

| | |
|----------------------------------------------------|----|
| EDITO | |
| AGENDA | |
| ACTUALITES | P2 |
| VEILLE | P3 |
| Protection technique des œuvres numériques | |
| ZOOM | P4 |
| Téléphonie et Voix sur IP (ToIP & VoIP) | |
| L'ESSENTIEL | P8 |
| Focus sur Le Correspondant Informatique et Liberté | |

EDITORIAL

Noël approche, les listes au Père Noël s'étoffent peu à peu. De plus en plus d'internautes, pour la plupart encore novice dans le domaine, effectuent leurs courses en ligne. Ils deviennent des proies idéales pour les pirates au travers d'attaques et d'escroqueries en tous genre. Le phishing en est l'exemple le plus flagrant. Le nombre d'attaques est en constante augmentation : rien que pour 2006 on estime les pertes à environ 2,8 milliards d'euros envers les consommateurs.

Une idée de cadeau pour les amateurs de rugby ? L'ouverture de la vente de billet a débuté en ce début de mois pour la coupe du monde en 2007 : que ce soit au guichet, par téléphone ou encore en ligne tous les moyens sont mis à disposition afin que vous puissiez acheter votre place. Pour un tel événement il faut que les moyens techniques puissent faire face à la demande. D'après les nouvelles sur la première journée, face au nombre important de connexions simultanées et malgré une saturation constatée à l'ouverture, les équipements ont tenu le cap (plus de 60 000 billets ont été vendus dès la première heure).

Il est important d'assurer une qualité de service et de pouvoir estimer la charge que devra supporter une infrastructure et cela passe par la sécurisation de son ensemble. Ainsi, les transactions financières et la disponibilité des moyens de paiements sont des enjeux sensibles voir critiques. D'une panne peuvent découler d'importants préjudices financiers ; une faille potentielle sur le système ou les applications peut faire naître des envies auprès de personnes mal intentionnées et avoir des conséquences financières non négligeables.

Parallèlement à cette problématique les entreprises et les particuliers doivent veiller à ne pas porter atteinte aux droits d'auteurs des œuvres numériques sur Internet. En effet ces œuvres numériques sont protégées et la responsabilité civile ou pénale peut être engagée avec potentiellement des demandes de dommages et intérêts importants. Notre article sur la protection des œuvres numériques apportera plus de visibilité à ce sujet.

Les 7 et 8 novembre 2006 s'est déroulée la convention sur la VoIP et ToIP. Les personnes qui se sont rendues à cet événement trouveront sans doute un complément d'information dans notre rubrique « **ZOOM** » du mois. Pas de soucis pour celles qui n'y sont pas allées, elles y découvriront aussi une très bonne source d'information. N'hésitez pas à consulter notre sélection pour la fin d'année 2006, dans notre agenda.

AGENDA - Sélection Fin d'année 2006

⇒ **TELECOM WORLD 2006 - Hong Kong -Chine, Du 4 au 8 décembre 2006**

Hong Kong accueille la plus grande manifestation mondiale des Télécommunications, sur le thème « LIVING THE DIGITAL WORLD ». Tous les plus grands partenaires du monde des télécommunications y participeront et y présenteront les nouvelles technologies de demain.

Plus d'infos : <http://www.itu.int/WORLD2006/>

⇒ **Les logiciels libres (Open Source) - Angers, 5 décembre 2006**

Face à l'émergence des logiciels libres, les entreprises y sont de plus en plus sensibles. Le CRITT organise une demi-journée technique sur le thème des Logiciels Libres (Open Source).

Plus d'infos : <http://www.meito.com/fr/>

⇒ **Salon Mobile Office - Paris, du 5 au 7 décembre 2006**

Les solutions mobiles sont des enjeux stratégiques pour de nombreuses d'entreprises. Au travers de ce salon elles pourront y trouver toute l'information nécessaire (présentations, conférences ou ateliers).

Plus d'infos : <http://www.mobileoffice.fr/>

⇒ **Conférence sur la « sécurité Informatique » - Granville, Mardi 12 Décembre 2006**

L'ENSICAEN organise une conférence sur la sécurité informatique et sa problématique.

Plus d'infos : <http://www.granville.cci.fr/>

Directeur de la publication :
Edouard Jeanson

Agence ESEC
Sogeti Infrastructures Services
6-8 rue Duret
75016 Paris - France
Tél : 33 (0)1 58 44 55 66

Société par Actions Simplifiée au
capital de 15 999 790 euros
RCS Paris 479 942 583

ACTUALITES

La sécurité des claviers virtuels contestés

Une étude récemment publiée sur l'efficacité des claviers virtuels a révélé la conclusion suivante : ils ne serviraient à rien face aux parasites actuels qui interceptent l'information lors de sa transmission au formulaire et non durant la saisie.

Le principe, de plus en plus adopté par les banques, est donc de cliquer avec la souris sur des touches virtuelles affichées dans un ordre aléatoire à l'écran.

Cependant, si cette technique protège bien des keyloggers (interception de la frappe au clavier), elle n'est nullement efficace face à certains codes malicieux (Haxdoor) qui interceptent les données lorsqu'elles sont transmises au formulaire.

En effet, une fois collectée par le clavier virtuel, l'information doit être transmise à l'organisme bancaire, ce qui se fait via une simple requête de formulaire (POST en langage HTML) facilement intercepté.

Des solutions sont à l'étude aussi bien coté serveur que coté client. Les banques pourraient investir dans la sécurisation des accès distants de leurs clients au travers d'authentification forte mais qui pourrait au final devenir très contraignantes pour l'utilisateur.

Pour l'instant, rien n'est envisagé pour renforcer la sécurité en France.

Pour en savoir plus :

<http://www.lesnouvelles.net/articles/attaques/847-claviers-virtuels-exploites.html>



Piratage d'une centrale aux USA

Les pirates ne se contentent plus de cibler les entreprises en s'attaquant aux serveurs de mails, aux serveurs web ou aux stations de travail. Désormais ils s'orientent vers les équipements industriels gérés par informatique.

Ainsi aux Etats-Unis, un pirate s'est introduit sur l'ordinateur portable d'un employé d'une centrale de traitement des eaux. Il a utilisé l'accès à distance comme point d'entrée et a mis en place un virus et un logiciel espion ou spyware sur le réseau de l'usine.

Selon les faits remontés, il n'aurait pas

tenté de prendre le contrôle global du système, mais de l'utiliser à son propre bénéfice pour y déposer et distribuer des emails et des logiciels piratés. D'après le FBI, cela aurait tout de même pu entraîner une interruption de service.

Ce n'est pas la première fois que ce genre d'événement se produit : lors d'une des attaques précédentes, les pirates avaient lancé une attaque de déni de service sur une centrale hydraulique, fait une intrusion au cœur du système de contrôle et d'acquisition des données d'une centrale d'épuration, et laissé des messages en guise de signature de leur passage..

Selon le WaterISAC (organisme qui fournit une solution de sécurité orientée métier améliorée, avec système d'alerte 24/7 et accès à des experts spécialisés dans le domaine de la cyber sécurité appliquée aux risques et enjeux des métiers de l'eau), il a été constaté une augmentation croissante des rapports sur les piratages de ce type depuis le 11 septembre 2001, et l'on peut envisager une extension au monde entier.

Pour en savoir plus :

<http://www.generation-nt.com/actualites/20505/cyber-attaque-terrorisme-centrale-traitement-eaux-fbi-usa>



La sécurité des échanges

De nos jours les internautes ont confiance dans la sécurisation des données, mais une nouvelle pourrait bouleverser cette sérénité.

En effet le cryptologue allemand Jean-Pierre Seifert et son équipe, révèlent une faille pouvant menacer l'intégrité de données numériques. Il serait possible en quelques millisecondes de récupérer la quasi-totalité d'une clé de cryptage de 512 bits.

C'est le mode de fonctionnement même de la puce, optimisé pour accélérer les calculs, ce qui le rend vulnérable. Il suffit de mesurer le temps de calcul du processeur pour en déduire la chaîne de cryptage.

Cette menace porte le nom « d'analyse de prédiction de branche » (BPA). Difficile à appliquer en temps normal, l'équipe de chercheurs a réussi le traitement du premier coup.

Connaissant la persévérance et la dextérité des pirates, on peut supposer qu'à terme un simple logiciel espion pourrait « écouter » une puce et en exploiter la clé à mauvais escient.

Ce scénario est encore loin de voir le jour. Les conditions dans lesquelles les tests ont été réalisés (en laboratoire) ne permettent pas d'annoncer la fin du e-commerce.

En effet, les résultats donnent une clé non finalisée de 508/512 bits, certes c'est énorme mais incomplet. De plus les essais pour trouver la bonne fréquence de décryptage n'ont pas été comptabilisés.

Cependant l'équipe de J.P Seifert soulève une problématique autour des techniques de BPA qui mérite d'être approfondie.

Pour en savoir plus :

<http://www.spyworld-actu.com/spip.php?article3028>

<http://sid.rstack.org/blog/index.php/2006/11/22/152-la-fin-du-monde#co>



VEILLE TECHNOLOGIQUE

⇒ Protection technique des œuvres numériques

📁 Introduction

Concomitamment à l'apparition d'Internet, un phénomène de piratage des œuvres numériques est apparu avec une ampleur sans précédent. Selon l'IIPA^[1], on évalue à environ 11 milliards de dollars^[2] le manque à gagner pour les industries de contenus, et selon une étude du cabinet Deloitte^[3], à 17 milliards de dollars. Cette fourchette, de pertes financières, peut être comparée au chiffre d'affaires 2004 du groupe « Danone » (13,7 milliards d'euros, soit 18,221 milliards de \$)^[4]. Le progrès en matière de compression numérique, l'émergence des réseaux P2P^[5], et le développement des connections Internet à haut débit, favorisant les copies illicites de fichiers numériques, représentent autant de facteurs qui peuvent expliquer ce phénomène. En conséquence, les systèmes de gestion numérique des droits ou DRM^[6] et les mesures techniques de protection des œuvres se développent parallèlement pour répondre à cette forme d'atteinte aux droits d'auteur. Le procédé de tatouage digital, qui est plus communément désigné sous le vocable de watermarking, en fait partie.

📁 1 Les DRM

Les DRM ou SGMN^[7] peuvent se définir comme « des systèmes techniques facilitant la gestion fiable et dynamique des droits quel qu'en soit le format d'information numérique, tout au long de son cycle chronologique, et peu importe le mode et le lieu de distribution de cette information numérisée »^[8]. La DRM doit être envisagée, comme un système complexe de gestion intégrée des droits, puisqu'elle assure de bout en bout la protection des œuvres numériques, notamment, en définissant des règles d'accès au contenu, en y insérant des métadonnées, en sécurisant leur transmission ou leur paiement ou en établissant des statistiques sur leur utilisation.

La DRM se base sur des mesures techniques de protection pour assurer une partie de ses fonctions.

Des produits DRM sont déjà disponibles sur le marché. « Real Networks », un des pionniers dans la diffusion de vidéos en mode streaming, c'est à dire sans téléchargement préalable d'un fichier, propose une solution commerciale, de distribution numérique multi-plate-forme « Helix Universal Server / RealOne Player », incluant un système de gestion des droits numériques.

📁 2 Les mesures techniques de protection

En revanche, les mesures techniques de protection ne répondent pas à cette problématique complexe de gestion des droits mais apportent des mécanismes techniques destinés à sécuriser une œuvre. Elles peuvent se classer en deux grandes catégories : celles qui érigent une protection à priori, par exemple avec des mots de passe ou avec des méthodes cryptographiques élaborées, et celles qui autorisent un contrôle à posteriori, permettant, en particulier, d'identifier le ou les auteurs d'une œuvre ou d'assurer le suivi de ses usages. Les techniques de dissimulation d'information ou « information hiding » se situent dans cette dernière catégorie.

Historiquement, la dissimulation d'information a connu de nombreuses formes et applications, mais elle connaît aujourd'hui un regain d'intérêt à cause de son applicabilité à la protection des œuvres numériques. Le graphe, ci-dessous, scinde ces procédés en deux branches, la stéganographie et le marquage.

La stéganographie (du grec steganos, couvert et graphein, écriture) consiste à dissimuler un message, que l'on souhaite conserver secret, dans un autre plus important, qui lui en revanche, peut être rendu public.

Ainsi, la stéganographie peut se définir comme étant « l'art et la science de communiquer de manière à masquer l'existence même de la communication ». Même si l'information cachée peut être codée, il ne s'agit pas de cryptographie. En effet, le secret reste imperceptible, non parce qu'il est chiffré, mais parce qu'il est intégré dans une autre information. C'est une technique de sécurité par l'obscurité puisque les personnes ignorent qu'un message secret se trouve transporté, par exemple, dans une photo ou un fichier. Un exemple très connu de stéganographie réside dans la lettre envoyée par George Sand à Alfred de Musset.

Le marquage ou tatouage électronique consiste à insérer, de manière indélébile grâce à un algorithme de codage, une faible quantité d'information dans une œuvre numérique, de façon à protéger les prérogatives de ses ayants-droits ou de ses cessionnaires. Ces éléments informatifs, souvent appelés des « métadonnées », sont rendus indissociables du signal numérique, issu du codage de l'œuvre (texte, flux audio ou vidéo, image...). Ces données insérées sont forcément relatives à l'œuvre. Il peut s'agir, par exemple, de son titre, du nom de son auteur, de ses conditions d'utilisation ou d'un numéro d'identification renvoyant à une base de données.

Cette différence majeure entre d'une part, la stéganographie, et d'autre part le marquage, se retrouve dans les types d'attaque susceptibles d'être menées contre ces techniques. Dans un cas, l'intention du pirate est de détecter, puis de lire un secret, tandis que dans le second cas, il souhaite laver le tatouage d'une œuvre, c'est à dire effacer ce dernier sans autorisation, tout en rendant indécélable cette suppression, afin de pouvoir se servir frauduleusement de cette œuvre numérique. Ainsi, pour le pirate, lire le contenu de ce marquage, qui est une tâche extrêmement malaisée à réaliser, ne constitue pas son objectif primordial.

Ce tatouage peut être robuste ou fragile. Dans le premier cas, toute tentative d'effacement de ce dernier endommage irrémédiablement l'œuvre, tandis que dans le second cas, toute modification, du marquage, le fait disparaître, prouvant ainsi que l'œuvre numérique n'est plus intègre.

Les techniques de marquage robustes, qui peuvent constituer une preuve en cas de litige puisqu'il est nécessaire de disposer d'un matériel adéquat pour extraire le tatouage, se divisent en deux ensembles, le fingerprinting et le watermarking, en fonction du contenu de l'information insérée.

Lorsque celle-ci est identique sur toutes les copies de l'œuvre, il s'agit de watermarking. C'est une sorte de tampon électronique qui permet, d'une part, d'identifier l'auteur (s'il a accepté que son nom apparaisse) et/ou le cessionnaire de l'œuvre, d'autre part, d'apporter des informations supplémentaires quant aux droits d'auteur ou aux droits voisins. Des méthodes cryptographiques peuvent être utilisées pour vérifier les assertions du propriétaire. Ce tatouage peut être visible (ou audible), correspondant alors au filigrane que nous pouvons trouver sur certains documents sécurisés (billets, passeports...) ou invisible (ou inaudible) qui devra être révélé avec un outil approprié.

Cet estampillage peut aussi assurer l'authenticité du contenu numérique marqué ou témoigner de son intégrité.

En revanche, lorsque le tatouage, ajouté au fichier à protéger, varie selon les utilisateurs destinataires, ce qui en l'occurrence correspond à une forme de numéro de série distinct, on parle de fingerprinting. L'objectif est d'assurer une traçabilité de l'œuvre en favorisant l'identification du contrevenant à l'origine de copies illégales. Pour cela, il suffit de récupérer l'identifiant de l'exemplaire

contrefait et de l'associer, grâce à une base de données, à une personne physique ou morale. Une des méthodes employées consiste à marquer spécialement chaque copie avec un algorithme cryptographique et à attribuer des clés spécifiquement à chaque utilisateur. Ainsi, pour ce dernier, l'usage légal de la copie de l'œuvre implique nécessairement de conserver ses clés d'une manière sécurisée sous peine de voir sa responsabilité engagée en cas de contrefaçon effectuée à partir de sa copie licite.

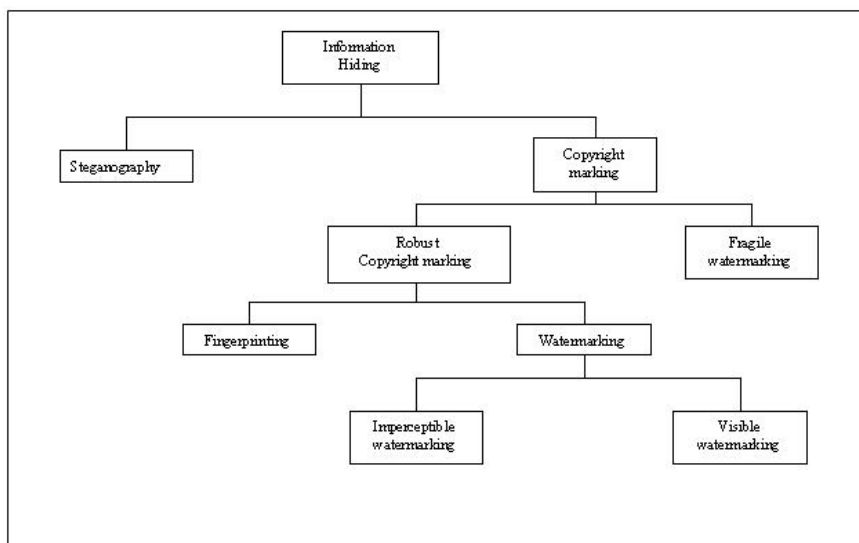


Figure 1 : Classification des techniques de dissimulation d'information^[11]

Conclusion

Alors que les dispositifs législatifs doivent normalement protéger les œuvres numériques, le coût lié au piratage a incité les ayants-droits des œuvres à les protéger aussi techniquement : la technologie est venue au secours du Droit. Mais, avec l'apparition des lois sanctionnant le contournement des dispositifs de protection technique, le Droit est venu au secours de la technologie, dont le thème sera abordé dans l'une de nos prochaines newsletters. Par la même occasion, des sujets sur des solutions techniques autour des œuvres numériques y seront approfondis tel que la stéganographie et le watermarking abordés brièvement dans cet article.

- [1]. *International Intellectual Property Association est une association regroupant les professionnels de l'industrie du copyright aux États-Unis*
- [2]. *D'après la publication du 29 avril 2005 de l'IIPA : http://www.iipa.com/pdf/2005_Apr29_USTR_301_DECISIONS.pdf.*
- [3]. *Étude sur le piratage disponible sur le site : http://www.deloitte.com/dtt/cda/doc/content/us_pswm&e_piracystudy_033004rev.pdf*
- [4]. *D'après, le rapport annuel 2004 du groupe « Danone » (1€ = 1,33 \$) disponible sur : <http://www.danone.com/cmcache/MYSESSION~369EC7EE5E548F4BC1256FEA0048B7F8/chiffre.pdf>*
- [5]. *Peer To Peer, réseaux d'échange à travers Internet dont les plus connus sont ou étaient « Napster », « Kazaa » ou « Gnutella ». « Napster » se limitait à l'échange de fichiers musicaux MP3, tandis que « Gnutella » et « Kazaa » transmettent n'importe quel type de fichiers (vidéos, musique...).*
- [6]. *Digital Rights Management*
- [7]. *Systèmes de Gestion des Droits Numériques*
- [8]. *http://www.pch.gc.ca/progs/ac-ca/progs/pda-cpb/pubs/protection/protection_f.pdf*
- [9]. *<http://membres.lycos.fr/black/romain/introduc.htm>*
- [10]. *<http://fr.wikipedia.org/wiki/St%C3%A9ganographie>*
- [11]. *Source de la figure - <http://mantis.free.fr/articles/doc/intro.zip>*

ZOOM

⇒ Téléphonie et Voix sur IP (ToIP & VoIP)

📁 Introduction

La simplicité accrue de l'utilisation des téléphones IP {soft|hard}phone, l'émergence des offres des opérateurs de convergence Wi-Fi/GSM font que la téléphonie sur IP (ToIP) devient de plus en plus accessible à tous. Cet état de fait ne doit pas faire oublier aux entreprises, et surtout aux décideurs, que la sécurité doit plus que jamais être présente dans la gestion de leurs réseaux Voix sur IP (VoIP). Cet article couvre les aspects de sécurité « standard » et détaillera ensuite l'aspect, primordial, de la sécurisation des données transitant sur les réseaux de VoIP.

📁 Définition

La Téléphonie sur IP ou ToIP consiste à mettre en place des services téléphoniques sur une infrastructure IP existante, en utilisant la technique de la Voix sur IP (VoIP). Les communications vocales sont alors transmises via un réseau IP à partir de et à destination de téléphones spéciaux. Les postes particuliers sont baptisés IP-Phone (Softphone ou Hardphone). Un téléphone IP doit être alimenté par courant. Il est capable de numériser la voix pour la transmettre sur des réseaux IP et peut, à l'inverse, rassembler les paquets entrants pour interpréter la voix reçue. La téléphonie sur IP circule sur des réseaux privés - LAN ou VPN - ou publics.

Le terme Voix sur IP ou VoIP représente la technologie utilisée pour transporter le service de téléphonie sur IP (transport de la voix) sur un backbone ou autre MAN/WAN.

Les standards utilisés en VoIP sont, pour les protocoles, H323 ou SIP pour la signalisation, et pour le transport, RTP (Real Time Protocol) et RTCP (Real-time Transport Control Protocol). Ces protocoles sont optimisés pour mettre en relation des équipements et pour transporter des flux temps réels. Cependant, ces protocoles n'ont pas été conçus pour gérer ni la sécurité, ni le chiffrement de la communication.

📁 Contexte Technologique

La VoIP, technologie de communication vocale en pleine émergence dans l'hexagone, fait partie d'un tournant dans le monde de la communication. En effet, la convergence du triple play (voix, données et vidéo) est en train de devenir un des enjeux principaux des grandes entreprises. Les nouvelles capacités des réseaux permettent de transférer de manière fiable des données en temps réel. Ainsi, les applications de vidéo d'audioconférence et de téléphonie envahissent le monde IP, réservé auparavant au transfert de données.

Outre les solutions propriétaires bien connues mais peu interopérables, d'autres moyens existent pour mettre en place une solution de ToIP sur des environnements élargis.

Ainsi, avec plus de 40 millions d'utilisateurs (croissance : 150 000 utilisateurs supplémentaires par jour), Skype est en passe de devenir un acteur incontournable de la communication sur IP. Cependant, le passé de ces créateurs (ce sont aussi les créateurs de Kazaa, outil d'échange peer to peer, ayant la fâcheuse réputation de regorger de logiciels espions), et les récentes études^[1] sur le fonctionnement (protocole propriétaire, aptitudes à déjouer les pare-feux) de ce logiciel doivent être pris en compte si on souhaite le déployer dans un environnement professionnel. D'aucun rétorqueront que la versatilité de Skype fait aussi sa difficulté à détecter sa présence sur le réseau. Cependant, une solution peut être mise en place simplement : vérifier régulièrement que Skype n'est pas installé pour un compte donné via des GPO par exemple, puis l'enlever le cas échéant.

Autre solution, Asterisk, IPBX libre, commence à obtenir la maturité suffisante pour convaincre les industriels. Il permet, entre autres, la messagerie vocale, la conférence, les serveurs vocaux, la distribution des appels. Asterisk implémente notamment les

protocoles H323 et SIP, il s'intègre donc aisément à une architecture de ToIP construite sur SIP. Asterisk peut également jouer le rôle de passerelle avec les réseaux publics (RTC, GSM, ...).

L'architecture de ToIP doit offrir au moins deux services fondamentaux aux yeux de la plupart des utilisateurs : une disponibilité du réseau téléphonique au moins équivalente et une qualité de service au moins identique à celle du réseau commuté. Pour obtenir de tels résultats, l'architecte utilise les recettes connues du domaine des Plan de Reprise d'Activité. Il doit, non seulement investir dans des équipements réseaux redondants spécialisés dans la gestion de la qualité de service pour la VoIP, mais aussi faire le nécessaire pour alimenter ses téléphones ({soft|hard}phones) en courant électrique quoiqu'il arrive.

📁 Services

Pour être attractif la VoIP fournit, au minimum, les mêmes services que ceux offerts par le réseau commuté : présentation du numéro, gestion des boîtes vocales, gestion des appels entrants, services vocaux interactifs, personnalisation des postes téléphoniques. On peut ajouter à ces services ceux issus directement du monde IP : utilisation du réseau local, déploiement d'applications Intranet sur les écrans des téléphones IP, réception de messages (mails, flux RSS), utilisation de softphone, vidéo conférence, vidéo surveillance, vidéo à la demande...

La technologie Voice over Wifi, ou VoWIFI, couplée aux capacités des réseaux GSM forment un nouveau service de mobilité permettant à un utilisateur de passer de son opérateur GSM à l'infrastructure VoIP de l'entreprise dès qu'il entrera dans le périmètre d'un point d'accès WiFi. Des tests et des mises en situation sur des parcs réduits sont en cours d'études chez les grands opérateurs et les grands constructeurs œuvrant dans la téléphonie.

Les enjeux économiques couverts par cette offre contribueront certainement à développer encore la percée de la ToIP non seulement dans les entreprises mais aussi chez le particulier.

Sécurité standard

Cependant, la multitude des nouveaux services induite par la VoIP ne doit pas faire perdre de vue le service associé aux appels d'urgences.

Toute la conception d'une architecture multi-sites doit tenir compte de la problématique de localisation de

l'appelant afin de le rediriger vers les services d'urgence les plus proches de lui.

Sécurité des données

Les aspects de sécurité cités ci-dessus ne doivent en aucun cas faire oublier aux décideurs l'aspect sécurité des données que nous allons analyser maintenant : la sécurisation des communications.

La sécurisation des communications passe par deux étapes : la sécurisation de la signalisation et celle du transport des données. Pourquoi sécuriser la signalisation ?

Parce que la signalisation (transportée par SIP ou par H323, notamment) transporte en clair un grand nombre d'informations utiles : le protocole SIP, qui ressemble fort au protocole HTTP, est très simple à comprendre. Ce protocole contient par exemple les identifiants nécessaires à l'authentification du client auprès du serveur.

La capture d'écran (**figure 2**) ci-dessous met en évidence la facilité qu'il y a à écouter et obtenir des codes secrets transitant sur le réseau.

```
* Reading and parsing dump file...
* Found Accounts:

Num      Server      Client      User      Algorithm      Hash / Password
1        192.168.19.81  192.168.19.120  500      PLAIN          12345
2        192.168.19.81  192.168.19.120  500      PLAIN          34after12
3        192.168.19.81  192.168.19.120  500      MD5            d3bc10e4f2c9c275fe7da2f20f17600f
4        192.168.19.81  192.168.19.120  500      MD5            e5827d8cda285252d5ce87ad8e3c64ca
5        192.168.19.81  192.168.19.120  500      MD5            6524e36531b0dd77efa87ced26b4af3

* Select which entry to crack (1 - 5): 3

* Generating static MD5 hash...1a24e68fa4904bd8ce0b7a2b37fffab2
* Starting bruteforce against user '500' (MD5 Hash: 'd3bc10e4f2c9c275fe7da2f20f17600f')
* Loaded wordlist: 'big-wordlist.txt'
* Tried 8462686 passwords in 13 seconds

* Found password: 'alb2c3'
* Updating 'logins-sip.txt'...done
```

Figure 2 : Décodage de mot de passes cryptés

Au travers de ces informations, le risque est, qu'une fois les identifiants de connexions sur le serveur de VoIP récupérés, n'importe qui peut usurper votre identité et donc se faire passer pour vous, écouter vos messages vocaux, recevoir vos appels, ...

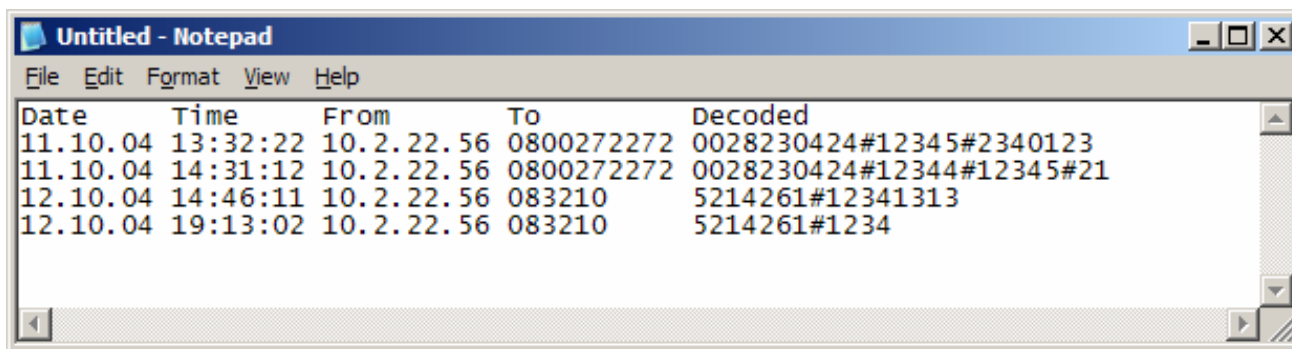
La solution réside dans la mise en place de mécanismes de sécurité au-dessus de SIP. Il existe par exemple des implémentations de SIPv2 (implémentation de TLS notamment) qui permettent de sécuriser les échanges de signalisation.

Bien entendu, il est nécessaire de vérifier la comptabilité des {soft|hard}phones avec ces protocoles.

Seconde partie à sécuriser : les communications proprement dites. En effet, outre le fait d'être certain que l'on communique avec l'interlocuteur choisi, il est primordial de s'assurer que la communication ne sera ni écoutée, ni rejouée plus tard par un tiers. Il est trivial avec un logiciel de capture de trame de trouver et d'écouter en différé une conversation téléphonique. Il est aussi possible avec des logiciels

spécialisés « d'écouter » d'autres choses nettement plus intéressantes : un code de boîte vocale tapé lors de l'interrogation de son répondeur, un code tapé pour accéder à son compte en banque, ...

Ceci est rendu possible par le fait que chaque fois qu'une touche est pressée, une fréquence est émise sur la ligne. Ce sont ces différentes fréquences qui sont rassemblées et décodées pour former ce qui a été tapé sur le clavier téléphonique, c'est-à-dire le code confidentiel.



| Date | Time | From | To | Decoded |
|----------|----------|------------|------------|---------------------------|
| 11.10.04 | 13:32:22 | 10.2.22.56 | 0800272272 | 0028230424#12345#2340123 |
| 11.10.04 | 14:31:12 | 10.2.22.56 | 0800272272 | 0028230424#12344#12345#21 |
| 12.10.04 | 14:46:11 | 10.2.22.56 | 083210 | 5214261#12341313 |
| 12.10.04 | 19:13:02 | 10.2.22.56 | 083210 | 5214261#1234 |

Figure 3 : Informations décodées

Le risque, on l'aura compris, est lié à la possibilité de voir des informations personnelles être écoutées et récupérées par un tiers. Pour se prémunir de ceci, il est indispensable de mettre en place un mécanisme de sécurisation du contenu des communications.

Les informations en VoIP sont

transportées par des protocoles (par exemple Real Time Protocol ou RTP) dont la caractéristique principale est de répondre au besoin « temps réel » nécessaire à toute communication vocale.

Outre les protocoles propriétaires et leurs algorithmes fermés, il existe des

implémentations dites « ouvertes », ajoutant la sécurité dans le protocole RTP. Ainsi SRTP ^[2] (ou Secure RTP) utilise différents mécanismes tels que le chiffrement par clé (MiKEY) pour s'affranchir de toute écoute inopportune.

Conclusion

L'intérêt majeur de le ToIP pour les entreprises est un intérêt financier. Mais cette mise en place ne doit en aucun cas mettre de côté le fait que la sécurité des données transportées doit être assurée. Pour ce faire, différents mécanismes de sécurité existent, mais une attention particulière doit être portée sur les législations en vigueur dans les pays où ils sont déployés (interceptions légales possible, chiffrement restreint, ...).

[1]. http://sid.rstack.org/pres/0606_Recon_Skype_Botnet.pdf

http://actes.sstic.org/SSTIC06/Castle_in_the_Skype/SSTIC06-article-Desclaux-Castle_in_the_Skype.pdf

[2]. <http://srtp.sourceforge.net/srtp.html>

L'ESSENTIEL

Focus sur Le Correspondant Informatique et Liberté

La traduction d'une directive Européenne a nécessité la réforme de la loi Informatique et Liberté (août 2004). Elle désigne une nouvelle fonction, celle du Correspondant Informatique et Liberté ou CIL, interlocuteur de l'entreprise spécialisé, chargé de garantir le respect de la Loi sur les sujets informatiques. Sans constituer un quelconque conseil juridique et sans prétendre à l'exhaustivité, cet article essaie de déterminer les questions essentielles qu'il faut se poser quant au correspondant CNIL : pourquoi, qui peut exercer cette fonction, quels sont ses pouvoirs ?...

Introduction

La fonction de correspondant existe déjà dans de nombreux pays européens ; il était donc nécessaire pour la France modifier la Loi pour se doter du même type de réglementation. Si son rôle est relativement bien défini, le choix de la personne, entre juriste et informaticien pourra se révéler difficile. A noter que plusieurs personnes peuvent exercer ce rôle et que la disposition, pour une entreprise d'un tel représentant n'est pas une obligation.

Quelle est sa mission ?

En deux mots, sa mission consiste à faire respecter la Loi Informatique et Liberté au sein de l'entreprise, notamment pour tous les aspects liés à la protection des données personnelles, et ce de manière indépendante. Mais ce n'est pas tout, il doit également tenir un registre des tâches effectuées par le responsable des opérations de manière à garantir que les modifications de traitement ne sont pas susceptibles de porter atteinte aux droits et libertés ou à la vie privée des personnes.

Son rôle est aussi de diffuser la culture CNIL pour sensibiliser l'ensemble de personnes ayant accès aux données personnelles. Sa mission est donc stratégique, d'autant qu'elle offre des intérêts non négligeables.

Les avantages pour l'entreprise

On trouve deux avantages majeurs :

- La simplification des formalités de déclaration à la CNIL : les traitements ordinaires et courants n'ont plus besoins d'être déclarés. Il faudra toutefois veiller à ce que les traitements dits sensibles soient dûment déclarés.
- La solution pour allier protection des libertés individuelles et intérêts de l'entreprise. Il est important de signaler qu'il s'agit bien d'une aide n'exonérant en rien le responsable des traitements de sa responsabilité civile et pénale.

Par ailleurs, il doit être consulté avant toute mise en œuvre de nouveau traitements ou de modification de traitement existant, il informe les responsables de tout manquement avant de saisir la CNIL et réalise des bilans réguliers de ses activités (registre).

Qui choisir ?

Deux profils se distinguent, c'est au chef d'entreprise de choisir entre l'informaticien et le juriste. Bien évidemment, dans le premier cas l'informaticien sera plus à même de fournir des aides au responsable des traitements alors que le juriste aura une meilleure appréciation des lois.

Si aucun niveau d'étude ou de formation n'est défini, le correspondant doit avoir « des qualifications requises pour exercer ses missions », ce qui démontre que le profil recherché correspond à une personne ayant déjà une certaine expérience ou qui aurait suivi des formations complémentaires dans les domaines qu'elle ne maîtrise pas.

Un consensus semble toutefois se dégager en faveur du profil informaticien sans doute parce qu'il sera plus au fait avec la démarche qui doit être celle d'un chef de projet.

Tout en étant un bon communicant, il devra être suffisamment ferme pour imposer des décisions quelquefois contraignantes et disposer de moyens pour mener à bien sa mission.

Il est nécessaire qu'il soit également bien organisé pour remonter les informations, notamment par le biais d'un registre des traitements, à toute personne qui en fait la demande, cette demande pouvant être également formulée par la CNIL.

Pour être impartial, il est impératif qu'il n'occupe pas de poste tel que les postes de direction, de responsable des traitements... ses activités exercées en parallèle ne devant pas entrer en conflit avec l'exercice de sa mission.

Reste une question : peut-on choisir un interlocuteur externe ? Physique ou morale, aucune précision n'est donnée sur son statut. Toutefois, à partir d'une certaine taille de structure on constate que cette tâche est généralement confiée à un ou des internes.

Nomination et révocation

Les deux actions sont à l'initiative du responsable des traitements, par le biais du formulaire dont le lien est fourni plus bas par envoi par lettre recommandée. A noter que la CNIL peut également demander la révocation en cas de manquement avéré.

Conclusion

Au travers de cet article, nous avons présenté le rôle du Correspondant Informatique et Liberté ainsi que ses devoirs. Nombre d'entreprises ne sont pas encore dotées d'un tel représentant ou confient ce rôle au RSSI. Dans le premier cas, on peut douter de la bonne application des dispositions de la Loi et perdre du temps en déclarations tandis que dans le second, on ajoute une tâche supplémentaire à un emploi du temps déjà chargé. Le texte offrant une souplesse dans la désignation du correspondant, qui, rappelons-le reste facultative, on peut se demander si leur compte dépassera les 500 pour la fin de cette année...

Pour en savoir plus : <http://www.cnil.fr/index.php?1821> et

<http://www.legifrance.gouv.fr/WAspad/VisuNav?cidNav=28066&indiceNav=1&tableNav=CONSOLIDE&ligneDebNav=1>

Association Française des Correspondants à la Protection des Données à Caractère Personnel (payant) : <http://www.afcdp.org/>

Formalités de déclaration d'un correspondant : http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CIL/form_CIL.pdf

Pour vous inscrire à la newsletter, veuillez envoyer un mail à :

newsletter-subscribe@esec.fr

Conformément à la loi « Informatique et libertés » du 6 janvier 1978, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent. Si vous souhaitez exercer ce droit et obtenir communication des informations vous concernant, veuillez vous adresser au directeur de l'agence ESEC.