- Pollution, destruction

La problématique de la sécurité d'un système de Cloud relève d'une tâche ardue, et les protections envisagées vont diminuer la potentialité de généralisation d'utilisation de Cloud multiples pour un même client.

De manière induite, la problématique juridique est, elle aussi, très difficile : Qui va être responsable des aléas direct ou indirect qui surviendront ? Comment obtenir la réalité sur les causes des situations ?

Il y a quelques années, les constructeurs de « main frame », DEC, BULL, IBM etc., exploitaient des systèmes identiques au Cloud avec sur le plan sécuritaire plusieurs différences essentielles :

- Très souvent, les clients du point central, appartenait à une même entité juridique : une banque, une industrie etc.

- Les systèmes de communications utilisés n'étaient pas l'Internet, ils permettaient un contrôle suffisant : lignes et réseaux spécifiques et propriétaires.
- La protection des ressources et la recherche des causes d'aléas étaient simplifiées, une seule entité juridique cliente et des systèmes de communication propriétaires des fournisseurs de « Main Frame » ou centre de ressources informatiques.

La nouvelle approche, modifie l'environnement précédemment présenté : clients avec des entités juridiques multiples, même si ces clients sont connus et identifiables à priori, et utilisation de moyens de communication ouverts et incontrôlables : l'Internet.

MYTHE N° 3 :

LE CLOUD PRIVE D'UN GRAND COMPTE EST COMPLETEMENT SECURISE

Dans les systèmes privés propriétaires d'un grand compte, ce type d'utilisation (très proche des PKI intra entreprise), le système est installé sur le site de l'entreprise et les risques sécuritaires sont minimisés. Ils relèvent de la protection des communications dans l'entreprise (internationales) et du contrôle des personnes et des systèmes dédiés au Cloud. Le responsable vis-à-vis des utilisateurs est alors le service informatique qui gère les services de Cloud. Sommes-nous face à un système qui possède un haut niveau de sécurité ?

Et bien cela n'est pas si clair, il est encore nécessaire de contrôler, les chemins utilisés par l'information afin que des copies illicites ne soient réalisées, de s'assurer de la pérennité du fournisseur du service, afin de ne pas perdre de l'information et ainsi désorganiser l'entreprise, contrôler les communications, etc.

Avec les systèmes réservés à plusieurs grands comptes, nous sommes en présence de la structure la plus exposée aux problèmes sécuritaires. En effet le site physique du Cloud n'est pas sous contrôle de l'entreprise mais contient des informations confidentielles de plusieurs entreprises.

MYTHE N° 4 :

LES INFORMATIONS STOCKEES SUR UN CLOUD PARTAGE SONT PROTEGEES, PAR CONTRAT, DES VIRUS, VERS ET AUTRES ATTAQUES

Les postes clients du système Cloud, utilisent sûrement des supports magnétiques amovibles, (il existe très peu d'application fermée) ou bien le poste client est utilisé pour d'autres travaux, ou dans le cas pire, le poste client est connecté à l'Internet de temps en temps.

Pensez-vous alors que les filtres anti virus du Cloud vont protéger les informations des entreprises clientes ? Et bien non ! En réalité ces filtres possèdent une efficacité toute relative et cela conduit au risque de pollution du Cloud par les virus et autres programmes malveillants positionnés par un client et ainsi polluer ou détruire des informations des entreprises clientes du Cloud

Vous imaginez peut-être, que les données des entreprises peuvent être séparées physiquement sur des machines différentes avec des accès réseaux différents ? Et bien non ! La réalité économique de ces systèmes oblige à mettre en commun les ressources afin de diminuer les coûts pour les clients.

Un fournisseur de systèmes de Cloud peut-il garantir par contrat la non destruction ou pollution des données stockées ? Les notions de virus et vers sont elles assimilées aux forces majeures : nature, guerre etc. ? La pérennité du fournisseur est-elle prise en compte par des clauses spécifiques ? Il semble que si l'on désire garder des coûts acceptables de service de Cloud, il soit très difficile de garantir de telles contraintes.

Pensez vous qu'il est possible, de détecter le client responsable d'une pollution ? Quelles sont les responsabilités partagées du Cloud et du client pollueur ?

Dans un environnement semi ouvert (les clients sont connus), la technique actuelle ne permet pas de protéger de la pollution un site de Cloud, de plus, cette dernière, peut être engendrée par un poste client, qui ne connaît pas obligatoirement son propre état de pollution. Il est donc très difficile de remonter au client initial, et les autres clients du Cloud sont alors en droit de se retourner vers le propriétaire du Cloud dans le cas de pollution de leurs données.

De plus des postes clients peuvent eux-mêmes être pollués, par un Cloud pollué par un autre client. Cela montre l'interaction informatique entre des entreprises qui ne se connaissent peut être pas,

Peut être pensez vous que si vous participez à un Cloud, le fournisseur vous garantit un cloisonnement informatique étanche ? Et bien non ! Votre entreprise (vos postes connectés au Cloud) devient une partie de la toile tissée par le Cloud et votre informatique est alors assujettie aux aléas d'autres entreprises.

C'est un des problèmes très important lié au système de type Cloud.

MYTHE N° 5 :

SI VOUS QUITTEZ VOTRE FOURNISSEUR, VOTRE CONTRAT GARANTIT LA CONFIDENTIALITE ET LA RESTITUTION DE VOS INFORMATIONS ET LEUR DESTRUCTION

En dehors des problèmes de confidentialité et d'authentification relatifs aux communications électroniques entre plusieurs sites, les informations (confidentielles ou non) des clients sont stockées chez un tiers. Il se pose alors le problème de la confiance dans le tiers par rapport aux problèmes suivants :

- Accès à des informations de clients par des employés du tiers (espionnage).
- Pénétration du site par autrui qui est ou non un client. (usurpation d'identité)

Même si les informations sont chiffrées sur les machines du Cloud, le chiffrement est propriétaire (algorithme et clef) du Cloud et pas de chaque client. Un chiffrement propre à chaque client avec des clefs différentes pour chaque envoi, minimise les risques d'indiscrétion, mais complique la gestion du Cloud et ouvre la porte à d'autres problèmes.

Comment pensez-vous accorder votre confiance à un fournisseur de service de Cloud ? Quel niveau d'informations confidentielles êtes-vous prêt à confier à autrui ? Pensez vous que par contrat le fournisseur de Cloud va vous garantir la non divulgation en interne, ou par accès extérieur, des informations stockées ?

Ces questions montrent la difficulté d'accorder sa confiance à un fournisseur de service de Cloud, que vous ne contrôlez pas.

Vous pouvez aussi penser à changer de fournisseur de Cloud ou vous pouvez vous retrouver face à la disparition de votre fournisseur.

Alors se pose la question de la récupération de vos données et de l'effacement des informations des supports magnétiques utilisés. Pensez-vous que par contrat, votre fournisseur va vous garantir l'effacement de vos informations, c'est-à-dire la destruction des supports magnétiques ? Il semble peu vraisemblable que vous obteniez cette clause dans votre contrat.

Les systèmes ouverts au public ne peuvent correspondre au monde industriel, y compris aux PME/PMI. Les dangers sont très importants, ils correspondent à ceux relatifs au réseau internet. Aucun contrat ne pourra garantir la sécurité des informations, donc ils ne peuvent être utilisés que pour des informations ou traitement non confidentiels.

Comme les puissances de calcul, les volumes de stockage, les prix des logiciels continuent de s'améliorer, on peut se demander si le grand public nécessite ce type d'offre.

MYTHE N° 6 :

AVEC UN SERVICE DE CLOUD, JE N'AI PLUS BESOIN DE ME PREOCCUPER DE MA SECURITE ET DE LA DISPONIBILITE DES SERVICES, ET MON CONTRAT COUVrira LES RISQUES INFORMATIQUES ENGENDRES

Comme tout problème de sécurité, la problématique de l'utilisation de systèmes de type Cloud peut être formalisée par les deux idées antinomiques suivantes :

D'un coté les diminutions de coût engendrées par la mise en commun et la meilleure utilisation des ressources informatiques et, d'un autre coté une augmentation importante des risques d'espionnage, pollution etc. dans le monde informatique.

Avec un service de Cloud Computing, les problèmes de sécurité sont très fortement amplifiés : destruction, pollution, confidentialité etc., et la disponibilité des ressources est assujettie au fonctionnement du réseau. Il est plus facile de sécuriser des informations dans son entreprise que sur un système non propriétaire partagé et utilisable à travers un réseau.

Il est clair, que pour des entreprises stratégiques de taille importante, la notion de Cloud ne peut exister que dans le périmètre de l'entreprise, le Cloud est physiquement installé sur un des sites et les clients appartiennent à un même environnement. C'est une vieille utilisation, même si l'exploitation des calculateurs est confiée à un tiers qui peut être le fournisseur de système Cloud.

Pour des entreprises (PME-PMI) stratégiques, un vrai problème se pose, et l'analyse entre la perte financière engendrée par la copie (espionnage ou destruction) de document, et le gain obtenu par la diminution des coûts journaliers de l'informatique, est très difficile à évaluer et dépend de nombreux facteurs.

L'utilisation des systèmes de Cloud ouverts et gérés par des tiers devient alors limitée à des applications dont le niveau de confidentialité est faible, dans le monde industriel, la dernière molécule, le dernier programme etc. ne se partage pas, et les informations relatives à la comptabilité client sont protégées.

L'utilisation de système de type Cloud pose le problème de la confiance vis-à-vis du fournisseur du Cloud, mais aussi vis-à-vis de ses clients, il manque un gendarme.

Pensez-vous vraiment confier vos informations confidentielles à un tiers, et pensez vous que votre contrat couvrira les risques informatiques engendrés ? L'informatique évolue, les types d'attaques aussi, et un contrat signé à une date, ne peut envisager les évolutions dans les années suivantes.

QUELQUES PLATEFORMES EXISTANTES

Plusieurs plateformes ont émergé dans le domaine du Cloud Computing. Parmi les plus connues, nous pouvons citer :

- **Amazon Elastic Compute Cloud (EC2)** : il s'agit d'une plateforme de type IaaS basée sur les machines virtuelles Linux. EC2 fournit une plateforme de création de machines virtuelles personnalisées (AMI pour Amazon Machine Image) et d'exécution de ces machines virtuelles.
- **Google App Engine** : il s'agit d'une plateforme de type PaaS de développement et d'exécution d'applications web. Une quantité de ressources minimum est allouée par la plateforme et peut évoluer en fonction des demandes de l'application.

- **Microsoft Live Mesh** : il s'agit d'une plateforme de type SaaS de stockage d'applications et de données. Elle assure la disponibilité et la synchronisation des données entre tous les équipements du client.

Ces quelques exemples montrent l'implication des grands acteurs. Si le Cloud Computing est plus une orientation stratégique et architecturale qu'une révolution technologique, il est clair que cette orientation risque de bouleverser les infrastructures informatiques de nos entreprises.

MYTHES ET LEGENDES DE LA CERTIFICATION CRITERES COMMUNS

*Gérard Peliks, CASSIDIAN
an EADS Company*

LA CONFIANCE OBJECTIVE EN UNE SOLUTION DE SECURITE

L'Information que vous détenez est sans doute protégée par des solutions de sécurité. Mais ces solutions sur lesquelles réside votre confiance, sont-elles sécurisées ?

Un logiciel de sécurité n'en reste pas moins un logiciel et comme toute œuvre de l'esprit humain, il peut être entaché d'erreurs de programmation, ou d'implémentation, qui sont autant de vulnérabilités ouvertes aux attaques que le logiciel est censé contrer. Il en est de même pour les cartes à puce et pour les logiciels embarqués.

Qu'est ce qui pourrait alors motiver la confiance que vous accordez à un logiciel de sécurité ? Serait-ce parce que votre voisin n'a pas eu de problèmes avec la même solution ? Est-ce la notoriété que le produit rencontre sur le marché ? Seraient-ce les sirènes d'un constructeur qui vous affirme que son produit est le meilleur ? Non, tout ceci n'est que confiance suggérée...

Une confiance objective peut-elle s'établir ? Oui, un certain niveau de confiance objective reste possible si la solution de sécurité a été soumise à des essais normalisés, conduits par un organisme indépendant, étroitement surveillé, et si un organisme officiel reconnu au plan international, quand les tests ont donné un résultat satisfaisant, appose sa signature sur l'attestation de certification. Et bien sûr chaque solution de même type doit passer les mêmes tests. C'est l'un des buts de la norme des Critères Communs (ISO/IEC 15408) conçue à la fin des années 1990 et qui évolue. Mais ces résolutions cachent bien des mythes et légendes, en voici quelques uns.

MYTHE N° 1 :

MA SOCIETE EST CERTIFIEE "CRITERES COMMUNS"

Non, la certification Critères Communs ne s'applique en aucun cas à un organisme. Elle ne peut être attachée qu'à une solution de sécurité. Si un produit qui a obtenu cette certification n'est plus commercialisé par le même éditeur, suite par exemple à un rachat de technologie ou suite à un rachat de l'éditeur qui a créé le produit, le produit n'en demeure pas moins certifié Critères Communs pour la version qui a obtenu cette certification.

Le sérieux affirmé par un organisme vis-à-vis de la sécurité, en d'autres termes vis à vis de la gestion de la sécurité de son propre système d'information, peut être certifié par rapport à d'autres normes comme celles de la famille ISO 2700x, en particulier par l'ISO 27001 qui est à la sécurité d'un système d'information, ce que l'ISO 9001 est à la qualité. Pour obtenir la certification ISO 27001, l'organisme doit gravir une pente qui le conduit à plus de sécurité en adoptant le modèle dit "roue de Deming". A chaque tour de la roue de Deming, les étapes "Plan, Do, Check, Act" se succèdent et la société mesure l'écart entre ce qui devrait être et ce qui est réellement, pour réduire cet écart. Cette ascension de la roue de Deming qui gravit une pente, conduit l'organisation à obtenir, puis à maintenir, sa certification ISO 27001. Mais cela est une autre facette de la sécurité et ne porte pas sur la certification d'un produit ou d'une solution intégrée de sécurité, donc sur la certification Critères Communs, objet de cet article.

Une société qui propose des services, mais aucun produit, peut être certifiée ISO 27001 et un constructeur ou éditeur de logiciels de sécurité qui n'est pas certifié ISO 27001 peut faire certifier ses produits "Critères Communs". Mais souvent il y a confusion entre ces normes.

La certification Critères Communs peut d'ailleurs s'appliquer également à des solutions comme des IPBX (autocommutateurs téléphoniques sur protocole IP) ou à des systèmes d'exploitation pour contrôler et affirmer dans le détail la robustesse c'est à dire l'exactitude des annonces de sécurité, et répondre à des questions comme : les protections sont-elles efficaces face aux menaces ?

MYTHE N° 2 :

LA CERTIFICATION CRITERES COMMUNS PORTE SUR L'ENSEMBLE D'UN PRODUIT

C'est un mythe de croire qu'un pare-feu (firewall), par exemple, certifié Critères Communs l'est sur l'ensemble de ses fonctionnalités, quelle que soit sa version et ses conditions d'emploi. La certification Critères Communs porte sur une version précise d'un produit, qui tourne sur une version précise d'un système d'exploitation ; le tout dans un environnement qui doit respecter un certain nombre d'hypothèses spécifiées dans le document « Cible de Sécurité ». Quand le pare-feu, ou autre logiciel, est proposé déjà intégré sur un ordinateur (une Appliance), la certification porte seulement sur certains des modèles de cet Appliance. Et quand l'Appliance comporte un pare-feu, un antivirus et un antispham, ni l'antivirus, ni l'antispham ne sont, le plus souvent, couverts par la cible de sécurité.

Tout ceci est écrit sur l'attestation remise avec la certification, encore faut-il la lire attentivement. Il ne serait pas très honnête, par exemple, pour un éditeur, d'affirmer "mon Appliance de sécurité a obtenu la certification Critères Communs au niveau EAL3+ (en insistant toujours sur le "+" !) alors que cette certification a été obtenue sur une version déjà ancienne de cette Appliance et qui n'est plus commercialisée, et peut-être sur un autre système d'exploitation que celui proposé à la vente. La sécurité du produit n'a pas forcément régressé depuis l'obtention de sa version certifiée, mais rien ne le prouve.

Un programme de maintenance de la certification de la solution existe, qui établit la non régression de la sécurité du produit sur la surface testée (la cible de sécurité) à chaque nouvelle version, ou après chaque action de maintenance majeure; mais l'éditeur a-t-il souscrit à ce programme ?

MYTHE N° 3 :

DEUX PRODUITS DE MEME TYPE, CERTIFIES CRITERES COMMUNS, SONT COMPARABLES

Il est certain que l'un des buts principaux des Critères Communs a été de permettre la comparaison, côté sécurité, entre des produits de même type, par exemple des pare-feux, des réseaux virtuels chiffrés (VPN) ou des produits de chiffrement sur disque. Les certifications précédentes, comme l'Orange Book aux USA ou les ITSEC en Europe n'avaient pas intégré cette possibilité, et c'est en quoi les Critères Communs se démarquent principalement des autres certifications de produits. Mais affirmer que deux produits de même type, certifiés Critères Communs à un même niveau, par exemple deux pare-feux certifiés Critères Communs EAL3+, sont comparables, peut être un mythe si on ne sait pas exactement ce que la certification recouvre pour chacun d'eux.

Une certification porte sur une certaine surface de fonctionnalités du produit, et sur certaines menaces que le produit doit contrôler. Tout ceci est consigné dans un document appelé la "cible de sécurité" (ST : Security Target). Deux outils de chiffrement sur disque certifiés EAL4+, chacun sur des cibles de sécurité différentes, ne sont assurément pas comparables. Avant de commencer une démarche de tests, le commanditaire doit faire accepter la cible de

sécurité par l'organisme officiel qui signera le certificat. En France, l'ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Information) est cet organisme. L'ANSSI, qui est rattachée au Premier Ministre, engage son sérieux par sa signature, et la confiance que porte un utilisateur dans un produit certifié dépend bien sûr de la confiance qu'inspire l'ANSSI

De plus, pour éviter que le commanditaire de la certification n'opère un savant découpage en dentelles de la cible de sécurité afin de n'y inclure que les fonctionnalités qu'il juge devoir réussir les tests sans problème, il a été introduit la notion de "Profil de Protection" (PP). Si des profils de protection existent, l'ANSSI peut exiger que le périmètre proposé à la certification respecte les exigences spécifiées dans ces documents. Ainsi deux produits de même type, peuvent présenter une cible minimale commune, mais bien sûr un constructeur peut faire certifier une cible plus étendue que celle constituée par l'ensemble des profils de protection exigés, afin de se démarquer de ses concurrents. Les produits ne sont alors plus comparables.

MYTHE N° 4 :

DANS EALx+, LE "+" EST LE PRINCIPAL FACTEUR DE QUALITE

Le niveau d'assurance (aussi communément appelé "niveau d'évaluation" ou "niveau de certification") définit la liste des contrôles qui doivent être réalisés sur le produit et son environnement de développement. Choisir un niveau d'évaluation, par exemple le niveau EAL4 (Evaluation Assurance Level de niveau 4) signifie sélectionner un paquet standard de contrôles tel que définit dans les Critères Communs. Les Critères Communs définissent 7 paquets de EAL1 à EAL7 comportant un nombre croissant de contrôles à réaliser. Mais les Critères Communs offrent aussi la possibilité aux commanditaires des évaluations de demander des contrôles supplémentaires, par exemple qui seraient requis pour des paquets EAL supérieurs. Cet ajout est nommé une "augmentation" du paquet standard EAL. Si la terminologie officielle impose de détailler dans le certificat la liste des augmentations, les fournisseurs de produits se contentent souvent d'un "+".

Ce que recouvre le "+" est parfois négligeable par rapport à ce que recouvre le paquet imposé par le niveau de certification choisi. Hors souvent l'acheteur est plus impressionné par le "+" que par le niveau de certification et ainsi se constitue le mythe du +, qui n'est pas le vrai différentiateur de qualité d'une certification Critères Communs. Mais le "+" peut tout de même recouvrir des éléments significatifs, comme les tâches d'assurance liées à la correction des défauts, ce qui intéresse directement l'acheteur.

MYTHE N° 5 :

UN CERTIFICAT CRITERES COMMUNS A UNE DATE DE PEREMPTION

Oui et Non. Comme nous l'avons indiqué auparavant, un certificat ne s'applique qu'à une version précise d'un produit. Il atteste qu'à la date de signature du certificat, le produit a passé avec succès tous les tests spécifiés dans sa cible de sécurité. Dans l'absolu, cette attestation n'a pas de raison d'être invalidée. En revanche, une personne qui souhaiterait utiliser ce certificat doit se poser la question suivante : vu les évolutions des techniques d'attaque depuis la signature de ce certificat, le produit ne risque-t-il pas aujourd'hui ou demain de ne plus passer la certification ? La ligne Maginot aurait sans doute obtenu la certification Critères Communs ... avant 1940.

L'ANSSI propose un programme de « Surveillance » qui revient à mettre à jour régulièrement les résultats des tests. Si cette surveillance est bien adaptée à des produits matériels qui n'évoluent pas, elle l'est moins pour des logiciels en constante évolution. En

effet, il faudrait alors se poser la question : si la version précédente du produit a passé avec succès l'évaluation il y a quelques mois, qu'en est-il de la nouvelle version aujourd'hui ?

Pour répondre à cette question, l'ANSSI propose deux solutions :

- fournir un rapport de maintenance qui, sur la base d'une analyse d'impact réalisée par le développeur, estime un niveau de "certificabilité" de la nouvelle version,
- faire réaliser par un CESTI une réévaluation de la nouvelle version du produit avec réutilisation au maximum des travaux déjà réalisés sur la version antérieure.

MYTHE N° 6 :

UNE CERTIFICATION CRITERES COMMUNS OBTENUE DANS UN DES PAYS CERTIFICATEURS EST AUTOMATIQUEMENT RECONNUE DANS TOUS LES PAYS

Les pays qui possèdent des centres de tests des produits et aussi des organismes officiels qui délivrent et maintiennent les certificats obtenus sont en nombre très limité. Seuls ces pays peuvent être des centres de certification. Un commanditaire qui veut faire certifier une solution de sécurité doit écrire la cible de sécurité sur laquelle portera la certification et la faire accepter par l'organisme officiel d'un des pays certificateurs, même s'il n'y réside pas. Les tests ayant donné un résultat satisfaisant, l'organisme officiel signera le certificat. La certification obtenue dans un des pays certificateurs est reconnue, en théorie, dans tous les pays.

Mais cela n'est vrai que jusqu'au niveau de certification EAL4. Au-delà, cela peut être un mythe. A partir du niveau de certification EAL5, une certification obtenue dans un des pays de la Communauté Européenne n'est reconnue que dans certains des pays de cette Communauté, et seulement aujourd'hui pour les "microcontrôleurs sécurisés et produits similaires". Cette certification Critères Communs au-delà du niveau EAL4 ne sera pas reconnue, aujourd'hui, par les USA. De même, une certification à partir du niveau EAL5 obtenue aux USA n'est pas reconnue dans les pays de la Communauté Européenne. Tout est question d'accords mutuels entre les organismes d'état de chacun des pays (CCRA, SOG-IS) et ces accords évoluent avec le temps.

MYTHE N° 7 :

UN NIVEAU DE CERTIFICATION EVALUE LES FONCTIONNALITES DE SECURITE D'UN PRODUIT

C'est ce qu'on pense généralement mais c'est une idée fausse. Le niveau EALx (Evaluation Assurance Level niveau "x") indique non pas l'étendue des fonctionnalités de sécurité soumises aux tests – c'est la cible de sécurité (ST) qui l'indique - mais la liste des contrôles qui doivent être réalisés sur ces fonctionnalités.

La documentation Critères Communs est constituée de trois volumes. Le deuxième volume est un catalogue de composants fonctionnels qui doivent être utilisés pour spécifier, dans le document Cible de Sécurité, les fonctionnalités de sécurité à évaluer. Une fois la cible de sécurité acceptée par l'organisme officiel (l'ANSSI en France), le niveau de certification sélectionné va définir la manière dont vont se dérouler les tests sur les fonctionnalités de la cible. Cette manière est définie par les composants d'assurance décrits dans le volume 3 des Critères Communs.

Ce niveau peut représenter une évaluation en boîte noire (EAL1) qui consiste à vérifier que le produit se comporte comme l'indique sa Cible de sécurité et sa documentation, ou en boîte blanche, à partir du niveau EAL2 où on commence à regarder comment le produit est conçu. La fourniture d'une partie des sources peut être exigée à partir du niveau EAL4.

A partir du niveau EAL5, les Critères Communs demandent à l'évaluateur de vérifier si le développeur a utilisé des méthodes semi-formelles ou formelles lors de la conception du produit pour la politique de sécurité (EAL5), pour la conception détaillée EAL6), pour la vérification du code (EAL7).

MYTHE N° 8 :

UNE SOLUTION DE SECURITE DOIT ETRE CERTIFIEE CRITERES COMMUNS POUR ENTRER DANS LE CATALOGUE DE L'ADMINISTRATION FRANÇAISE

Comme la démarche pour obtenir une certification Critères Communs dure plusieurs mois et coûte cher, y compris par les ressources internes du commanditaire qu'elle mobilise, peu de PME peuvent se permettre de réunir ce budget.

Pour permettre à tous de faire certifier un produit de sécurité, et même pour que les logiciels libres puissent obtenir une certification, l'ANSSI a conçu une certification plus légère : la CSPN (Certification de Sécurité de Premier Niveau).

En 25 jours de travaux (coûts limités), 35 jours si le produit comporte des mécanismes cryptographiques, une organisation peut faire évaluer son produit pour obtenir la certification CSPN. Bien entendu, la solution de sécurité peut ne pas obtenir cette évaluation à l'issue des 25 ou 35 jours mais les coûts sont limités et connus d'avance.

Pour entrer dans le catalogue des solutions de sécurité des administrations française, le produit certifié doit être également qualifié. La qualification implique une vérification par l'ANSSI que la cible de sécurité est conforme à des profils d'exigences et correspond aux besoins des administrations.

Trois niveaux de qualifications sont définis : élémentaire, standard, et renforcé. La qualification élémentaire implique une certification CSPN, les deux autres une certification Critères Communs. Il est donc faux d'affirmer qu'une solution de sécurité qui n'a pas la certification Critères Communs ne peut être vendue aux administrations.

Un logiciel libre peut ainsi trouver un commanditaire dans son club d'utilisateurs pour être évalué CSPN et entrer dans le catalogue des solutions de sécurité des administrations. TrueCrypt par exemple est certifié CSPN. Attention, la certification CSPN qui est purement française n'est reconnue qu'en France.

MYTHE N° 9 :

EN FRANCE, C'EST L'ANSSI QUI CONDUIT LES TESTS D'EVALUATION

Non, l'ANSSI n'intervient que dans la supervision le contrôle de la conformité des actions d'évaluations de sécurité effectuées par des laboratoires, et l'analyse du rapport d'évaluation, donnant ou non lieu à la délivrance du certificat Critères Communs ou CSPN. L'ANSSI publie les résultats sur son site Web.

Les tests d'évaluation sont menés par une société d'experts qui réalise les tests sur la base du document cible de sécurité écrit par le commanditaire et qui constitue son cahier des charges. Ces sociétés d'experts s'appellent des CESTI (Centre d'Évaluation de la Sécurité des Technologies de l'Information). Il existe en France deux CESTI habilités à mener les tests d'évaluation Critères Communs pour les logiciels et trois CESTI habilités à mener des tests pour les logiciels embarqués et les cartes à puces. Le CESTI est l'interface obligée entre le commanditaire et l'ANSSI qui signe le certificat au vue des rapports techniques délivrés par le CESTI. Toutefois, si la solution de sécurité comporte des mécanismes cryptographiques, l'ANSSI peut mener des analyses complémentaires sur ces mécanismes.

POUR EN SAVOIR PLUS :

www.ssi.gouv.fr/site_rubrique71.html

www.commoncriteriaportal.org/

MYTHES ET LEGENDES DU DROIT DE LA COMMUNICATION SUR L'INTERNET

*Sadry Porlon
Avocat au Barreau de Paris*

Le droit de la presse, dont la pierre angulaire reste la loi 29 juillet 1881, a été suivi par la création d'un droit plus large dit de la communication après l'apparition de la télévision, de la radio et plus récemment d'internet.

Ce droit de la communication qui, de prime abord, semble abordable, est en réalité un droit des plus techniques au sein duquel un formalisme des plus stricts doit être respecté pour envisager intenter avec succès une action devant les tribunaux ou encore faire valoir ses droits devant le responsable d'un site internet.

Il convient, en effet, de savoir distinguer la diffamation, de l'injure, du dénigrement ou encore de la simple atteinte à la vie privée pour être certain de voir ses demandes accueillies valablement par les juges.

L'apparition d'internet, sans pour autant avoir révolutionné le droit de la communication, a nécessité la mise en place des textes spécifiques contenus, pour la plupart, dans la loi du 24 juin 2004 dite Loi de Confiance dans l'Économie Numérique.

De nombreuses idées reçues sont diffusées autour du droit de la communication quand il touche à internet.

Gros plan sur certaines d'entre elles...

MYTHE N° 1 :

UNE INJURE OU UNE DIFFAMATION DONT ON EST VICTIME SUR INTERNET EST SUSCEPTIBLE D'UNE ACTION DEVANT LES TRIBUNAUX TANT QUE LE MESSAGE EST VISIBLE SUR LE SITE LITIGIEUX

A la fin des années 1990, la doctrine s'est penchée sur la question de savoir si les infractions de presse commises sur internet devaient ou non présenter une spécificité d'ordre procédural par rapport aux infractions propres à la presse écrite.

Elle s'est demandée si ces infractions devaient être considérées comme continues, lesquelles subsistent tant que les messages sont accessibles et ne font courir le délai de prescription qu'à compter de la date de leur suppression, ou comme « instantanées », ce délai démarrant alors dès la date de la mise en ligne, constitutive du fait de publication.

La Cour de cassation a posé, après quelques hésitations jurisprudentielles, que « lorsque des poursuites pour l'une des infractions prévues par la loi de 1881 sont engagées à raison de la diffusion, sur le réseau internet, d'un message figurant sur un site, le point de départ du délai de prescription de l'action publique prévu par l'article 65 de la loi du 29 juillet 1881 doit être fixé à la date du premier acte de publication ; que cette date est celle à laquelle le message a été mis pour la première fois à la disposition des utilisateurs ». (Cass. crim., 27 nov. 2001, C. : Comm. com. électr. 2002, comm. 32, obs. A. Lepage ; Légipresse 2002, n° 189, III, p. 26 et 27).

Dès lors, il faut donc considérer que sur internet, comme en matière de presse écrite, le délai de prescription commence à courir à compter du premier jour de la publication et que le fait que le message demeure accessible ou disponible n'y change rien.

Ce principe, qui peut paraître injuste à bien des égards, oblige celui qui s'interroge sur le bien fondé d'une action pour diffamation ou pour injure, suite à la découverte sur internet de propos litigieux, à s'assurer préalablement que le message a bien été publié moins de trois mois avant.

L'article 6-V de la loi de la Loi de Confiance dans l'Économie numérique du 21 juin 2004 renvoie, en effet, aux dispositions de l'article 65 de la loi de 1881 qui prévoit que ce délai de prescription est de trois mois à compter de la date de la publication.

Par ailleurs, depuis une loi n° 2004-204 du 9 mars 2004, le délai de prescription des infractions à caractère raciste (exemples : provocation à la discrimination ou à la haine raciale, diffamation raciale, injure raciale) est d'un an. Ce délai s'applique également à Internet.

MYTHE N° 2 :

IL FAUT AVOIR ETE INJURIE, DIFFAME OU DENIGRE POUR POUVOIR OBTENIR UN DROIT DE REPONSE AUPRES DU SITE INTERNET A L'ORIGINE DE L'INFRACTION

Le droit de réponse à un caractère général et absolu. Cela implique donc qu'il n'est pas subordonné à la preuve que les propos auxquels il répond soient motivés par une intention de nuire de la part de son auteur.

L'article 6, IV alinéa 1 de la loi du 21 juin 2004 dispose en effet que :

« Toute personne nommée ou désignée dans un service de communication au public en ligne dispose d'un droit de réponse, sans préjudice des demandes de correction ou de suppression du message qu'elle peut adresser au service (...) ».

Il suffit donc d'avoir été nommée ou désignée sur internet pour pouvoir prétendre à un droit de réponse auprès du directeur de publication du site.

Dans l'absolu, même un article flatteur et complètement exact est susceptible de provoquer un droit de réponse des plus valables de la part de la personne nommée ou désignée dans l'article ou le message disponible sur internet.

Une disposition des plus utiles pour une personne physique ou morale qui, ne trouvant pas la matière suffisante à une action pour diffamation ou pour injure aurait, par cet intermédiaire, l'occasion de donner son point de vue et sa version des faits en réplique à l'article ou un message litigieux.

MYTHE N° 3 :

IL FAUT AVOIR ETE INJURIE, DIFFAME OU DENIGRE POUR POUVOIR OBTENIR UN DROIT DE REPONSE AUPRES DE LA TELEVISION OU DE LA RADIO A L'ORIGINE DE L'INFRACTION

Tout dépendra en réalité du moyen de diffusion de cette télévision ou de cette radio.

Il faut savoir que la réglementation du droit de réponse dans les services de communication audiovisuelle (c'est à dire à la télévision ou à la radio) est extérieure à la loi du 29 juillet 1881.

Le droit de réponse spécifique à la presse écrite n'a donc pas été, contrairement à internet, directement transposé en matière audiovisuelle.

Le droit de réponse à la radio ou à la télévision est subordonné à la démonstration « d'imputations susceptibles de porter atteinte à l'honneur ou à la réputation d'une personne ».

L'article 6 de la loi du 29 juillet 1982 dispose que : « Toute personne physique ou morale dispose d'un droit de réponse dans le cas où des imputations susceptibles de porter atteinte à

son honneur ou à sa réputation auraient été diffusées dans le cadre d'une activité de communication audiovisuelle (...)

Il existe néanmoins une exception à ce principe.

Dans le cas de ce qu'on appelle une web télé ou d'une web radio (médias diffusés exclusivement sur internet), la réglementation relative au droit de réponse redevient celle prévue à l'article 6 IV de la loi du 21 juin 2004, ce qui implique que tout message désignant une personne peut être à l'origine d'un droit de réponse ; quelle que soit sa teneur.

MYTHE N° 4 :

DEMANDER UN DROIT DE REPONSE A L'EDITEUR D'UN SITE INTERNET ET L'OBTENIR EMPECHE TOUTE ACTION DEVANT LES TRIBUNAUX CONTRE L'AUTEUR DES PROPOS.

Les actions pour diffamation ou pour injure sont indépendantes de l'exercice du droit de réponse.

Une personne peut donc légitimement solliciter un droit de réponse en engageant simultanément une action devant les tribunaux contre l'auteur du message diffusé sur internet.

MYTHE N° 5 :

LE FAIT QUE L'AUTEUR D'UN MESSAGE DIFFAMATOIRE OU INJURIEUX SE SOIT EXCUSE PUBLIQUEMENT SUITE A LA DIFFUSION DU PROPOS LUI PERMETTRA D'ECHAPPER A UNE SANCTION EN CAS D'ACTION DEVANT LES TRIBUNAUX.

Le repentir actif, c'est-à-dire l'action qui consiste pour l'auteur d'un message injurieux ou diffamatoire à présenter ses excuses publiques ou à publier un rectificatif, ne supprime pas l'intention coupable.

La personne directement visée par les propos litigieux pourra toujours agir et obtenir la condamnation de son auteur.

MYTHE N° 6 :

LE FAIT POUR L'EDITEUR D'UN SITE INTERNET DE NE PAS AVOIR MIS A DISPOSITION DES INTERNAUTES UN CERTAIN NOMBRE D'ELEMENTS D'IDENTIFICATION COMME, POUR LES PERSONNES PHYSIQUES, (SON NOM, SON PRENOM, SON DOMICILE) OU POUR LES PERSONNES MORALES (SA DENOMINATION, SA RAISON SOCIALE OU ENCORE SON SIEGE SOCIAL) NE PEUT PAS LUI VALOIR UNE CONDAMNATION DEVANT LES TRIBUNAUX.

Le non-respect des obligations prévues à l'article 6-III-1 de la loi du 21 juin 2004 est « puni d'un an d'emprisonnement et de 75 000 euros d'amende ». (Article 6-VI-2 de la loi du 21 juin 2004).

Les personnes morales peuvent se voir interdire d'exercer leur activité « pour une durée de cinq ans au plus ». (L. 131-38 et L. 131-39 du Code pénal).

L'article 6-III-2 prévoit une exception notamment pour les blogueurs anonymes qui exercent cette activité à titre non professionnel.

Cet article pose, en effet, que « les personnes éditant à titre non professionnel un service de communication au public en ligne peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination ou la raison sociale » de leur fournisseur d'hébergement, « sous réserve de lui avoir communiqué les éléments d'identification personnelle » exigés des éditeurs de services agissant à titre professionnel.

C'est d'ailleurs cette distinction entre les obligations d'identification auxquelles sont tenus les éditeurs professionnels et les éditeurs non professionnels de services en ligne qui a motivé la fameuse proposition de loi en date du 3 mai 2010 du Sénateur Jean-Louis Masson, laquelle tendait « à faciliter l'identification des éditeurs de sites de communication en ligne et en particulier des « blogueurs » professionnels et non professionnels ».

MYTHE N° 7 :

IL EST POSSIBLE DE REPRODUIRE INTEGRALEMENT L'ARTICLE D'UN AUTEUR SUR SON SITE A CONDITION DE CITER SON NOM ET LA SOURCE DE L'ARTICLE.

L'article L. 122-4 du Code de la propriété intellectuelle dispose que :

« Toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droits est illicite. Il en est de même pour la traduction, l'adaptation ou la transformation, l'arrangement ou la reproduction par un art ou un procédé quelconque. »

L'article L. 335-2 alinéa 3 du Code de la propriété intellectuelle ajoute que :

« Toute édition d'écrits, de composition musicale, de dessin, de peinture ou de toute autre production imprimée ou gravée en entier ou en partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est une contrefaçon, et toute contrefaçon est un délit. »

Il s'agit d'un délit puni de trois ans d'emprisonnement et de 300.000 euros d'amende.

L'article L. 122-5 du Code de la propriété intellectuelle prévoit néanmoins une exception dans le cas où il s'agit d'une courte citation de l'article.

La courte citation s'évaluera par rapport aux dimensions de l'œuvre citée, mais aussi de celle de l'œuvre citante. Cette citation devra être justifiée par certaines finalités (critique, polémique, pédagogique, scientifique ou d'information) de l'œuvre d'origine.

Elle devra également être intégrée à une œuvre ayant une autonomie propre en dehors des citations.

MYTHE N° 8 :

LE FAIT DE REPRODUIRE UNE ŒUVRE OU UN CONTENU SUR UN SITE INTERNET A VOCATION NON COMMERCIALE PERMET D'ÉCHAPPER A UNE CONDAMNATION POUR CONTREFAÇON.

Malgré une forte croyance chez l'internet lambda, la loi n'a jamais entendu faire de distinction l'éditeur d'un site qui reproduit l'œuvre d'un tiers sans autorisation et dans un but commercial et celui qui le fait dans un but non commercial.

Les deux sont, dès lors, potentiellement condamnables pour contrefaçon à ce titre tant sur le plan pénal que sur le plan civil.

CONCLUSION

Ces quelques exemples contribuent à illustrer le fossé qui existe entre la perception qu'à l'internaute lambda d'un internet dans lequel régnerait le vide juridique et la réalité dans laquelle ce média n'a finalement eu que peu de mal à se voir appliquer des règles datant du XIX^{ème} siècle.

Les contentieux sans cesse croissants générés par quelques uns des millions de messages diffusés quotidiennement sur les blogs, les forums de discussion ou encore à travers les réseaux sociaux comme Facebook ou Twitter, sont d'ailleurs là pour en témoigner.

MYTHES ET LEGENDES DES TELECHARGEMENT ILLEGAUX

Sadry Porlon
Avocat au Barreau de Paris

La loi du 12 juin 2009 favorisant la diffusion et la protection de la création (dite HADOPI 1), puis celle du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet (dite HADOPI 2) ont conduit d'une part, à la création de la HADOPI, Haute autorité pour la diffusion des œuvres et la protection des œuvres, à celle de création d'une obligation pour le titulaire de l'accès à l'internet ne soit pas utilisé à des fins de contrefaçon, sorte d'obligation de sécurisation de l'accès à l'internet à la charge de l'abonné, faute de quoi il s'exposera notamment à la contravention de négligence caractérisée, et d'autre part à adapter le dispositif pénal applicable aux contrefaçons commises sur internet.

Quelques idées reçues existent encore sur le téléchargement illégal en général et sur HADOPI en particulier...

MYTHE N°1 :

L'EXCEPTION POUR COPIE PRIVEE PERMET A CELUI QUI TELECHARGE UNE ŒUVRE SUR INTERNET SANS AUTORISATION DE NE PAS ETRE CONDAMNE DEVANT LES TRIBUNAUX S'IL DEMONTRE QUE LADITE COPIE A FAIT L'OBJET D'UNE UTILISATION STRICTEMENT PRIVEE

L'article L. 122-5 du Code de la propriété intellectuelle prévoit qu'il est possible de copier une œuvre pour un usage privé.

L'article L. 122-5 alinéa 2 refuse, en effet, la possibilité à l'auteur de l'œuvre d'interdire « les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective (...) ».

L'exception affirmée par le Code de propriété intellectuelle ne distingue pas selon les supports.

Mieux, il n'est nulle part exigé que le copiste se doive de disposer de l'œuvre originale pour en faire la copie. L'article L 122-5 du Code de la propriété intellectuelle qui accorde à l'utilisateur un droit à la copie privée ne distingue pas non plus selon que la copie soit légale ou pas ou encore que l'utilisateur possède l'original dont il fait la copie.

La question de savoir si l'exception de copie privée trouve ou non à s'appliquer dans le cas d'une copie d'œuvres téléchargées sur internet, notamment via logiciel peer to peer, a donc longtemps été, de ce fait, l'objet d'une vive controverse doctrinale et jurisprudentielle.

Des opinions défavorables à la prise en compte de l'exception pour copie privée en cas de téléchargement sans autorisation se sont développées à partir de l'idée selon laquelle la copie réalisée à partir d'un exemplaire contrefaisant est elle-même contaminée par ce caractère illicite et ne peut donc pas être couverte par l'exception pour copie privée.

La jurisprudence est venue depuis clarifier quelque peu la situation.

Dans une affaire qui a fait beaucoup parler, un étudiant avait gravé près de 500 films sur cédéroms ; films qu'il avait, notamment, auparavant téléchargés sur Internet. Poursuivi

devant les tribunaux pour contrefaçon de droit d'auteur par la majeure partie de l'industrie cinématographique mondiale, il a tenté de se prévaloir de l'exception pour copie privée.

En premier instance, le Tribunal correctionnel de Rodez a conclu, le 13 octobre 2004, à l'absence de contrefaçon, ce qu'a confirmé la Cour d'Appel de Montpellier, dans un arrêt en date du 10 mars 2005, sans pour autant se prononcer sur le caractère licite ou illicite de la source des copies.

La Cour de Cassation est venue casser l'arrêt précité en retenant notamment que :

« Attendu que, pour confirmer le jugement entrepris, l'arrêt retient qu'aux termes des articles L 122-3, L 122-4 et L 122-5 du code de la propriété intellectuelle, lorsqu'une œuvre a été divulguée, l'auteur ne peut interdire les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective ; que les juges ajoutent que le prévenu a déclaré avoir effectué les copies uniquement pour un usage privé et qu'il n'est démontré aucun usage à titre collectif ;

Mais attendu qu'en se déterminant ainsi, sans s'expliquer sur les circonstances dans lesquelles les œuvres avaient été mises à disposition du prévenu et sans répondre aux conclusions des parties civiles qui faisaient valoir que l'exception de copie privée prévue par l'article L 122-5, 2°, du code de la propriété intellectuelle, en ce qu'elle constitue une dérogation au monopole de l'auteur sur son œuvre, suppose, pour pouvoir être retenue que sa source soit licite et nécessairement exempte de toute atteinte aux prérogatives des titulaires de droits sur l'œuvre concernée, la cour d'appel n'a pas justifié sa décision ; ».

Dès lors, il n'est donc pas possible de prétexter valablement de l'exception pour copie privée pour télécharger, sans autorisation, des œuvres sur internet.

MYTHE N°2 :

DEPUIS LES LOIS HADOPI, LE TELECHARGEMENT ILLEGAL D'UNE ŒUVRE SUR INTERNET NE PEUT PLUS ETRE SANCTIONNE « QUE » PAR UNE SUSPENSION D'INTERNET PENDANT UN MOIS MAXIMUM ET D'UNE AMENDE NE DEPASSANT PAS 1500 EUROS.

Un décret du 25 juin 2010, pris en application de la loi HADOPI 2 est venu définir ce qu'est la contravention de négligence caractérisée tout en précisant la caractérisation de ce manquement et les sanctions encourues par l'abonné.

L'article R. 335-5 du Code de la propriété intellectuelle dispose désormais que :

« I.-Constitue une négligence caractérisée, punie de l'amende prévue pour les contraventions de la cinquième classe, le fait, sans motif légitime, pour la personne titulaire d'un accès à des services de communication au public en ligne, lorsque se trouvent réunies les conditions prévues au II :

1. Soit de ne pas avoir mis en place un moyen de sécurisation de cet accès ;
2. Soit d'avoir manqué de diligence dans la mise en œuvre de ce moyen.

II.-Les dispositions du I ne sont applicables que lorsque se trouvent réunies les deux conditions suivantes :

1. En application de l'article L. 331-25 et dans les formes prévues par cet article, le titulaire de l'accès s'est vu recommander par la commission de protection des droits de mettre en œuvre un moyen de sécurisation de son accès permettant de prévenir le renouvellement d'une utilisation de celui-ci à des fins de reproduction, de représentation ou de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise ;

2. Dans l'année suivant la présentation de cette recommandation, cet accès est à nouveau utilisé aux fins mentionnées au 1° du présent II.

III.-Les personnes coupables de la contravention définie au I peuvent, en outre, être condamnées à la peine complémentaire de suspension de l'accès à un service de communication au public en ligne pour une durée maximale d'un mois, conformément aux dispositions de l'article L. 335-7-1.

L'abonné s'expose donc à ce titre à une contravention de 5ème classe (amende de 1500 euros maximum) ainsi qu'à une peine complémentaire de suspension de l'accès à internet qui ne pourra excéder un mois.

Cependant, le recours à la procédure judiciaire simplifiée de l'ordonnance pénale prévue par la loi HADOPI 2 n'est qu'une possibilité qui vient s'ajouter aux actions civiles et pénales liées à la contrefaçon de droit d'auteur et en aucun un préalable nécessaire à l'engagement de poursuites.

Tout abonné dont l'accès à internet a été utilisé à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits reste, en effet, sous la menace d'une action en contrefaçon de droit d'auteur et des sanctions encourues en matière de contrefaçon soit une peine maximum d'emprisonnement de 3 ans et une amende de 300.000 euros (article L. 335-2 du Code de la propriété intellectuelle).

La loi HADOPI 2 a d'ailleurs apporté des changements en matière de sanctions pénales en précisant qu'une nouvelle possibilité de sanction pénale est donnée au juge lorsque le délit de contrefaçon a été commis par le biais d'un service de communication au public en ligne à savoir celle de prononcer une peine complémentaire de suspension de l'accès à internet pendant une durée maximale d'un an (Article L. 335-7 alinéa 1).

MYTHE N°3 :

SI MON ACCES A INTERNET EST SUSPENDU SUITE A UNE DECISION DU JUGE, IL ME SUFFIT DE SOUSCRIRE IMMEDIATEMENT UN NOUVEL ABONNEMENT

Il est interdit à un abonné dont l'accès à internet aurait été suspendu suite à une décision du juge de se réabonner par un autre moyen.

L'article L. 335-7-1 du Code de la propriété intellectuelle prévoit d'ailleurs que le fait pour la personne condamnée à la peine complémentaire de suspension d'internet de ne pas respecter l'interdiction de souscrire un autre contrat d'abonnement à un service de communication au public en ligne pendant la durée de la suspension est puni d'une amende d'un montant maximal de 3 750 euros.

MYTHE N°4 :

SI LE JUGE DECIDE D'UNE SUSPENSION DE MON ABONNEMENT, JE NE VAIS QUAND MEME PAS ETRE CONTRAINT DE CONTINUER A PAYER CET ABONNEMENT PENDANT LA DUREE DE CETTE SUSPENSION

Dans l'hypothèse d'une suspension d'internet pendant un maximum d'un an au motif qu'une sanction pénale au titre d'une contrefaçon aurait été prononcée par le juge cette suspension de l'accès n'affecte pas, par elle-même, le versement du prix de l'abonnement au fournisseur du service.

L'article L. 121-84 du code de la consommation qui dispose : « Tout projet de modification des conditions contractuelles de fourniture d'un service de communications électroniques est communiqué par le prestataire au consommateur au moins un mois avant son entrée en

vigueur, assorti de l'information selon laquelle ce dernier peut, tant qu'il n'a pas expressément accepté les nouvelles conditions, résilier le contrat sans pénalité de résiliation et sans droit à dédommagement, jusque dans un délai de quatre mois après l'entrée en vigueur de la modification » n'est pas applicable au cours de la période de suspension.

Les frais d'une éventuelle résiliation de l'abonnement au cours de la période de suspension sont supportés par l'abonné.

Pour information, le fait pour une le fournisseur d'accès à internet de ne pas mettre en œuvre la peine de suspension qui lui a été notifiée est également puni d'une amende maximale de 5 000 euros.

MYTHE N°5 :

L'ABONNE QUI REÇOIT DES RECOMMANDATIONS DE LA PART DE LA HADOPI DEVRA ATTENDRE D'ÊTRE POURSUIVI DEVANT LES TRIBUNAUX POUR FAIRE VALOIR SES DROITS

L'abonné qui reçoit un ou plusieurs avertissements peut directement présenter ses observations à la Commission de protection de la HADOPI et demander des précisions sur le contenu des œuvres et objets protégés concernés par le ou les manquements qui lui sont reprochés.

Il pourra notamment être convoqué ou demandé à être entendu et pourra se faire assister du conseil de son choix.

Si une ordonnance pénale venait à être rendue à son encontre, l'abonné aura également la possibilité de contester la décision rendue, dans un délai de quarante cinq jours à compter de la notification en formant opposition à l'exécution de ladite ordonnance.

Cela a pour conséquence de renvoyer l'affaire devant le tribunal correctionnel pour un débat qui sera, cette fois, contradictoire.

Il reviendra alors à l'abonné de monter, le cas échéant avec l'aide de son conseil, un dossier visant à démontrer, preuves à l'appui, qu'il n'est en aucun cas le responsable des faits qui lui sont directement reprochés et qu'eu égard à l'article 121-1 du Code pénal disposant que : « Nul n'est responsable que de son propre fait », il ne peut être valablement sanctionné.

MYTHE N°6:

EN PRESENCE D'UN TELECHARGEMENT ILLEGAL AVERE, LE JUGE A UNE MARGE DE MANŒUVRE ASSEZ FAIBLE DANS LA FIXATION DE LA DUREE DE LA SUSPENSION DE L'ACCES A INTERNET

L'article L. 335-7-2 du Code de la propriété intellectuelle prévoit que pour prononcer la peine de suspension (peine complémentaire à l'amende de contravention de 5^{ème} catégorie) prévue aux articles L. 335-7 (un an maximum en cas de contrefaçon) et L. 335-7-1 (un mois maximum en cas de négligence caractérisée) et en déterminer la durée, la juridiction prend en compte les circonstances et la gravité de l'infraction ainsi que la personnalité de son auteur, et notamment l'activité professionnelle ou sociale de celui-ci, ainsi que sa situation socio-économique.

Ainsi, cet article permet notamment au juge de tenir compte de la personnalité de l'abonné afin de déterminer la peine complémentaire de suspension d'internet.

On imagine que cela puisse être le cas d'une entreprise pour laquelle le maintien de la connexion à internet est la condition sine qua non du maintien de son activité ou encore d'un particulier qui justifierait que ce média est pour lui une ouverture indispensable sur le monde.

L'article 335-7-2 du Code de la propriété intellectuelle précise d'ailleurs que la durée de la peine prononcée doit concilier la protection des droits de la propriété intellectuelle et le respect du droit de s'exprimer et de communiquer librement, notamment depuis son domicile.

MYTHE N°7 :

C'EST LA HAUTE AUTORITE POUR LA DIFFUSION DES ŒUVRES ET LA PROTECTION DES ŒUVRES QUI COLLECTE, ELLE-MEME, LES ADRESSES IP DES ABONNES DONT L'ACCES A SERVI A TELECHARGER DES ŒUVRES

La HADOPI, saisie en cela par les ayants droits des œuvres, peut constater et établir des procès verbaux de manquements à l'obligation de sécurisation, adresser des avertissements aux abonnés ou encore transmettre au procureur de la République tout fait susceptible de constituer une infraction.

Elle ne collecte pas directement les adresses IP.

Ce sont les organismes assermentés représentant les titulaires des droits (pour l'heure, la société Trident Media Guard - TMG) qui, ayant reçu préalablement les autorisations nécessaires de la CNIL pour effectuer ces démarches, se chargent d'observer les œuvres circulant sur les réseaux et de collecter ce type informations.

La HADOPI se contente de recevoir les saisines des sociétés de perception et de répartition des droits et des organismes de défense professionnelle ayant reçu une autorisation de la CNIL.

Elle peut par la suite obtenir des fournisseurs d'accès à l'internet ou des prestataires d'hébergement, l'identité, l'adresse postale, l'adresse électronique et les coordonnées téléphoniques de l'abonné dont l'accès à l'internet a été utilisé à des fins de contrefaçon et ce sur la base des adresses IP collectées par les sociétés privées mandatées par les ayants droit pour surveiller les réseaux de téléchargement illégal.

La réponse graduée débutera ensuite par l'envoi d'une recommandation ou « avertissement » à l'abonné par le biais d'un courriel et par l'intermédiaire du fournisseur d'accès auprès duquel il a souscrit un abonnement.

Celle-ci prévoit notamment un rappel de l'obligation de sécurisation, la mention de la date et l'heure auxquelles les faits susceptibles de constituer un manquement à l'obligation de sécurisation ont été constatés ainsi que les coordonnées téléphoniques, postales et électroniques où l'abonné peut s'adresser, s'il le souhaite, pour formuler ses observations et obtenir des précisions sur ce qui lui est reproché.

Si dans les six mois suivant cette recommandation l'accès à internet devait à nouveau être utilisé pour « des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits lorsqu'elle est requise », une seconde recommandation pourra lui être adressée par le biais d'une lettre recommandée avec avis de réception ou encore par tout autre moyen permettant d'établir la preuve de la date de présentation de cette recommandation.

La loi HADOPI 1 a imposé à la personne titulaire de l'accès à des services de communication au public en ligne l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits lorsqu'elle est requise.

Si malgré un second avertissement l'accès internet de l'abonné devait de nouveau servir à des fins de contrefaçon de droit d'auteur, la HADOPI pourra remettre son dossier à un juge afin que l'abonné soit, notamment, sanctionné d'une amende et/ou d'une suspension de son accès à internet ou encore transmettre au procureur de la république tout fait susceptible de constituer une infraction.

CONCLUSION

Ces quelques exemples démontrent une fois de plus le fossé qui existe entre le grand public qui associe assez souvent internet gratuité et le législateur qui n'a finalement qu'à de rares exceptions accepté que ce média puisse déroger aux grands principes du droit de la propriété intellectuelle.

GLOSSAIRE

MYTHES ET LEGENDES DE L'INTERNET

ATM : Asynchronous Transfer Mode

ETSI : European Telecommunications Standards

ICANN : Internet Corporation for Assigned Names and Numbers

IETF : Internet Engineering Task Force

IPsec : Internet Protocol Security

IPv6 : Internet Protocol version 6

ISO : International Organization for Standardization

NAT : Network Address Translation

P2P : Pair-to-Pair

RINA : Recursive Inter-Network Architecture

ToIP : Telephony on IP

UIT : Union internationale des télécommunications

MYTHES ET LEGENDES DE LA SECURITE DE L'INFORMATION

CERT : Computer Emergency Response Team

MYTHES ET LEGENDES DU CHIFFREMENT

3DES : Triple Data Encryption Standard

AES : Advanced Encryption Standard

RSA : Rivest Shamir Adleman, algorithme de cryptographie asymétrique du nom de ses inventeurs

MYTHES ET LEGENDES DE LA SIGNATURE ELECTRONIQUE

MD5 : Message Digest 5, fonction de hachage

PIN : Personal Identification Number

SHA1,2,3 : Secure Hash Algorithm

MYTHES ET LEGENDES DE LA CERTIFICATION CRITERES COMMUNS

ANSSI : Agence nationale de la sécurité des systèmes d'information

EALn : Evaluation Assurance Level n

ITSEC : Information Technology Security Evaluation Criteria

VPN : Virtual Private Network

BIBLIOGRAPHIE

A PROPOS DES AUTEURS

Par ordre alphabétique :



Jean Pierre CABANEL est Professeur à l'Institut National Polytechnique (INP / ENSEEIHT) de Toulouse et membre du laboratoire IRT (Institut de Recherche en Informatique de Toulouse), équipe Université. Il anime un groupe de recherche sur le futur des télécommunications. Ses travaux récents traitent de l'autonomie des vecteurs aériens et spatiaux.

Jean Pierre Cabanel est Docteur d'état de l'Université Paul Sabatier (Toulouse) en 1982. Il travaille en premier au sein du laboratoire IBM de Yorktown (USA), avant de retrouver les projets « pilotes » de l'INRIA dans le cadre du laboratoire de l'IRT. Il anime avec le Professeur Guy Pujolle le « Working Group » 6.4 de l'IFIP sur les LAN et PABX et organise plusieurs congrès au sein de Sup Telecom. Paris.

Il travaille ensuite sur la problématique de la sécurité des systèmes de communication : PKI : Private Key Infrastructure, et TPC : Tierce Partie de Confiance. [jeanpierre.cabanel \(at\) free.fr](mailto:jeanpierre.cabanel@free.fr)

Franck FRANCHIN, co-auteur de l'ouvrage "Le Business de la Cybercriminalité", travaillant à la Direction de la Sécurité Groupe de France Telecom, est spécialiste depuis 20 ans en architectures sécurisées de systèmes civils ou militaires et en cybercriminalité. Il est ingénieur diplômé de Supélec et de l'ENSEEIH et titulaire d'un MBA de l'ESCP. Il mène aussi des recherches sur la résilience des infrastructures vitales dans l'équipe de la Professeure Solange Ghernanouti-Hélie de la Faculté des Hautes Etudes Commerciales de l'Université de Lausanne.



David GROUT est responsable avant vente chez McAfee

Titulaire d'un master en Informatique eBusiness, il est également titulaire de plusieurs certifications comme CISSP, Comptia Security +.

Il est aujourd'hui à la tête d'une équipe de 5 personnes et gère l'ensemble du marché entreprise en France. Présent dans le domaine de la sécurité depuis plus de 7 ans il intervient aussi lors de séminaires ou de parutions dans la presse informatique : [David_Grout \(at\) McAfee.com](mailto:David_Grout (at) McAfee.com)



Daniel HAGIMONT est Professeur à l'Institut National Polytechnique (INP / ENSEEIHT) de Toulouse et membre du laboratoire IRT (Institut de Recherche en Informatique de Toulouse), où il anime un groupe de recherche autour des systèmes d'exploitation, des systèmes répartis et des intergiciels. Ses travaux plus récents concernent les systèmes d'administration autonomes.

Daniel Hagimont a obtenu un doctorat de l'Institut National Polytechnique de Grenoble en 1993. Après une année postdoctorale à l'Université de Colombie Britannique (Vancouver) en 1994, il a rejoint l'INRIA en 1995 comme Chargé de Recherche. Il a ensuite pris ses fonctions de Professeur en 2005. daniel.hagimont@enseeiht.fr



Gérard PELIKS est expert sécurité dans le Cyber Security Customer Solutions Centre de EADS.

Il préside l'atelier sécurité de l'association Forum ATENA, participe à la commission sécurité des systèmes d'Information de l'AFNOR et anime un atelier sécurité dans le cadre du Cercle d'Intelligence Économique du Medef de l'Ouest Parisien. Il est membre de l'ARCSI et du Club R2GS.

Gérard Peliks est chargé de cours dans des écoles d'Ingénieurs, sur différentes facettes de la sécurité. *gerard.peliks (at) cassidian.com*



Sadry PORLON est avocat au barreau de Paris

Docteur en droit, il est également chargé d'enseignements, au sein d'une école de commerce, notamment, en droit des médias et de la communication, en droit du commerce électronique et du multimédia ainsi qu'en droit des marques.

avocat (at) porlon.net



Nicolas RUFF est chercheur au sein de la société EADS.

Il est l'auteur de nombreuses publications sur la sécurité des technologies Microsoft dans des revues spécialisées telles que MISC. Il dispense régulièrement des formations sur le sujet et participe à des conférences telles que SSTIC, les Microsoft TechDays ou la JSSI de l'OSSIR.

nicolas.ruff (at) eads.net



Philippe VACHEROUT est président de Capucine.net

Entré à la Cnamts en 1975, il est à l'initiative de la création des Centres de traitements électronique inter-caisses et des Centres de traitement informatique de Saint-Etienne, Troyes et Rouen.

La carte à puce citoyenne Capucine est une carte sans contacts, acoustique. Le son émis est différent à chaque fois, donc impossible à décrypter.

phvacheyrout (at) capucine.net

