MYTHES ET LEGENDES DES TIC TOME 2

24 novembre 2011

Collection ATENA

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

Louis Derathe, Jean-Denis Garo, Francesca Musiani, Gérard Peliks, Nicolas Ruff

Livre collectif sous la direction de Gérard Peliks

INTRODUCTION

Ce document est le début du tome 2 du livre collectif "Mythes et légendes des TIC" développé dans le cadre de l'association Forum ATENA.

Si vous désirez obtenir la version complète PDF du tome 1 du livre "Mythes et légendes des TIC", il est téléchargeable en :
http://www.forumatena.org/LB47/MythesEtLegendesDesTIC1605.pdf

Si vous désirez commander sa version papier c'est sur :
http://www.lulu.com/product/couverture-souple/mythes-l%C3%A9gendes-des-tic/15739496

Si vous êtes intéressés d'être tenus au courant de ses développements, voire si vous désirez en devenir un des auteurs, demandez le moi par e-mail.

Gérard Peliks
gerard.peliks@cassidian.com
Président de l'atelier sécurité de Forum ATENA

SOMMAIRE

1° PARTIE : ASPECTS INFORMATION ET SYSTEMES D'INFORMATION

MYTHES ET LEGENDES DU PEER-TO-PEER

Francesca Musiani, CSI, MINES ParisTech

INTRODUCTION

Le *peer-to-peer* (P2P, « pair-à-pair » en français) est devenu l'un des termes les plus largement discutés dans le domaine des technologies de l'information et de la communication. Il se réfère à la notion que dans un réseau d'égaux ou de pairs, à l'aide de systèmes de communication et d'échanges appropriés, deux ou plusieurs individus sont en mesure de collaborer spontanément, sans nécessairement avoir besoin de coordination centrale.

Depuis la fin des années 90, les technologies P2P ont fait l'objet d'une évolution très rapide. Le grand succès dont les applications de cette technologie ont bénéficié a certes été un catalyseur important de la créativité de leurs développeurs, et des perfectionnements de ces outils en termes d'efficacité, mais les évolutions du secteur ont largement été influencées par des contraintes politiques, économiques et juridiques, notamment les menaces de procès mises sur la table par certains des grands acteurs de l'industrie du contenu numérique. Trois générations technologiques se sont ainsi succédées, tandis que le modèle P2P commençait à être appliqué non plus seulement au partage de fichiers mais à une variété d'usages et d'applications, dévoilant la complexité de l'objet et la multiplicité de ses mobilisations. Ce chapitre rend compte de comment, autour et au moyen de ces mobilisations, des discours partiels ou réducteurs ont pris forme avec le P2P – discours qui cachent trop souvent les expérimentations socio-économiques à l'œuvre de par ou avec le P2P, et qui empêchent ou entravent un renouvellement du débat politique autour de ces systèmes.

MYTHE N° 1 : LE PEER-TO-PEER, C'EST DU PIRATAGE

Depuis que, en 1999, la naissance de *Napster* leur a donné visibilité et diffusion auprès du grand public, les réseaux informatiques *P2P* ont été considérés presque exclusivement comme une menace pour l'industrie des contenus numériques. L'usage principal de ces réseaux par le public étant le partage non autorisé de fichiers musicaux ou vidéo, le problème du droit de propriété intellectuelle, du droit d'auteur notamment, s'est imposé en tant que cadrage médiatique et politique prédominant des réseaux P2P et leurs usages. Cependant, l'argument qui consiste, essentiellement, à assimiler P2P et piratage, présente plusieurs limites.

Avec des millions d'usagers à l'échelle mondiale (le pionnier *Napster* comptait, l'année même de sa création, 60 millions d'usagers « partageurs »), les réseaux P2P facilitent la distribution massive de copies parfaites et gratuites de contenus numériques. Il serait difficile de nier que cette capacité soit la raison principale à la base du succès universel de ces dispositifs ; pourtant, comme soulignent quelques auteurs interdisciplinaires entre le droit et l'informatique (par exemple Niva Elkin-Koren et Barbara van Schewick) leur signification politique et technique serait à chercher ailleurs, dans un ensemble de propriétés qui tiennent à la fois du technique, du social, de l'économique et du légal.

La capacité de ces systèmes à tirer avantage de leur architecture décentralisée peut donner lieu, en effet, à une meilleure efficacité économique, une plus grande liberté et à l'émergence

de nouveaux principes organisationnels et légaux, rendus possibles par l'échange direct de contenus entre les différents nœuds du réseau. Une architecture décentralisée peut augmenter le niveau de liberté personnelle car il devient plus facilement possible pour les utilisateurs de rester anonymes et de protéger leur *privacy* : il n'est plus nécessaire de s'enregistrer en tant qu'utilisateurs d'un serveur particulier, mais il est possible de se « déplacer » entre réseaux *ad-hoc*. Par ailleurs, une plus grande protection de l'anonymat peut dans certains contextes être « libératrice », en ouvrant plus de possibilités de développement de différents aspects de son identité, rendant plus facile l'expression de préférences authentiques, et facilitant par conséquent la formation d'un environnement plus participatif pour tester de nouvelles idées. Outre que dans la nature et l'étendue des libertés personnelles, la décentralisation des réseaux informatiques peut faciliter les processus de décision alternatifs, en augmentant notamment la capacité à favoriser l'exclusion des intermédiaires, le tout dans des contextes qui incluent, certes, mais qui dépassent amplement, le partage de contenus numériques protégés : par exemple, la démocratie directe, le débat public et la recherche de consensus.

MYTHE N° 2 :
LE PEER-TO-PEER, C'EST DU PARTAGE DE FICHIERS

Tout comme le peer-to-peer est devenu la « technologie des pirates », il est souvent considéré comme la technologie « du partage de fichiers », le plus souvent protégés par le droit d'auteur. Cependant, cette technologie de réseau ne sert pas seulement au partage de fichiers : elle a certes été, au cours de ses premiers pas, reléguée à ce seul domaine, ce qui constitue l'option technique la plus facile et nécessitant un minimum de ressources humaines et techniques pour sa réalisation – mais le P2P est aussi exploité, et ce de plus en plus, pour des applications « alternatives » et « légales », qui peuvent servir plus d'une nécessité des usagers/consommateurs/citoyens d'aujourd'hui, et qui se proposent en tant qu'alternatives décentralisées à des services et instruments aujourd'hui fondamentaux de notre vie quotidienne : moteurs de recherche, réseaux sociaux, stockage de fichiers en ligne. Cela se doit non seulement aux évolutions technologiques à large échelle (qualité des connexions Internet, espace disque à disposition sur chaque ordinateur), mais aussi à la prise de conscience (soit par les chercheurs, soit par le public) de l'existence d'une *« écologie Internet »* de plus en plus délicate et articulée.

Avec *Google*, *Facebook* ou encore *Picasa*, à chaque fois qu'un usager exécute une recherche, échange un message avec quelqu'un ou met un album photo en ligne pour le montrer à ses amis, des données sont envoyées et téléchargées à des serveurs avant de rejoindre leur destinataire prévu, contribuant à constituer le scénario de « concentration » de contenus dont on a parlé ci-dessus. En revanche, mettant à profit le potentiel décentralisateur du P2P, ces autres applications récentes visent à répondre aux mêmes exigences du point de vue de l'utilisateur final (qui continuera donc à rechercher des mots, à former des réseaux d'amis et à partager des photos), mais en se basant sur une architecture technique différente. Ce qui a des implications à plusieurs niveaux : meilleures performances techniques, certes, mais aussi possibilité de reconsidérer des concepts tels que la sécurité et la *privacy*, en reconfigurant les emplacements des données et des échanges, les frontières entre l'usager et le réseau, la prise en compte des outils qu'on a à disposition : en somme, l'attribution, reconnaissance et modification de droits entre utilisateurs et fournisseurs des services.

Parmi les exemples les plus intéressants de ces applications pionnières, on retrouve bien sûr les services de voix sur IP qui ont chamboulé le marché traditionnel de la téléphonie ; mais

aussi des applications moins connues, de stockage et accès distribué de fichiers privés ; de moteur de recherche P2P, qui se fonde sur la détection des préférences personnelles et des affinités entre les usagers ; de streaming vidéo ; de messagerie ; de réseautage social.

MYTHE N° 3 :
LE TRAFIC EN PEER-TO-PEER EST EN BAISSE PUISQUE LE TRAFIC EN STREAMING AUGMENTE

Nombre d'études constatent dans les dernières deux ou trois années « une baisse des échanges peer-to-peer face à la montée du streaming », notamment vers les sites de streaming et de téléchargements direct, comme RapidShare ou Megaupload. Si cela est certes indicatif d'une tendance de certaines pratiques de consommation numérique à se déplacer vers d'autres arènes – notamment à cause de mesures juridiques visant des technologies plutôt que des usages – mettre en corrélation directe la baisse du P2P et la hausse « du streaming », comporte, encore une fois, des imprécisions et une confusion entre les usages et les infrastructures qui les supportent. En effet, si le streaming vidéo correspond dans l'imaginaire d'une très grande majorité d'utilisateurs à des solutions centralisées proposées par des grandes plateformes, de YouTube et DailyMotion à nombre de sites au statut légal plus douteux, le streaming vidéo en P2P est déjà largement utilisé, et plusieurs projets de recherche étudient actuellement les moyens d'améliorer sa qualité de service. Ce système est plus particulièrement à l'œuvre dans le domaine du P2PTV.

Les applications P2PTV sont destinées à redistribuer des flux (streams) vidéo en temps réel sur un réseau P2P ; les flux vidéo distribués sont généralement des chaînes de télévision, mais peuvent aussi provenir d'autres sources. Le potentiel de ces applications est qu'elles peuvent rendre toute chaîne de télévision disponible au niveau mondial par toute personne alimentant ce flux au sein du réseau ; chaque pair qui rejoint le réseau pour voir la vidéo contribue au visionnage des autres pairs/téléspectateurs, permettant un passage à l'échelle du système au fur et à mesure que le public augmente, sans coût supplémentaire pour la source du flux vidéo.

Dans un système de P2PTV, chaque utilisateur, quand il télécharge un flux vidéo, est simultanément en train de permettre aux autres utilisateurs de télécharger ce flux, contribuant ainsi à la bande passante totale disponible. Les flux qui arrivent sont typiquement en retard de quelques minutes par rapport aux sources originales. La qualité vidéo des canaux dépend généralement du nombre d'utilisateurs qui sont en train de les regarder ; la qualité vidéo est meilleure s'il y a plus d'utilisateurs. Un système de diffusion en P2PTV est généralement beaucoup moins cher que les alternatives, et peut être initié au niveau individuel. En revanche, il pose des problèmes de qualité de service si comparé à l'unicasting (l'architecture client-serveur généralement utilisée dans le streaming) puisque personne ne peut garantir une source fiable, chaque utilisateur étant aussi un réémetteur.

MYTHE N° 4 :
LE PEER-TO-PEER, C'EST DU LOGICIEL LIBRE ET/OU DE L'OPEN SOURCE

Comme les autres « mythes » présentés dans ce chapitre, l'idée que le peer-to-peer et le logiciel libre ou open source coïncident dérive d'un ensemble de conceptions et de facteurs qui tiennent à la fois du « politique », de l'économique, du social, mêlant des arguments établis à des idées reçues. Beaucoup d'outils en peer-to-peer, en particulier les premiers grands systèmes de partage de fichiers, sont effectivement nés au sein des communautés de logiciel libre et de l'open source et en ont, à leur tour, facilité le développement et

l'organisation, dans une démarche éthique commune de partage de ressources, de gestion consensuelle et sans centre, d'attribution d'importance au choix et à la liberté de l'utilisateur. Pourtant, un nombre important d'applications, sous-tendant une technologie P2P et servant des usages variés, sont à ce jour partiellement ou complètement propriétaires.

Comme a souligné en 2000 le développeur Dave Winer, *« The P in P2P is People »* : c'est-à-dire, ce qui est important dans les réseaux peer-to-peer, ce sont les gens. Ce commentaire souligne en quoi la connexion entre le développement d'applications peer-to-peer et le mouvement open source est significatif : les projets open source s'organisent autour de groupes de travail décentralisés, qui s'autogèrent et sont eux-mêmes rendus possibles par des technologies Internet en peer-to-peer. Si la P dans P2P est celle de « People » - note Tim O'Reilly - soit les technologies permettant aux gens de créer des communautés qui s'auto-organisent, soit les cadres organisationnels développés afin de gérer ces communautés, donnent d'importantes leçons pour ceux qui veulent travailler dans l'espace P2P.

L'open source n'est pas tout simplement déterminé par un ensemble de licences pour la distribution des logiciels, mais, à un niveau plus profond, par un ensemble de techniques pour un développement de logiciels collaboratif et global. C'est là que, en effet, que la boucle entre l'open source et le peer-to-peer se voit bouclée, comme avait déjà montré un des moteurs de la première communauté open source, Usenet : un système qui, sans contrôle central, copie des fichiers entre ordinateurs, et dans lequel chaque site participant au réseau sauvegarde ses copies des messages postés dans les forums, et se synchronise périodiquement avec ses pairs. Les « labels » open source et peer-to-peer indiquent donc tous les deux, généralement, des technologies ou des communautés permettant aux gens de s'associer librement, de manière directe, et sont souvent parmi les incubateurs d'innovation les plus prometteurs.

Ces similitudes, pourtant, ne devraient pas emmener à traiter le peer-to-peer et l'open source comme étant tout à fait coïncidents, ce que montrent plusieurs cas récents. Un désormais célèbre service de voix sur IP implémente une architecture P2P basée sur un protocole propriétaire. A côté de nombreux avantages, liés à la connexion directe et au partage de ressources de bande passante entre utilisateurs, le « mariage » entre P2P et propriétaire à l'œuvre dans ce logiciel a cependant donné lieu à une importante controverse quant au manque d'interopérabilité du système avec d'autres systèmes, P2P et non.

Une start-up proposant un moteur de recherche P2P qui vise une « distribution totale » de la recherche en ligne ne publie pas, quant à elle, son produit comme open source. Elle considère que le modèle open source est parfait lorsqu'on compète au moyen d'un avantage de coût avec un produit commercial au même niveau technologique, comme c'est le cas avec les systèmes d'exploitation Linux ou le logiciel de traitement de texte OpenOffice, mais que ce modèle n'est pas une bonne idée quand on possède un avantage technologique par rapport à un monopole, comme ce serait le cas pour un moteur de recherche P2P par rapport au « géant » Google, et on doit se confronter à un service fourni de façon gratuite, soutenu par un « pouvoir de marque » très puissant.

Une entreprise développant une application pour le stockage et l'accès distribué de fichiers privés, reposant à la fois sur une plateforme de serveurs et sur une approche d'architecture distribuée et décentralisée, où le fonctionnement du dispositif repose sur la mise à disposition de ressources *hardware* de la part des usagers, revendique quant à elle un statut de dispositif hybride P2P. Cependant, celui-ci est aussi un logiciel propriétaire, car son code source est fermé, même si les projets universitaires sur lesquels le logiciel se fonde sont

partiellement, à l'origine, de l'open source, et leur contribution reconnue sur le site de l'entreprise.

MYTHE N° 5 :
LE PEER-TO-PEER PRIVE, C'EST DU « DARKNET », DE L'« INTERNET ILLEGAL »

A la fin de 2002, quatre ingénieurs faisant partie du groupe de recherche sur la sécurité de Microsoft créèrent le terme « darknet », dans un papier très influent pour la suite, appelé *« The Darknet and the Future of Content Distribution »,* pour se référer à l'Internet « souterrain ». On était alors dans l'environnement d'après-Napster et d'avant-Gnutella. Les ingénieurs définirent dans ce papier le darknet en tant que « collection de réseaux et de technologies utilisées pour partager du contenu numérique ». Suivant le papier, le mot a infiltré les médias généralistes, et a été utilisé pour se référer à une variété d'activités et technologies « clandestines » sur l'Internet. Entre 2003 et 2005, le terme « darknet » a été utilisé comme étiquette d'une quantité d'activités à l'allure menaçante et incertaine, de « cyberclubs » privés, à bases de données en ligne mais puissamment sécurisées et non-traçables avec les moteurs de recherche grand public, ou encore, au monde du cybercrime et du spam, et les autres « endroits obscurs » de l'Internet utilisés pour échapper à la loi.

En même temps, le mot a été utilisé pour distinguer les réseaux distribués anonymes et privés de leurs prédécesseurs « publics ». L'élément de *privacy* a été introduit pour la première fois dans un travail juridique en 2004 ; le darknet y est défini comme la collection de réseaux et autres technologies qui permettent aux personnes de partager matériaux numériques « sans peur d'être découverts ». J. D. Lasica décrit ailleurs le darknet comme un réseau de personnes qui utilisent des espaces fermés – des ports francs, à la fois virtuels et réels, où il n'y a que peu ou pas de possibilité d'être découverts – pour partager du matériel numérique avec des autres, afin d'éviter les restrictions sur les médias numériques imposés par les compagnies du monde du divertissement. Il en résulte une superposition des darknet et des réseaux P2P privés dans une vision de supermarché de médias numériques avec une mentalité de *« wild west »*, qui pourrait rivaliser les produits et services fournis par les grandes industries du contenu avec les armes de la *privacy*, de l'invisibilité même. L'ambigüité entre le peer-to-peer privé et le réseautage Internet illégal et souterrain s'est donc vue renforcée.

Pourtant, le peer-to-peer « privé » ne se limite pas aux darknet. Au delà de la connotation d'illégalité qu'ils peuvent avoir assumé, la caractéristique principale de ces réseaux est leur statut de systèmes de connexion « friend-to-friend », à signifier que des connexions directes sont établies seulement entre des amis reconnus. Plus généralement, tout réseau de partage de fichiers privé peut être défini comme un réseau, ou un ensemble de réseaux, distribué et décentralisé (sans index central) qui inclut des fonctions de privacy, sécurité (encryptage), et anonymat de l'usager, qui a le but primaire de partager de l'information avec des membres certifiés du réseau.

Une des entreprises proposant un service de P2P privé souligne que ce système permet d'apporter une « solution nouvelle à un problème classique », mieux que d'autres solutions existantes : les services de stockage en ligne sont limités au niveau de l'espace disponible et nécessitent la recopie des fichiers chez un tiers ; les services d'envoi de fichier ne conviennent pas pour partager des dossiers complets ; le FTP demande des connaissances techniques pointues ; les plateformes de streaming ne sont pas adaptées pour les échanges privés et les solutions de P2P existantes ne sont pas assez sécurisées.

Comme explique Fabrice Le Fessant, dans des connexions peer-to-peer privées, ami-à-ami, chaque usager héberge sa page personnelle sur son ordinateur, avec, en particulier, toute

information ou donnée qu'il considère personnelle. Il autorise ses amis, un par un, à accéder à son ordinateur. A cette fin, il envoie à chaque ami une clé secrète, qui sera utilisée par l'ami lors de sa première connexion au moyen de l'application P2P. Au moment de cette première connexion, un nouveau « secret » est échangé, et sera utilisé pour toutes les connexions suivantes. La première clé secrète n'est pas réutilisable, en évitant ainsi toute interception par une troisième personne ou entité.

Ce mécanisme d'identification et de distribution de contenus est actuellement utilisé dans nombre d'applications pour le partage de données et d'informations personnelles, en permettant un accès plus rapide aux contenus (puisque ceux-ci sont directement disponibles sur l'ordinateur de l'usager, sans besoin de le recopier sur un site), tout en les rendant accessibles seulement à des amis utilisant le même programme.

MYTHE N° 6 :
LA DIFFUSION DU CLOUD COMPUTING SIGNIFIE LA MORT DU PEER-TO-PEER

Bien que la définition même de *Cloud* soit actuellement l'objet de vives controverses (une revue spécialisée a récemment réuni plus de vingt définitions différentes du concept), ce modèle indique généralement que le vendeur fournit l'infrastructure physique et le produit logiciel, abritant ainsi à la fois les applications et les données dans un lieu inconnu de l'utilisateur (le fameux « nuage », ***Cloud*** en anglais) et interagit avec ce dernier grâce à une interface client. On s'achemine dans ce cas vers un modèle de déportation et de virtualisation sur des serveurs distants de traitements informatiques traditionnellement localisés sur le poste utilisateur. Eben Moglen, professeur à Columbia University et inspirateur du réseau social décentralisé Diaspora, a récemment affirmé que, dans un paysage de services internet dominé par le paradigme client-serveur, ce qui est actuellement rangé sous l'étiquette de la tendance ***Cloud Computing*** n'est rien d'autre que « des serveurs qui ont gagné [davantage de] liberté. Liberté de bouger. Liberté de louvoyer ; de combiner et de diviser, de ré-agréger et d'utiliser toute sorte d'astuces. Les serveurs ont gagné en liberté. Les clients n'ont rien gagné ».

Dans ces conditions - alors qu'un modèle économique et technique dans lequel l'utilisateur final sollicite de puissants centres de serveurs, qui stockent l'information et gèrent le trafic sur le réseau - certains soutiennent que un « P2P turn », tel qu'on l'a décrit dans les sections précédentes, pourrait ne plus être possible. Certes, il s'agit là d'une tendance inverse à celle proposée avec le modèle P2P, qui vise à (re-)placer l'utilisateur et sa machine au centre de la création, du partage, de la gestion de contenus numériques. Toutefois, le nuage décentralisé ou P2P est aussi envisageable. En fait, les premières expérimentations avec le nuage décentralisé sont déjà à l'œuvre, et seraient conçues pour répartir la puissance de calcul et les ressources du nuage entre les terminaux de tous les utilisateurs/contributeurs, avec l'idée que la liberté de l'utilisateur au sein du 'nuage' et la possibilité pour lui de contrôler entièrement, et par ses propres moyens, ses données personnelles, ne sont pas des buts incompatibles entre eux.

MYTHES ET LEGENDES DE LA VIDEOCONFERENCE

Jean-Denis Garo, Aastra

La vidéo redevient un sujet d'actualité pour les DSI et les DG. Il est vrai que l'offre s'est diversifiée : des solutions gratuites sur PC, aux solutions intégrées dans les solutions de communications unifiées, aux nouveaux terminaux dédiés, sans oublier les salles de téléprésence. Toutefois subsistent autour de ces solutions un certain nombre de mythes.

MYTHE N° 1 :
LA VIDEOCONFERENCE EST RESERVEE AUX GRANDES ENTREPRISES

L'usage de la vidéo au sein des entreprises est plus que jamais une réalité. Il persiste néanmoins un décalage entre les attentes des utilisateurs, les messages marketing des acteurs spécialisés, et la mise en œuvre réelle de ces solutions. Réservées auparavant à certaines catégories d'utilisateurs dans l'entreprise les solutions tendent aujourd'hui à se généraliser à la plupart des utilisateurs de l'entreprise. La vidéo est de plus en plus considérée comme une extension du système de communications et d'informations (SI), et donc comme un média complémentaire à la voix et la data.

La vidéoconférence se démocratise, elle répond à de nouvelles attentes, et prend de nouvelles formes. En effet les solutions historiques de vidéoconférence (salles dédiées) répondent généralement à des besoins de réunions longues, programmées, privilégiant la parole (à l'écrit), dans des salles dédiées, offrant parfois l'apparence d'une réunion virtuelle (téléprésence, co-présence physique).

Désormais plus facilement utilisables, les solutions de vidéoconférence peuvent aussi être initiées depuis un PC portable (favorisant le nomadisme ou le télétravail), et bientôt à partir d'un téléviseur, d'une tablette numérique, ou même d'un Smartphone. Les solutions de vidéoconférence sur PC sont, elles, plus utilisées pour des réunions impromptues, où le partage de document prendra rapidement le pas sur la fenêtre vidéo. Souvent utilisées pour un suivi de projet (follow up) elles sont, du fait de leurs coûts réduits, plus accessibles aux PME. L'appropriation de ces nouveaux modes de communication a profité de l'usage banalisé des applications Skype ou MSN par le grand public. Ils sont aujourd'hui également relayés par d'autres solutions de vidéoconférence comme les Webconférences.

L'émergence de terminaux dédiés à la vidéo et à certaines applications offre une troisième voie. Celle du confort et de la convivialité d'un terminal vidéo HD, utilisable directement sur le poste de travail individuel ou en salle de réunion, permettant de poursuivre le partage de documents sur le PC, mais surtout offrant une simplicité d'usage telle qu'elle révolutionne les comportements utilisateurs. Il n'est ainsi pas interdit de penser que demain les appels voix dans l'entreprise seront naturellement remplacés par des appels vidéos, de la même manière que les messages vocaux ou les messages d'attentes, d'accueil deviendront des messages vidéos. …

Le besoin crée donc toujours la solution, l'ensemble des solutions de vidéoconférence s'interconnectent / inter-opèrent pour répondre aux nouveaux usages de la mobilité et aussi aux budgets des entreprises.

MYTHE N° 2 :
LA VIDEOCONFERENCE NECESSITE DES INVESTISSEMENTS COUTEUX.

Depuis 2005 et la version beta de Skype qui introduisit la vidéo sur les ordinateurs familiaux, il n'est plus possible de tenir cette position. On nous opposera que ce type de solutions est plutôt réservé à un usage grand public, notamment du fait de failles de sécurité révélées ces dernières années. Reste que cette solution est répandue dans nombre de PME . L'affirmation des coûts ne touche plus les solutions dédiées aux entreprises. Les grands acteurs historiques des salles de conférences ont en effet vue croître un certain nombre d'acteurs proposant des solutions logicielles sur PC, et offrant des garanties en terme de sécurité, mais sans être capables pour autant d'offrir la qualité HD souvent attendue par les entreprises pour les relations externes. Pour combler cette lacune, d'autres acteurs proposent depuis le début 2001 de porter des solutions de vidéoconférence sur des équipements dédiés HD, qu'il s'agisse de terminaux multimédia ou de tablettes. Le positionnement de ces offres se situe le plus souvent un peu au-dessus du prix d'un ordinateur portable haut de gamme.

Concernant le déploiement, l'émergence de protocoles comme SIP (Session Iniation protocol) facilite et simplifie tant l'administration que le temps dévolu à l'installation, engendrant des économies immédiates. En outre les interfaces tactiles et intuitives remisent les nombreuses télécommandes aux solutions du passé, et permettent de réduire significativement les coûts de formation et d'utilisation généralement induits par ce type d'outil.

MYTHE N° 3 :
LA VIDEOCONFERENCE EST RESERVEE AUX EXECUTIFS

Au-delà des impacts techniques et financiers amenés par la mise en place d'une solution vidéo IP dans une entreprise, on constate que la vidéo ne concerne souvent que certaines catégories de personnels et de groupes de travail. Le secteur d'activité de l'entreprise est aussi un élément très segmentant. Ce résultat n'est pas une surprise, dans la mesure où les entreprises recherchent de moins en moins à mettre en œuvre des solutions ponctuelles mais plutôt à faire de la vidéo une application clé de leur système d'information. Les entreprises sont au milieu du gué sur ce type de projet, partagées entre leur volonté de généralisation de ce type de projets et les difficultés technologiques et économiques qui président à intégrer complètement la vidéo dans le système d'information

Le coût n'étant plus un frein à l'utilisation, la démocratisation est en marche et de nouveaux usages apparaissent. Des entreprises commencent d'ailleurs à se servir des Terminaux Multimédias HD comme elles utilisent un vidéoprojecteur. Elles le réservent pour une réunion dans une salle qui n'en serait pas encore équipée. Les télétravailleurs sont aussi équipés….

MYTHE N° 4 :
LA VIDEO C'EST JUSTE POUR LES SALLES DE CONFERENCE

La vidéo aujourd'hui est omniprésente. Sur son téléphone mobile, sa console de jeux, sur une tablette, sur son PC, sur un terminal multimédia, dans une salle de conférence, sur une borne interactive, sur le portier de son immeuble, et prochainement sur la télévision, ou dans les lunettes. La vidéo devient un média simple, facile à déployer, intuitif et attendu : là ou nous prenions des photos, nous réalisons des minis films que l'on s'empresse de partager quelque soit le support. Dans les années à venir, la pression des usages grand public et le

consumérisme des solutions technologiques feront qu'il deviendra rapidement indispensable de se voir aussi bien dans l'environnement entreprise, que dans l'environnement privé. Et ce besoin sera récurrent, quel que soit l'environnement existant : à son bureau ou en salle de réunion, en déplacement professionnel ou en situation de télétravail. A ce titre, la salle de conférence ne deviendra qu'un des environnements possibles.

MYTHE N° 5 :
LA VIDEO EST UNE SOLUTION TOTALEMENT SEPAREE

Une solution vidéo est considérée comme une extension du système de communication, et donc comme un média complémentaire à la voix et la data. Les entreprises restent encore attentives et prudentes à considérer la vidéo comme une application bureautique généralisée, sachant qu'elle nécessite une infrastructure système et réseau beaucoup plus rigoureuse. La tentation de déployer des solutions autonomes et indépendantes du SI de l'entreprise est donc grande.

Cependant, le simple fait que la vidéo soit de plus en plus considérée comme une extension du système de communication démontre sa place importante au sein même des processus métiers de l'entreprise. En conséquence, il devient aujourd'hui impensable que les solutions traditionnelles isolées (solutions traditionnelles de vidéoconférence reposant sur la technologie TDM) ne soient pas progressivement remplacées par des solutions vidéo capables de s'imbriquer presque nativement dans le SI et donc de contribuer à la productivité des directions métiers de l'entreprise.

MYTHE N° 6 :
LA VIDEO EST IMPERSONNELLE ET RETIRE LA VALEUR ATTACHEE A UN VRAI FACE A FACE

Rien ne remplace une rencontre, mais pour la suite, la qualité des solutions (voix, image) apportent le non corporel nécessaire, et enrichissent particulièrement la communication. En ajoutant l'image à la voix, la vidéo donne à la communication une dimension complémentaire dans laquelle la gestuelle et les comportements viennent enrichir le contenu oral : la communication vidéo est une bonne illustration d'un fait bien connu des professionnels de la communication, pour lesquels la signification d'un message passe autant par son contenant que par son contenu.

CONCLUSION

La vidéo est en passe de devenir un média aussi important et naturel que le mail ou le téléphone.

Dans une étude récente, les utilisateurs considèrent que la vidéo ne doit pas être cantonnée aux salles de conférences dédiées ou à une simple utilisation depuis un PC : si 30% des personnes interrogées estiment que la vidéo doit être utilisée uniquement pour les réunions, 45% considèrent aussi la vidéo comme un moyen naturel pour enrichir les communications interpersonnelles au sein de l'entreprise. Vraisemblablement vers un usage « à la volée ».

Plusieurs facteurs expliquent ce regain d'intérêt et ce nouveau regard sur la vidéo :

D'une part, les crises économiques de ces dernières années, conjuguées aux différents risques de catastrophes naturelles et pandémiques, ont contraint les entreprises à trouver des solutions pour préserver leur compétitivité (réduction des coûts et d'optimisation des

dépenses) et la productivité de leurs employés ; et cela tout en renforçant leurs démarches de développement durable.

D'autre part, la vidéo a atteint une maturité technologique qui la place comme un média incontournable pour apporter de la valeur et améliorer la collaboration entre les équipes et les salariés. Ces derniers, éduqués pas les solutions grand public, ont trouvé dans les solutions professionnelles les garanties de sécurité et de qualité nécessaires à leur activité professionnelle.

Au final, c'est à la fin du paradigme que nous assistons : celui selon lequel les terminaux dédiés à la téléphonie et la vidéo seront totalement remplacés par les PC et les logiciels de web et vidéoconférence. Les utilisateurs se sont vite vus confrontés aux problèmes de performances des PC : disponibilité, ergonomie, etc.… Le choix d'un terminal n'est plus tant dicté par le contenu qu'il pourra relayer, que par l'environnement dans lequel il sera utilisé.

2° PARTIE : ASPECTS SECURITE ET SURETE

MYTHES ET LEGENDES DES APT

Nicolas RUFF – EADS Innovation Works

Pour commencer, précisons immédiatement qu'APT signifie "*Advanced Persistent Threats*", soit "attaques complexes et récurrentes" dans une traduction approximative. Il s'agit d'un *buzzword* qui (si ma mémoire est bonne) a été inventé autour de 2008 par la société MANDIANT[1], en réponse aux incidents de sécurité de plus en plus nombreux et de plus en plus graves rapportés par la presse à cette époque.

Il est difficile de définir plus précisément le terme APT. Pour paraphraser l'expert en sécurité Cesar Cerrudo: "Lorsqu'une petite entreprise est piratée, elle est victime de ses lacunes en sécurité. Lorsqu'une grande entreprise est piratée, elle est victime d'une APT".

La confusion est également alimentée par les vendeurs de produits de sécurité, qui prennent le train en marche et rajoutent une couche de marketing-fiction avec des noms futuristes tels que: opération "Titan Rain", opération "Aurora", opération "Ghost Net", opération "Night Dragon", opération "Shady RAT", et autres "*Advanced Evasion Threats*".

On notera toutefois que les entreprises piratées étaient quasiment toutes équipées avec la plupart des solutions de sécurité du marché. Et que les vendeurs de ces solutions apparaissent également sur la liste des victimes …

MYTHE N° 1 : LES APT NE ME CONCERNENT PAS

C'est l'idée fausse la plus répandue: seules les institutions politiques, les systèmes militaires et les centres de recherche des grandes multinationales occidentales seraient visés.

Or l'actualité nous démontre tout le contraire:

Une petite entreprise peut être ciblée, car elle dispose d'un savoir-faire ou d'une technologie unique en son genre.

Une entreprise commerciale quelconque peut être visée, car elle est sous-traitante d'une cible plus intéressante. C'est le cas de la société RSA, qui fournit des solutions de sécurité à Lockheed Martin[2] (et de nombreux autres industriels). La pratique anarchique de l'externalisation multiplie le nombre de vecteurs d'entrée.

Une cible intéressante, mais difficile à pénétrer "en direct", peut être compromise par le biais d'une filiale de moindre importance. En effet, le niveau d'isolation et de surveillance entre réseaux internes est souvent bien moindre qu'avec Internet. Google suspecte fortement sa filiale chinoise d'être à l'origine de la compromission détectée en janvier 2010[3].

Même une organisation à but non lucratif peut être victime. Ce fût le cas par exemple de plusieurs agences anti-dopage[4], ou d'association de défense des droits de l'homme au Tibet[5].

[1] http://www.mandiant.com/services/advanced_persistent_threat/
[2] http://www.nytimes.com/2011/05/30/business/30hack.html?_r=1
[3] http://fr.wikipedia.org/wiki/Op%C3%A9ration_Aurora
[4] http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

MYTHE N° 2 :
LES APT FONT APPEL A DES COMPETENCES TECHNIQUES HORS DU COMMUN

C'est aussi une idée fausse, bien souvent propagée par les victimes pour se défausser de leurs responsabilités.

Mon analyse de plusieurs dizaines de cas réels démontre que:

- Les attaquants recyclent du code écrit par d'autres, parfois même sans le comprendre.
- Les attaquants utilisent des outils librement téléchargeables sur Internet (tels que la *backdoor* Poison Ivy[6] ou la suite d'outils Pass-The-Hash[7]).
- Les codes d'attaque sont souvent bogués.
- Les attaquants se propagent sur les réseaux internes en utilisant des techniques simples, tels que des mots de passe par défaut ou triviaux.

Patrick Pailloux, directeur général de l'ANSSI, a rappelé récemment[8] que la plupart des cas d'intrusions dans lesquels ses services sont intervenus découlaient d'une hygiène informatique déplorable, malgré une apparente maitrise (telles que les certifications ISO 2700x, ITIL, CMMI, et consorts).

Il existe quelques points durs dans les intrusions, comme la découverte et l'exploitation de failles "0day"[9]. Mais pour 1 attaquant qui dispose d'une telle faille, il en existe 10 (ou 100) qui copient son code sans même le comprendre. Les codes les plus populaires sont rapidement disponibles dans le projet libre et gratuit Metasploit[10], ce qui facilite leur dissémination.

Il est évident que toute stratégie de défense contre les intrusions doit prendre en compte la présence de failles dans les logiciels: entre les failles restant à découvrir, celles qu'on peut déjà acheter sur le marché gris, et celles pour lesquelles le correctif n'a pas été déployé sur l'intégralité du parc informatique …

MYTHE N° 3 :
ON PEUT SE PROTEGER EFFICACEMENT CONTRE LES APT :

Bien entendu, chaque vendeur de solution de sécurité va vous promettre (mais pas vous garantir) que son produit vous protège contre "100% des attaques connues et inconnues".

Mais bien entendu, les attaquants achètent les mêmes produits et savent comment les mettre en défaut.

Compte-tenu du flot ininterrompu d'attaques diverses et variées (dont les APT) qui arrivent chaque jour dans vos boites aux lettres et dans vos navigateurs, il est illusoire de croire qu'aucun poste de travail ne sera jamais compromis chez vous. StuxNet (mais avant lui

---

http://www.franceinfo.fr/faits-divers-justice/floyd-landis-condamne-pour-piratage-informatique-d-un-laboratoire-antidopage-442981-2011-11-10

[5] *http://fr.wikipedia.org/wiki/GhostNet*

[6] *http://www.poisonivy-rat.com/*

[7] *http://oss.coresecurity.com/projects/pshtoolkit.htm*

[8] *http://www.ssi.gouv.fr/fr/anssi/publications/communiques-de-presse/cloture_les_assises_de_la_securite_et_des_systemes_d_information_2011.html*

[9] *Faille logicielle inconnue de l'éditeur, et a fortiori pour laquelle aucun correctif n'est disponible.*

[10] *http://metasploit.com/*

Conficker) ont démontré que même les réseaux déconnectés d'Internet pouvaient être attaqués …

La plupart des entreprises disposent aujourd'hui d'une protection "à l'état de l'art": antivirus, pare-feu, proxy filtrant, utilisateurs non administrateurs de leurs postes de travail, politique de mots de passe robuste …

A contrario, rares sont les entreprises qui disposent d'une politique de *détection* et de *réaction* adaptée à l'état de la menace … Ce sont aujourd'hui deux axes d'amélioration majeurs sur lesquels il faut investir.

Il n'est pas question de stéganographie ou de canaux cachés improbables. La plupart des APT se soldent par l'envoi de fichiers de plusieurs gigaoctets, le samedi soir, vers des serveurs situés à l'étranger … Comment une telle anomalie peut-elle échapper à la vigilance de tous les produits de sécurité, et des humains chargés de les faire fonctionner ?

Malheureusement, la plupart des intrusions sont détectées "par hasard", suite à un problème d'apparence banale: saturation de l'espace disque sur un serveur, lenteur de la connexion Internet …

Et lorsque le problème est détecté, reste à savoir quoi faire … Qui contacter ? Faut-il débrancher le serveur ou le laisser actif ? Quel est l'étendue des dégâts ? Comment repartir dans un état sain ? Les premières réactions sont souvent improvisées et catastrophiques: par exemple effacer toutes les traces de l'attaquant …

MYTHE N° 4 : L'ATTRIBUTION DES ATTAQUES EST IMPOSSIBLE SUR INTERNET

Il est vrai que la nature pervasive d'Internet permet de masquer efficacement ses traces, pour peu qu'on s'en donne la peine. Il est parfois possible de remonter jusqu'à une adresse IP ou une machine. Mais il reste impossible de savoir qui était au clavier lors de l'attaque …

Toutefois cette assertion doit être relativisée dans le cas d'une APT. En effet, une attaque longue et récurrente va forcément laisser beaucoup plus de traces qu'une défiguration unitaire de site Web ou l'envoi d'un spam. Parmi tous les indices qu'on peut collecter, on peut citer:

1. Les motifs de connexion discernables.

   En analysant les horaires de connexion des attaquants sur une période suffisamment longue, il est possible d'identifier plusieurs informations utiles, telles que le fuseau horaire ou les fêtes nationales. Bien entendu cette information peut être falsifiée si tous les attaquants se mettent d'accord pour agir les jours fériés à 3h du matin … mais les informations obtenues actuellement par cette méthode sont cohérentes avec les autres sources d'informations.

2. Les sources des outils utilisés.

   Il existe souvent de nombreux outils capables de réaliser la même tâche: par exemple il existe un nombre considérable de *backdoors* librement disponibles sur Internet. L'attaquant va privilégier les outils dont la documentation est rédigée en anglais … ou dans sa langue maternelle.

3. Les traces involontaires.

   L'outil de compilation d'un programme ou de génération d'un document va laisser de nombreuses traces à l'insu de l'utilisateur.

   Dans le cas de StuxNet, la présence de la chaine "myrtus" a fait gloser de nombreux

observateurs. S'agit-il d'une référence biblique, ou faut-il lire "My RTUs" (*Real Time Unit*) ? La question reste ouverte.

Mais dans d'autres cas, les traces involontaires sont beaucoup plus faciles à interpréter: par exemple la langue par défaut de l'interface graphique, ou le nom d'utilisateur de l'attaquant …

4. Le mobile de l'intrusion.

   Indépendamment des aspects techniques, on peut noter que le nombre de personnes susceptibles d'être intéressées par des informations sur les négociations du G20 ou la construction de réacteurs nucléaires se compte sur les doigts d'une main. Contrairement à des numéros de CB volés, de telles informations sont difficilement exploitables sur le marché gris … Ce qui fait dire à certains que les APT sont le fait d'états et non de criminels.

Il existe quelques cas où il a été possible d'approcher de très près la source de l'attaque. Lors de l'opération "Aurora", Google a nommément désigné une source chinoise[11]. Il semble que les équipes sécurité de Google aient contre-attaqué et remonté le fil rouge jusqu'à la source de l'intrusion, bien que cela n'apparaisse qu'en filigrane dans leur communiqué officiel. Il est également arrivé qu'un serveur de rebond sous le contrôle direct de l'attaquant ait été saisi (cas de l'opération "Shady RAT").

MYTHE N° 5 : LA SECURITE INFORMATIQUE A 100% N'EXISTE PAS

Ceci est l'un des mythes les plus destructeurs qu'on puisse entendre.

Il est vrai que le risque zéro n'existe pas. Mais cette assertion sert bien souvent à justifier des arbitrages totalement absurdes tels que: "… donc je garde mon iPhone et je fais suivre tout mon mail professionnel sur GMail" !

"La sécurité à 100% n'existe pas" sert bien souvent de prétexte pour faire une sécurité à 10%.

L'information est comme un fluide: si votre plomberie est à 99% étanche … alors vous avez déjà un sérieux problème de fuite !

Il est impossible d'empêcher les attaques d'arriver, ni d'appliquer les correctifs de sécurité sur l'intégralité d'un parc informatique hétérogène et étendu. Mais il est possible de faire beaucoup mieux qu'actuellement, grâce aux leviers de la détection et de la réaction évoqués précédemment:

- Une attaque détectée et éradiquée en 1 heure n'a aucun impact sérieux.
- Une attaque détectée et éradiquée en 1 journée nécessitera une analyse post-mortem pour déterminer l'étendue de la compromission.
- Une attaque détectée et éradiquée en 1 semaine laissera le temps à l'attaquant de collecter suffisamment de mots de passe et de poser suffisamment de *backdoors* pour pouvoir revenir à volonté …

P.S. Les attaques les plus longues documentées dans la nature ont officiellement duré … 3 ans.

[11] http://www.theregister.co.uk/2010/02/19/aurora_china_probe_latest/

MYTHES ET LEGENDES DE L'ANALYSE DE RISQUE

Louis Derathé, Thales

MYTHE N° 1 : LES CRITERES TRADITIONELS DE CONFIDENTIALITE, INTEGRITE ET DISPONIBILITE DES INFORMATIONS SONT INSUFFISANTS !

Depuis de très nombreuses années, la sécurité d'une information est appréciée à l'aune de trois critères[12] : la Confidentialité, l'Intégrité et la Disponibilité (la fameuse triade C I D).

Longtemps ces critères ont paru suffisants pour conduire à l'élaboration de politiques de sécurité techniques et organisationnelles dans les systèmes informations, permettant de protéger ces informations de toutes les attaques … enfin, autant que cela était possible !

Mais, les Nouvelles Technologies de l'Information et de la Communication et leur cortège de cyber attaques ont bousculé les certitudes et entaché de doute cette caractérisation ; de nombreux critères sont apparus comme pouvant compléter cette caractérisation « sécurité» des informations et mieux répondre à la menace ambiante : de nombreux gourous ont donc complété la liste proposant en guise de critère, aussi bien des fonctions de sécurité que de sûreté, arguant que tout est dans tout et la sécurité partout.

Certes, la communauté de la SSI su faire la part des choses et rejeter l'ivraie, mais une suggestion récurrente engage encore aujourd'hui un vrai questionnement : **Est-ce que l'authenticité d'une information peut être un critère de sécurité ?**

En effet, une information authentique, c'est-à-dire vraie, ne peut pas nuire à la sécurité d'un système d'information … et donc, cette qualité devrait être, à l'évidence, protégée ! La confiance, la véracité, la conviction ou la preuve sont des valeurs partagées sur lesquelles une sécurité devrait ce construire ; voilà l'évidence qui nous aveugle soudain !

Et voilà surtout l'analyste sécurité plongé dans les affres du doute et de la crainte de l'incomplétude … de la faille logique de sa démarche d'analyse !

Si l'on se réfère aux définitions couramment offertes par nos dictionnaires, « authenticité » se décline selon deux approches complémentaires : *ce qui est conforme à la vérité, ce dont l'exactitude ne peut être contestée* (Larousse).

Poursuivons notre analyse ! Deux concepts constitutifs de cette notion d'authenticité apparaissent donc : la vérité et sa preuve.

Nous conviendrons sans hésiter que la vérité, en soi, n'est pas une qualité relevant de la sécurité puisqu'elle procède plus de la foi ou de la confiance (du point de vue plus centré sur les systèmes d'information, elle relève des utilisateurs du SI ; c'est une qualité relevant de la source de l'information comme par exemple pour les systèmes de Renseignement et ses logiques de cotation).

Mais l'exactitude, la preuve ! Voilà qui fleure bon la sécurité, non ?

Récapitulons, ce ne serait donc pas l'authenticité en soi, mais bien sa composante preuve/démonstration qui serait alors un nouveau critère sécurité de l'information.

[12] *Cf. la méthode EBIOS*

Or, quelques mots d'un certain Jacques Stern[13], trouvés sur le web, éclairent notre réflexion :

« *Un service d'authenticité garantit l'identité d'une entité donnée ou l'origine d'une communication ou d'un fichier. Lorsqu'il s'agit d'un fichier, et que l'entité qui l'a créé est la seule à avoir pu apporter la garantie d'authenticité, on parle de « non-répudiation ». Ce service de non-répudiation est réalisé par une signature numérique, qui a une valeur juridique depuis la loi du 20 mars 2000*»

…. « Signature numérique » ! Le mot est dit … car, qu'est-ce qu'une signature, sinon effectivement un élément permettant à un émetteur de garantir l'intégrité et la provenance d'une information ?

L'authenticité ne serait donc finalement, du point de vue sécurité, que l'intégrité d'une information associée à l'identité de son émetteur … ce que l'on traduit plus communément dans le langage technique : preuve d'origine ! Et nous voilà à nouveau revenus aux trois critères immémoriaux.

Vite un autre critère ! Un autre gourou !

MYTHE N° 2 : MAITRISER LE RISQUE INFORMATIONNEL AU NIVEAU D'UN ORGANISME (HYPERVISION), C'EST POUR DEMAIN !

Même si les méthodes comme EBIOS 2010 et les travaux actuels regroupés sous le terme « d'hypervision[14] » visent à intégrer dans l'analyse du risque, les aspects « métiers » de l'entreprise (en particulier au travers des modalités d'expression des événements redoutés pour la première), la déclinaison d'évènements redoutés en risques, traduits par des scénarios de menaces sur des biens supports, valorisés par des facteurs de gravité ou vraisemblance, ne se convertit pas facilement en états gradués d'occurrence des évènements redoutés : nous restons à un stade d'appréciation de la probabilité/vraisemblance d'occurrence des risques sur le système informatique et non à celui du degré d'imminence de ces mêmes risques dans une appréhension globale de l'organisme.

Quelles sont les qualités nécessaires d'une véritable hypervision, une maîtrise du risque au niveau de l'organisme ?

TOUT D'ABORD, UNE ANALYSE DE RISQUE FONDEE SUR LES MISSIONS DE L'ORGANISME

Lorsqu'on parle d'analyse de risque, on pense naturellement à la méthode préconisée par l'ANSSI : EBIOS. Dans le cadre d'une homologation de système d'information, cette méthode, au même titre que PILAR pour l'OTAN, vise à guider l'analyste dans l'expression des besoins de sécurité du système d'information.

Longtemps utilisée dans une optique d'analyse systématique de toutes les vulnérabilités d'un système d'information, la méthode EBIOS dans sa nouvelle version 2010 introduit une nouveauté dans le cadre de l'analyse de risque : elle vise à cerner les principaux enjeux de cette sécurité au travers de l'expression « d'Évènements Redoutés » au niveau fonctionnel de

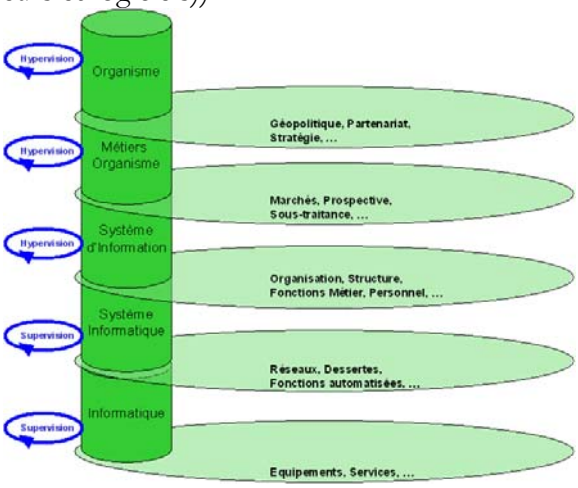
[13] *Directeur du Laboratoire d'informatique de l'École normale supérieure*

[14] *Ces travaux visent à mettre en œuvre une supervision dynamique étendue à plusieurs systèmes d'information et intégrant des analyses selon les couches classiques : système information - système d'information – organisme ; la prise en compte de la dimension « métier » du risque est sa caractéristique actuelle ; plus qu'une méta-supervision, c'est une supervision au niveau de l'entreprise qui est recherchée.*

l'organisme ; l'analyse de risque qui en découle est donc fortement orientée par les missions de l'Organisme.

Bien entendu, il n'est pas envisageable de traduire directement des évènements redoutés relatifs aux missions d'un organisme en événements informatiques à surveiller, il faut bien décliner ces besoins primordiaux selon les 5 couches du système informationnel de l'organisme qui supportent ces missions :

- Une couche basse composée des architectures techniques informatiques (équipements, services)
- Support de celle supérieure du système informatique au sens de l'outil de traitement (réseaux, dessertes, grandes fonctions (serveurs et logiciels))
- Lui-même, composant principal du système d'information (fonctions supportées essentiellement par l'informatique, mais englobant aussi toute l'organisation de ses métiers comme les approvisionnements, l'organisation et la structure, la sélection du personnel, etc.)
- Au service des métiers de l'organisme (vision opérationnelle par grande fonction de l'organisme)
- Caractérisant l'Organisme dans toutes ses dépendances.



Ainsi, faut-il à l'évidence décliner l'analyse de risque, telle une poupée russe, selon ces couches dont les objectifs de sécurité sont de nature et d'expression différentes.

Le niveau supérieur exprime donc les évènements redoutés de l'organisme, imagine les scénarii qui peuvent conduire à ces évènements, les apprécie et exprime ainsi les risques encourus. Puis, en cascade, les niveaux subalternes prennent alors en tant qu'évènements redoutés de leur analyse, les risques du niveau supérieur et ceci jusqu'aux composants informatiques.

Cette analyse de risque en cascade présente deux caractéristiques très particulières rarement formalisées : si les évènements traduisant l'occurrence de risques sont uniquement techniques et de valeur souvent binaire (ON/OFF) aux plus bas niveaux, plus on monte dans les couches, plus ceux-ci quittent la technique pour englober des domaines plus larges comme la politique, le personnel, la stratégie, l'environnement, les pressions externes, etc. De plus, plus on monte dans ces couches, plus les évènements à relever et les capteurs associés sont externes à l'organisme.

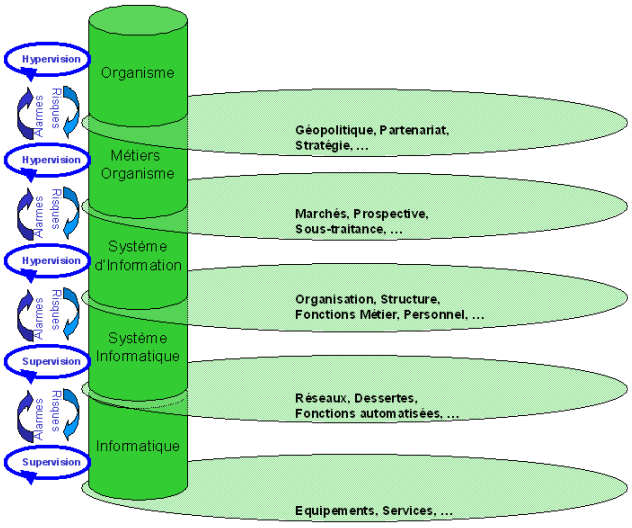
ENSUITE UN FLUX TRANSPOSE DE LA SUPERVISION VERS L'HYPERVISION

Si l'on considère que l'objet de l'hypervision est bien de détecter, mesurer et répondre aux atteintes subies par l'organisme, la surveillance devrait naturellement s'appliquer à ce que redoutent les acteurs de l'organisme ; les éléments surveillés devraient donc permettre de détecter l'occurrence des risques conduisant à l'ensemble des évènements redoutés qui ont été déterminés lors de l'analyse présentée ci-dessus.

Cette surveillance devrait donc s'effectuer par niveau, et chaque alarme (risque échu) devrait remonter au niveau supérieur en tant qu'événement où elle serait prise en compte et corrélée

avec les événements de ce niveau ; les événements devraient donc remonter par bulles successives de la supervision telle qu'on la connaît jusque l'hypervision :

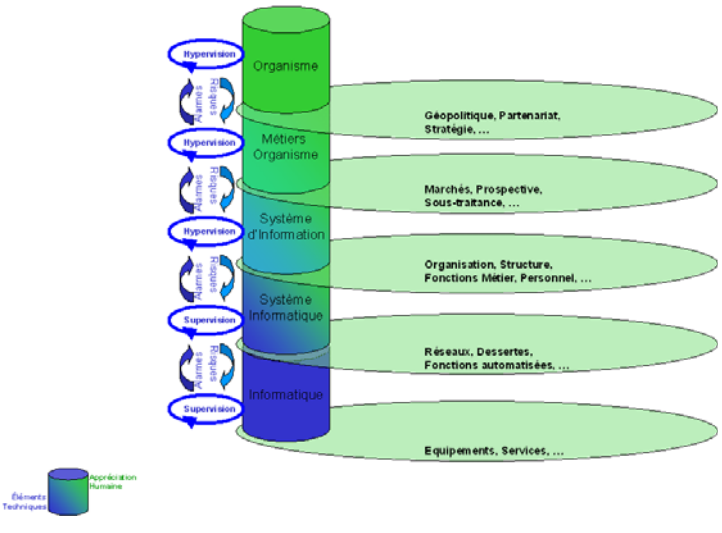
- Les évènements informatiques vers le niveau système informatique lorsqu'ils constituent un risque pour ce dernier
- Les risques du niveau système informatique vers le niveau système d'information lorsque corrélés avec des évènements relatifs aux architectures, dessertes, personnel informaticien, méthodes du service ou Politique de sécurité informatique
- Puis vers le niveau métier lorsque corrélés avec les aspects de distribution du système, de partage d'information ou de dépendance informationnelle
- Vers le niveau organismes lorsque confortés avec des évènements relatifs aux marchés, la concurrence, à l'évolution des pratiques ou de l'état de l'art (intervention de l'Intelligence économique)
- Où enfin pourraient être analysées les conséquences de ces risques pour l'organisme en rapport avec la géopolitique, les groupes de pression, l'image ou l'espionnage



PASSER DE L'OBSERVATION D'ETATS A L'APPRECIATION D'UNE SITUATION

Si l'on veut atteindre un niveau d'appréciation de la sécurité d'un organisme, il faut obtenir une représentation de l'état de cette sécurité en référence aux événements redoutés de plus haut niveau et donc représenter non seulement des faits (panne d'un composant, dysfonctionnement d'une fonction) mais des renseignements, c'est à dire une analyse de ces faits ou d'états potentiels traduits en connaissance d'un état futur.

Ainsi, si au niveau informatique, les événements peuvent se traduire en état O/N, puis au niveau système informatique en probabilité selon des arbres d'attaque, autant dès le niveau Système d'information l'appréciation d'un événement relève d'une analyse plus complexe et généralement humaine (est-ce ou non un facteur de risque ? Est-ce que l'impact est direct ? Est-ce que l'on peut y répondre autrement ? Doit-on réorienter nos capteurs ?) et sa représentation (alarme/alerte) doit s'exprimer autrement : plus intuitive, plus proche d'une traduction en logique floue de type important, critiques, etc.



QUITTER L'INSTANTANE POUR LE CONTINU

Avoir la capacité d'apprécier une situation à un instant précis est indéniablement intéressant, mais s'attendre à ce que le système de surveillance et d'analyse, une fois défini et mis en œuvre, présente de lui-même un état toujours actualisé serait une erreur. Deux impératifs conduisent à faire évoluer ce système :

- L'évolution naturelle des menaces, en écho aux évolutions dans le monde de l'information (capacités, vulnérabilités) qui conduisent à une nouvelle expression des scénarios de risque, voire à un changement des priorités de l'organisme
- L'avancement d'une atteinte à l'organisme, conduisant à des adaptations du périmètre de surveillance (limitation des connexions, cloisonnement des sites) ou un renforcement des réponses avec de nouveaux indicateurs (ex : mise en œuvre d'une journalisation certifiées ou extension des éléments observés).

Ainsi, non seulement les capacités du système d'observation doivent être dynamiques, mais son mode de fonctionnement aussi.

Si l'on en revient à l'expression d'événements redoutés, dont on dit qu'elle devrait conduire la LID et ici l'hypervision, on peut affirmer de même qu'elle est influencée en retour par cette hypervision ; en effet, cette expression doit traduire :

- les nouvelles priorités de l'organisme,

l'évolution, l'apparition ou disparition de métiers

l'inclusion de SI ou les externalisations

Les failles découvertes

Les attaques réalisées

C'est donc bien un cycle en boucle continue « objectifs de sécurité - hypervision » qui doit être mis en action.

Et si l'on projette ce cycle sur les différents niveaux cités plus haut c'est en réalité une accumulation de cycles imbriqués qu'il faut animer :

- Cycle d'évolution/maintenance du système informatique au travers de l'état de l'art
- Cycle de correction/évolution du système d'information au travers du MCS
- Cycle d'orientation de la LID pour ce qui concerne les fonctions/missions de l'organisme
- Cycle de définition d'un plan de maîtrise de l'information (en référence avec les concepts de guerre de l'information) pour une réelle hypervision.

AVOIR UNE VISION PROSPECTIVE

Cet état de fait amène les constatations et déductions complémentaires suivantes :

- Si l'analyse automatisée du risque ne peut viser actuellement à prédire/prévenir l'occurrence d'un événement redouté mais tente seulement de représenter la possibilité que cet événement advienne, les réponses du niveau hypervision ne peuvent en conséquence être automatisées ;

- Si l'on vise à composer une équipe d'hypervision, celle-ci devrait être composée de tous les acteurs de l'organisme pour traduire la gravité des impacts[15] (l'arrêt d'une fonction peut être considéré comme *négligeable* par la direction de l'organisme du point de vue de l'inertie de son fonctionnement et des impacts sur la production, mais *grave* pour les personnes en charge de réaliser cette fonction, du point de vue des emplois, de la survie de la sous-traitance, etc.) et selon le modèle de la gestion de crise (Décision, conduite, communication, conseil) pour répondre efficacement et durablement à l'avènement des risques ;
- Si l'on envisage une hypervision, la surveillance ainsi que démontré plus avant, doit prendre en compte les évènements de niveau « système » d'un organisme (grèves, changements de politique de l'entreprise, concurrence, géopolitique, etc.), et inclure les interactions et dépendances extérieures de l'organisme ; bien évidemment, une telle surveillance implique dès le niveau système d'information, de nouveaux capteurs (ex : cellule I.E.) et indicateurs puisqu'il faut prendre en compte des sources externes (réseaux personnels, analyse par cabinets).

CONCLUSION

En conclusion, si l'on veut une véritable « hypervision », il faut largement dépasser le paradigme actuel de l'informatique et concevoir cette supervision améliorée, étendue, dans une appréhension systémique de l'organisme, couvrant toutes ses facettes et dépendances internes et externes, et selon l'éclairage du concept de guerre de l'information : son avènement n'est pas a priori pour demain.

[15] *Voir à ce sujet de l'évaluation du risque, l'excellent article de Rey Senjen et Steffen Foss Hansen « Towards a nanorisk appraisal framework » présenté dans les « Comptes-rendus de l'Académie des Sciences » de septembre 2011 (ISSN 1631-0705)*

MYTHES ET LEGENDES DE LA GUERRE DANS LE CYBERESPACE

Gérard Peliks, Cassidian Cyber Security

D'abord définissons ce qu'on entend par guerre dans le cyber espace ou cyberguerre. Si on sépare les acteurs entre organismes d'état et organismes privés et si on sépare les domaines d'action entre sécurité nationale et économie, la cyberguerre est menée par les organismes d'état, et leurs intermédiaires, et inquiète la sécurité nationale du pays attaqué.

A l'autre bout du spectre, quand des organismes privés, ou des individus autonomes, s'en prennent à l'économie d'un pays ou aux avoirs d'un particulier, on parle de cybercriminalité. Les deux autres espaces, cyber espionnage (état, économie) et cyber terrorisme (organismes privés, sécurité nationale) sont évidemment très proches de la cyberguerre et présentent avec elle, une surface de recouvrement non négligeable.

On entend dire que la troisième guerre mondiale sera une cyberguerre avec une quasi certitude qu'elle se produira dans les années qui viennent. On dit que les bits et les électrons vont remplacer les missiles et les arbalètes. Détrompez-vous ! La cyberguerre n'a pas obligation d'être mondiale et elle a déjà commencé depuis plusieurs années.

Que ce soit, en citant des faits qui ont été particulièrement médiatisés :

- Estonie en 2007 où les botnets ont constitué une arme de perturbation massive ;
- guerre entre la Russie et la Géorgie en 2008 qui a commencé par l'attaque des réseaux de communication ;
- attaque cybernétique de l'usine d'enrichissement d'uranium de Natanz, en Iran, en 2010 où le ver Stuxnet était dans les centrifugeuses ;
- cyber guéguerre entre Marocains et Algériens en 2011 où c'est à qui défigurera le plus de sites Web officiels de l'autre pays en y injectant des messages politiques ;

la cyberguerre n'est pas, loin de là, qu'une vue de l'esprit dans les pensées de quelques experts de la sécurité de l'information. Elle se concrétise dans la réalité, elle sévit autour de vous.

Des pays s'y préparent. Citons Gordon Brown qui fut premier ministre britannique : "*Tout comme au 19eme siècle nous avons eu à sécuriser les mers pour la défense de notre pays et sa prospérité, qu'au 20eme siècle ce furent les cieux qu'il fallut rendre plus sûrs, au 21eme siècle nous prenons place désormais dans le cyber espace*".

Voilà le décor planté, mais que de mythes et légendes accompagnent déjà aujourd'hui la cyberguerre

MYTHE N° 1 : UNE CYBERGUERRE NE FAIT QUE DES CYBER MORTS

Allez demander aux Géorgiens, durant l'attaque des Russes en Ossétie du Sud en 2008, s'ils n'ont pas eu de victimes humaines bien réelles, pas des morts d'avatars ou autres constructions cybernétiques ! Et ces victimes auraient sans doute pu être évitées si les systèmes de télécommunication, de transferts d'information et de commandements de la Géorgie avaient fonctionné correctement.

Bien sûr, on n'occupe pas un terrain avec des data qui transitent par les réseaux et s'introduisent dans un système d'information. Mais une guerre moderne commencera par paralyser un pays ; et plus le pays sera dépendant de ses systèmes d'information et de ses réseaux de données, plus vite le chaos s'installera et la panique gagnera la population attaquée. Et le pays tombera sous le joug de l'assaillant comme un fruit mur.

Du chaos et de la panique qui résulteraient (je pourrais sans doute tout aussi bien écrire "qui résulteront" de la cyber attaque préalable, on pourra aussi compter nombre de victimes (et là je n'écrits pas de "cyber victimes").

MYTHE N° 2 : MON ORGANISATION N'EST PAS CONNECTEE A I'INTERNET, ELLE N'A RIEN A CRAINDRE

Comment existe-t-elle alors, votre organisation, dans cette quatrième dimension que constitue le cybermonde, là où de plus en plus d'administrés se rencontrent et où se nouent des relations privilégiées entre les entreprises, leurs partenaires, leurs fournisseurs et leurs clients ?

Mais la question n'est pas là, vous pensez être protégés parce que vous n'êtes pas connectés ? L'usine d'enrichissement d'uranium de Natanz en Iran, site sensible par excellence car le programme nucléaire iranien dépend de sa bonne marche, vous vous en doutez, n'était bien entendu pas connectée à l'Internet. Et pourtant elle a fait l'objet, en 2010 d'une attaque perpétrée par un maliciel très sophistiqué venu d'ailleurs, le ver Stuxnet.

Tout est nominal sur les écrans de la salle de contrôle des centrifugeuses de l'usine de Natanz. Elles tournent à vitesse constante. Un ver, appelé depuis Stuxnet, est introduit au moyen d'une clé USB infectée. Rapidement l'infection se propage sur les ordinateurs sous Windows connectés au réseau interne de l'usine, puis se répand sur les PLC (automates programmables) de Siemens que ces ordinateurs contrôlent. Ces composants Siemens assurent des vitesses de rotation des centrifugeuses nominales et constantes. Ce sont précisément ces contrôleurs que cherche et trouve le ver Stuxnet avant de libérer sa charge létale. Les vitesses de rotation des centrifugeuses, désormais sous contrôle du ver Stuxnet, deviennent alors hors de contrôle de la centrale. Les centrifugeuses accélèrent, décélèrent, leurs axes de rotation vibrent, l'ensemble chauffe. Pendant ce temps, les écrans de la salle de contrôle disent que "tout va bien", car le ver envoie également des informations rassurantes vers les capteurs. La situation réelle est devenue catastrophique. L'attaque n'est pas venue de l'Internet mais le résultat final a été le même.

Connectés ou pas connectés, si vous avez des informations numériques, elles sont en danger. Si vous gérez des infrastructures sensibles de type SCADA, même non connectées, elles peuvent être infectées par un maliciel venant d'une clé USB, comme ce fut le cas pour Stuxnet, ou par un transfert direct par disque dur comme ce fut le cas pour le Pentagone.

MYTHE N° 3 : JE TRAVAILLE DANS LE DOMAINE DE LA SANTE, JE NE SUIS DONC PAS CONCERNE

Noble secteur que celui de la santé, mais ultra sensible !

Que veulent les cyber agresseurs quand ils attaquent à des fins terroristes ? : Provoquer le chaos en causant une panique généralisée. Quoi de mieux que de s'en prendre aux hôpitaux, aux ambulances ? Les hôpitaux sont équipés de nombreux systèmes commandés par l'informatique qui sont autant de cibles intéressantes. On prend le contrôle des respirateurs,

de la climatisation : panique assurée, cela en parallèle bien sûr avec l'arrêt de la distribution d'électricité, l'empoisonnement de l'eau, la paralysie des transports.

Non, dans une cyberguerre, le secteur de la santé ne sera pas un havre de paix, bien au contraire.

MYTHE N° 4 :
SI ON M'ATTAQUE, JE RIPOSTE PLUS FORT ET L'ATTAQUE S'ARRETE

Si c'est de la légitime défense et si votre riposte n'est pas exagérée par rapport à l'attaque, l'opinion publique ne vous le reprochera pas. Mais au juste, contre qui allez-vous riposter ? Contre une adresse IP qui s'avèrera être celle d'un adolescent d'Europe de l'est ? Contre un pays dont les ordinateurs ont transmis l'attaque à l'insu de leur plein grés, parce que contaminés par des bots, et qui ne savent pas du reste que leurs ordinateurs sont devenus des "zombies" ? Contre la Chine parce que dans l'écosystème de l'insécurité, ce sont toujours les Chinois qui sont les méchants ?

Après avoir déplacé une statue érigée à la gloire du soldat soviétique durant la deuxième guerre mondiale, l'Estonie a été attaquée en déni de service distribué, simultanément par une cinquantaine de pays, peut être aussi par votre ordinateur. L'agresseur a utilisé un réseau de botnet pour déclencher une tempête numérique qui a bloqué les serveurs de plusieurs administrations estoniennes, pendant plusieurs jours.

Contre qui l'Estonie aurait du riposter ? Contre les cinquante pays d'où sont venues les attaques, alors qu'elles ne faisaient que transiter par les ordinateurs infectés de ces pays ? Contre la Russie parce que visiblement, c'était à elle que profitait le crime ? Et si c'était une attaque juste initialisée par un groupe de hackers russes échappant à tout contrôle ?

Oui, décidemment il n'est pas facile de reconnaître qui est son adversaire dans le cybermonde, et si on se trompe, non seulement on n'arrête pas l'attaque mais on accumule ses ennemis.

MYTHE N° 5 :
DANS UNE CYBERGUERRE, NOUS SORTIRONS VAINQUEURS

Parce que nous sommes les plus forts ?

Si Sun Tzu, auteur, dans la Chine antique, de l'art de la guerre avait vécu à notre époque, il aurait sans doute écrit que la seule façon de gagner une cyberguerre était de l'éviter. Plus un pays est connecté, donc à priori plus il est fort, plus il est vulnérable. Dans une cyberguerre opposant un pays tel que les Etats-Unis et un pays tel que le Rwanda, à votre avis, qui pourrait faire le plus de mal aux systèmes d'information de l'autre ?

La guerre dans le cyberespace est assurément une guerre asymétrique. Il convient de s'y préparer et de connaître ses adversaires potentiels.

ACRONYMES

PLC : Programmable Logic Contoller

SCADA : Supervisory Control and Data Acquisition

GLOSSAIRE

POUR ALLER PLUS LOIN DANS LA CONNAISSANCE DES TIC

Les contributeurs de cet ouvrage collectif ont également écrit, ou participé à l'écriture de livres dans leurs domaines d'expertises. Voici, sans être objectif, loin s'en faut, quelques uns de ces livres qui peuvent vous permettre d'aller plus loin dans la connaissance des TIC.

.

Jean-Denis Garo

Auteur de :

- « Mon papa travaille dans l'Informatique et les Télécoms » - 2007
- « Anita & Béatrix – Le sens caché du vocabulaire des IT » - 2010

Co-Auteur des livres collectifs :

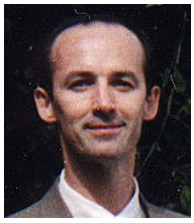
- « Sécurité des Systèmes d'Information » Les Guides ECOTER, Edition Mission Ecoter – 2002
- « Guide TIC des petites et moyennes collectivités », Edition Ficome – 2004
- « La sécurité à l'usage des décideurs ». Edition etna France- 2005
- « La sécurité à l'usage des PME et des TPE », Edition Ténor – 2006
- « La Sécurité à l'usage des collectivités locales et territoriales », Edition Forum ATENA- 2009
- « Lexique des TIC », Edition Forum ATENA – 2010
- « L'Internet à l'usage ....de l'écosystème numérique de demain », Edition Forum ATENA - 2011

Responsable éditorial de :

- « L'Off-Shore et les centres de contacts Cap sur l'île Maurice », Edition 1Angle2Vues - 2007

A PROPOS DES AUTEURS

Par ordre alphabétique :



Louis DERATHE présente une expérience de plus de 15 ans en SSI, successivement informaticien, responsable de l'organisation d'une Cie d'Assurance, consultant en Système d'Information, officier en charge de SSI et maintenant expert SSI à THALES. Il est à ce sujet l'auteur d'un roman sur la guerre de l'information « Opération ACCAPARE » Ed l'Harmattan (et bientôt d'un autre sur la Métacommunication) *Louis.DERATHE (at) thalesgroup.com*

Jean-Denis GARO, Directeur Communication et Marketing Support d'Aastra, est Titulaire d'un DEA Science et Technologie du CSTS, complétant un DUE à la Faculté de droit de Bordeaux et une école de Commerce dans la même ville.

Il a effectué sa carrière dans les IT, Matra Communication, Nortel Networks, EADS Telecom et Aastra. Administrateur du Forum ATENA, il est auteur de plusieurs ouvrages spécialisés. Il intervient dans les domaines touchant à l'évolution des usages dans les centres de contacts, les communications unifiées et collaboratives, la téléphonie IP, les solutions de vidéoconférence et les réseaux sociaux d'entreprises. *jgaro(at) aastra.com*

Francesca MUSIANI est ingénieur de recherche ARMINES, attachée de recherche et doctorante au Centre de sociologie de l'innovation (CSI) de MINES ParisTech (UMR 7185 CNRS) et enseigne à l'Université Pierre et Marie Curie. Diplômée en communication des organisations (Université de Padoue, Italie) et en droit international (Université pour la Paix des Nations Unies), elle participe actuellement au projet ANR ADAM et rédige sa thèse sur la technologie P2P appliquée aux services Internet.

Francesca est l'auteur de plusieurs articles sur les pratiques "alternatives" du P2P, publiés dans Terminal, Observatorio et tripleC, et de Cyberhandshakes: How the Internet Challenges Dispute Resolution (...And Simplifies It), publié en 2009 par EuroEditions grâce à une bourse de publication de la European Foundation for the Information Society. *francesca.musiani (at)* ***mines-paristech.fr***

Gérard PELIKS est expert sécurité dans le Cassidian Cyber Security Il préside l'atelier sécurité de l'association Forum ATENA, participe à la commission sécurité des systèmes d'Information de l'AFNOR et anime les Lundi de l'IE, pour les aspects sécurité de l'information dans le cadre du Cercle d'Intelligence Économique du Medef Ile de France. 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*

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