NOUVELLE FORMULE 100% INFO

NUMÉRO #9 / OCTOBRE - NOVEMBRE 2005

www.hackernewsmag.com

HACKER Magazine

LE MAGAZINE 100% SÉCURITÉ

2€
0% DE PUBLICITÉ
DES ARTICLES ET DE L'INFORMATION SEULEMENT

» UTILISER GRATUITEMENT INTERNET DES KIOSQUES

» EMULATION : RESSUSCITER LES ANCIENS JEUX

» CRÉER SON BLOG PERSO

» A LA DÉCOUVERTE DE FREEBSD

» ESPIONNAGE TOUS NOS CONSEILS

EXCLUSI
LA REPRODUCTIO
DES SIGNATURES 3

GOOGLE

LES ASTUCES ET SECRETS DU PLUS CÉLÈBRE MOTEUR DE RECHERCH

BEL/LUX : 2,3€ - CH : 4.00 FS $ CAN : 3.25 - DOM :

Sprea Editori

M 02736 - 9 - F: 2,00 € - RD

Année 2 – N. 9
Bimestriel

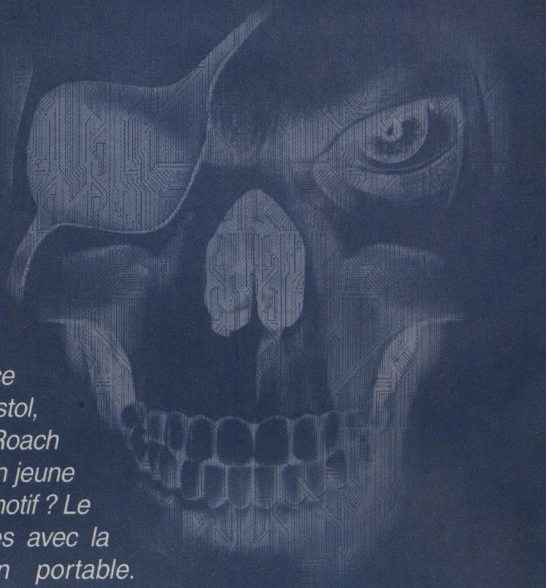
HACKER news Magazine
www.hackernewsmag.com
Le magazine ANTI-PIRATE, 100% SECURITE

Éditorial

La loi du plus fort

Ceux qui croient encore que la vie est une cour de récréation risquent d'en être pour leurs frais. On n'est pas là pour rigoler, terminé tout ça. Oubliez ce que l'on vous a appris, l'injustice est le fondement de la société, pas sa conséquence. A dire vrai, c'est même bien pire, l'injustice est le sel de la vie…

Blasphème ? Et pourtant… C'est l'injustice qui nous arrache à la léthargie, qui nous pousse à la révolte, à la réflexion, et parfois même à la compréhension puis au progrès. Tant qu'il s'indigne, l'homme est vivant et tant qu'il est vivant, il avance. Remercions donc les "plus forts", ceux-là même qui nous imposent leurs lois scélérates et iniques. De toutes façons une pétition soutenant "la loi du plus faible" n'obtiendra guère que la signature des amateurs d'oxymore… Glanons ça et là quelques beaux exemples d'injustice susceptibles de nous toucher. A Bristol, au Royaume-Uni, un certain juge Roach a condamné à six mois de prison un jeune homme de dix-neuf ans. Pour quel motif ? Le joyeux plaisantin a filmé un procès avec la caméra vidéo intégrée à son portable. Dommage qu'il se soit fait repérer, on aurait peut-être pu visionner tout ça sur Internet. Treviglio, Italie. Un petit entrepreneur qui portait le même nom qu'un célèbre styliste à dû céder après des années de lutte. Il n'aura plus le droit d'utiliser son propre nom dans un but commercial. Et tout ça pourquoi ? Parce que le célèbre styliste avait les moyens, lui, de payer un longue et coûteuse procédure judiciaire. Les petits écrasés par les gros. Darwin était-il prophète ? Aux Etats-Unis, c'est la mère célibataire de cinq enfants qui se voit réclamer 7500 dollars par la toute-puissante RIAA, au prétexte qu'elle aurait téléchargé illégalement de la musique. Et pourtant il y a peu, cette brave dame avouait n'avoir aucune idée de ce que pouvait être un Mp3. Quant au P2P, n'en parlons pas. Peu importe, seul le côté de la barrière duquel nous nous trouvons importe. La loi du plus fort n'est pas le problème, c'est la loi des autres, le problème.



Hacker News : votre magazine

Hacker News Magazine
1er magazine européen Hacker
http://www.hackernewsmag.com
contact@hackernewsmag.com

Contact France:
35 rue Emile Zola
92150 Suresnes
Tel. : 01 41 44 38 70
Fax : 01 45 06 24 19

Ont collaboré à ce numéro:
Grégory Peron, Benoît Bailleul
David Bourdier, Gualtiero

Maquette : NoviMedia LLC & OOO

Imprimerie : Roto3 (Italie)
Print : Roto3 (Italy)
Via Turbigo 11/B, CASTANO PRIMO

Distribution:
CCEI , 33 Rue Henard, 75012 Paris

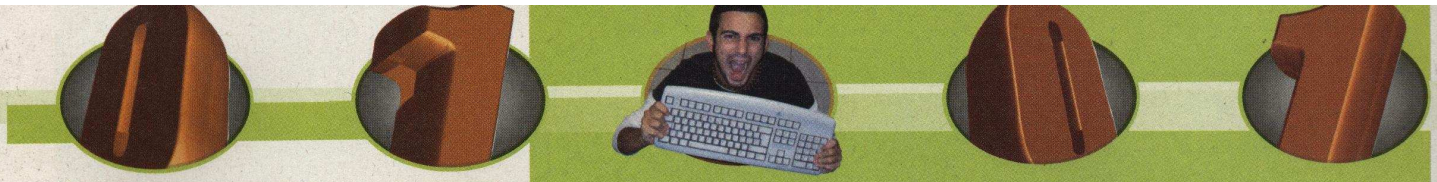
Commission paritaire : en cours

Dépôt légal : à parution
ISSN: en cours

Hacker News magazine est une publication du **groupe Sprea Editori**

Directeur de la publication
Luca Sprea

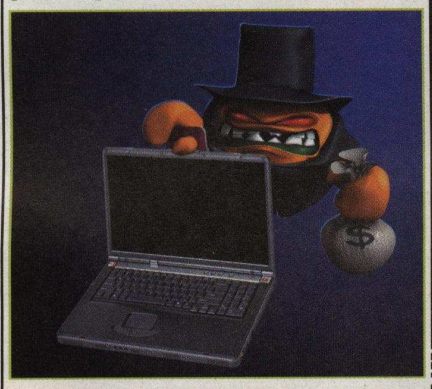
Editeur :
Sprea Editori SPA
Via Torino 51 - 20063 Cernusco s/N,
Milano - Italie



FONCTION

ANTI-PHISHING POUR INTERNET EXPLORER

Une fonctionnalité "anti-phishing" est désormais disponible pour MSN Toolbar (la barre d'outils de MSN). Initialement prévu pour Internet Explorer 7, cet outil peut être intégré dès aujourd'hui sous forme de plug-in. En partenariat avec la société WholeSecurity, qui édite une liste noire des sites de phishing, ce programme préviendra les utilisateurs d'Internet Explorer dès qu'ils tenteront d'accéder à un site suspect. Le phishing consiste à attirer les internautes sur de faux sites commerciaux, bancaires ou institutionnels (qui copient les originaux) pour leur subtiliser informations personnelles et coordonnées bancaires. Ce phénomène est en pleine explosion.



LES LOGICIELS LIBRES S'ENVOLENT

Le monde des logiciels libres est plébiscité par les Français et nos administrations publiques. Selon le cabinet Pierre Audouin Consultant, "*La France est un des pays les plus friands de logiciel libre, avec l'Allemagne et le Japon*". Dans son étude "*Le logiciel libre : mythes & réalités*", le cabinet estime que le marché a progressé de 46% en 2004 et devrait se maintenir à un taux de 40% chaque année jusqu'en 2008 !

En France, ce marché représenterait 146 millions d'euros, car, ne l'oublions pas, libre ne veut pas forcément dire gratuit : achat, dons et services payants participent à ce modèle économique émergent. Comparé aux 27 milliards d'euros du marché global des logiciels, le libre fait encore office de petit poucet... mais sa progression reste la plus forte du secteur.

Et le libre, longtemps considéré comme étant réservé à une élite informaticienne, se démocratise enfin, notamment sous l'impulsion des pouvoirs publics. Si ces programmes ont gagné en simplicité, en stabilité et en ergonomie, ils séduisent aussi les Français par leur image "contre-culture". Ils sont souvent considérés comme une alternative militante à l'hégémonie de programmes propriétaires, notamment américains, comme ceux de Microsoft.

Moins de dépendance, personnalisation des programmes, économies à l'acquisition et à l'utilisation, souplesse de distribution : les atouts du libre sont indéniables. Le Cabinet Pierre Audouin Consultant rappelle cependant que l'argument d'un "*développement communautaire plus fiable est discutable*". Il serait "*moins encadré et moins abouti que les développements réalisés par un éditeur de logiciels*". Le cabinet affirme aussi que "*le logiciel à l'avantage d'avoir un coût d'acquisition relativement faible et très compétitif, mais les simulations de retour sur investissement montrent que le coût total de possession après quelques années n'est pas forcément en faveur du logiciel libre*".

Trublion, le libre a globalement favorisé l'innovation au sein du secteur informatique : "*le logiciel libre a fait sortir les concepteurs de logiciels de leur tour d'ivoire et les a rapprochés des attentes du marché en redynamisant le développement spécifique*".

>> MICROSOFT INVITE DES HACKERS !

Au mois de mars dernier, Microsoft a invité des hackers dans son quartier général de Redmond ! Lors de cette conférence baptisée Blue Hat (sans doute une référen-

ground" conférence Black Hat), des participants volontaires étaient présents pour discuter des différentes failles dans la sécurité de Windows et des principaux logiciels de Microsoft. Un hacker a fait une démonstration saisissante : il a réussi à leurrer les systèmes de sécurité en introduisant un PC portable Windows dans un réseau Wi-Fi malicieux. Très admiratifs, les pontes de Microsoft ont déclaré qu'ils voulaient réorganiser ce genre d'événement deux fois par an. Ils ont ajouté que ces deux jours de meeting ont été très intéressants et productifs pour les ingénieurs de la firme au papillon.

>> DES PIRATES À LA STAR AC'

Il y a peu de temps, la nouvelle saison de la Star Academy a débarqué sur TF1. Dès les premiers jours, les pensionnaires du château se sont rendu compte d'un fait gênant. La platine CD sur laquelle ils doivent écouter leurs chansons pour s'entraîner ne fonctionnait pas très bien : pas moyen de lire les CD que la production leur a fourni pour leurs cours de chant. Et pour cause, il s'agit en fait de CD-R et leur platine ne les lit tout simplement pas. Le piratage existe donc bel et bien à la Star Ac' ! Le bon

L'ALLEMAGNE DÉCLARE LA GUERRE

"La sécurité informatique est devenue une question nationale", déclarait fin août Otto Schily, le ministre de l'Intérieur allemand. L'Allemagne s'est dotée d'un "Centre de veille et de réaction" aux attaques du Net. Cet organisme pilotera la lutte anticybercriminalité de l'État fédéral qui doit faire face, toujours selon le ministre, à "une menace croissante d'une autre dimension que celle que nous avons connue jusqu'à présent".

En janvier 2006, un "Centre d'urgence IT" (Krisenreaktionszentrum IT) sera inauguré, hébergé au sein de l'Agence fédérale pour la sécurité informatique (BSI) qui emploie déjà 400 personnes. Ce centre aura une mission d'alerte et de lutte contre les attaques lancées sur le Web à destination des particuliers, des entreprises ou des services publics. Une plus grande coopération entre organismes de sécurité est aussi à l'ordre du jour.

GOOGLE, COLLECTIONNEUR DE PHOTOS PORNOS VOLÉES ?

Le moteur de recherche d'images de Google, qui scanne et affiche les photos trouvées sur le Web, est attaqué par le responsable d'un site de charme. Perfect10. Ledit site accuse Google de rendre publiques ses photos dénudées, *"travaux artistiques d'une indéniable qualité"* sans autorisation préalable. Google se servirait de ces clichés (comme ceux de milliers d'autres sites) pour attirer les chalands et donc vendre plus de publicité. Mais il ne les sélectionne pas et ne vérifie pas semble-t-il les copyright liés à ces clichés. Il causerait un préjudice au site, qui s'estime spolié. Le responsable de Perfect10 n'est pas un illuminé, mais une pointure universitaire : il s'agit du docteur Norm Zada, un ancien professeur à Stanford et Columbia et ex-chercheur chez IBM.

100 000 SPYWARES EN CIRCULATION

Le nombre de spywares circulant sur le Net aurait doublé au premier semestre 2005. C'est en tout cas ce qu'affirme l'éditeur de logiciels Webroot Software qui en dénombrerait plus de 100 000.

L'étude indique que ces logiciels espions sont de plus en plus sophistiqués pour contourner les protections logicielles du marché. Webroot estime que 80% des machines professionnelles ou grand public seraient d'ores et déjà infectées par des spywares. On en recenserait en moyenne 25,4 sur un PC familial et 27 sur un poste de travail en entreprise.

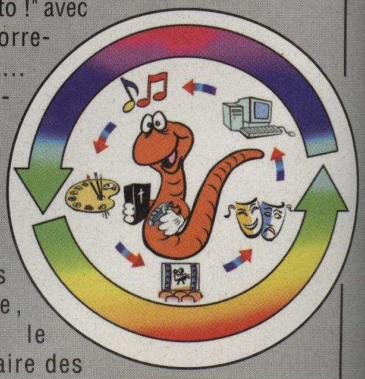
Le Web abriterait quelque 300 000 URL hébergeant des logiciels espions, et les premiers pays "producteurs seraient " les États-Unis, la Pologne et les Pays-Bas.

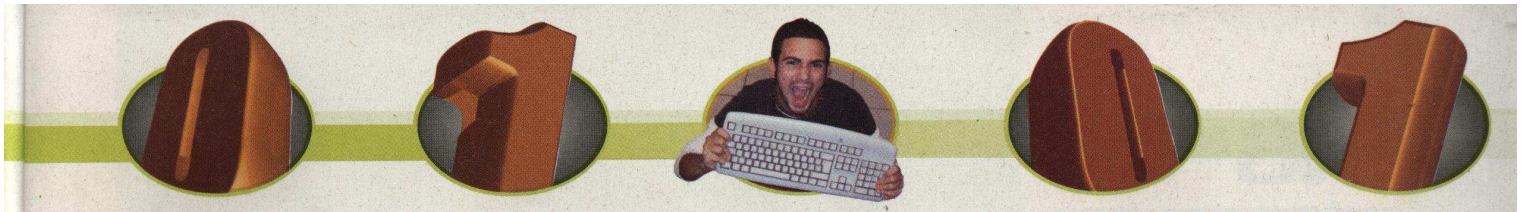
» CASE PRISON DÈS LE 1ER TOUR !

Mi-août, le méchant ver Zotob s'installait sur les réseaux des plus grandes sociétés américaines, rendues ainsi vulnérables à des attaques ultérieures. Son créateur présumé, un Marocain de 18 ans, a été arrêté une dizaine de jours plus tard, repéré en un temps record par un FBI sur les crocs.

» MSN ET LE VER MUTANT

Kelvir.HI est doué... Repéré sur MSN, ce ver issu de la lignée Kelvir (plus de 100 variantes) a la particularité de s'adapter à la langue des utilisateurs. Polyglotte, il peut envoyer ses messages en anglais, allemand, français, hollandais, grec, italien, portugais, suédois, espagnol et turc ! Kelvir.HI vous laisse un message "J'ai trouvé votre photo !" avec un lien correspondant... bien évidemment contaminé. Il s'attaque à vos outils système, comme le gestionnaire des tâches, l'éditeur de registre et la restauration système.

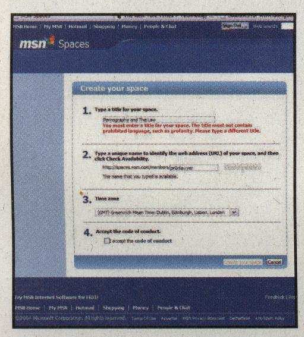




MSN SPACES OU MSN SPAMS?

MSN Spaces, le service de création de blogs de Microsoft, abrite "à l'insu de son plein gré" des essaims entiers de spammers. Ces derniers hébergent du contenu illicite sur ces espaces et s'en servent comme plateforme pour envoyer leurs "pourriels".

La société SurfControl, spécialisée dans la sécurité Internet, estime que, début août, "30% des spams dirigeaient les victimes vers des sites Geocities vantant des produits pharmaceutiques.

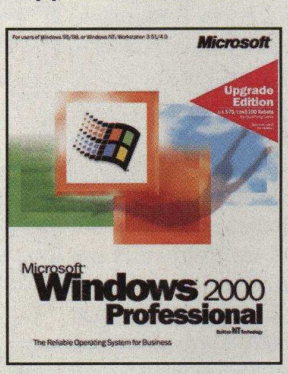


Les spammeurs ont maintenant déplacé leur contenu vers MSN Spaces. D'après les informations dont nous disposons, le volume de spam ciblant des sites MSN est d'environ 10%, et ce chiffre devrait augmenter".

Pourquoi MSN Spaces ? Il semble que la procédure d'enregistrement et de création de compte "Passport", très simplifiée, attire les spammeurs désireux de bénéficier de services en ligne gratuits et peu contrôlés.

LE CODE SOURCE DE WINDOWS SÉCURISÉ?

William Genovese, plus connu sous le pseudonyme "Illwill", plaide coupable dans le procès qui l'oppose à Microsoft. Cet internaute américain de 28 ans est accusé d'avoir piraté puis revendu une partie du code source de Windows. La victime ? Microsoft, qui s'était fait chiper de grosses portions du code source de Windows (2000 et NT 4.0). Doué mais peu discret, le jeune homme les proposait à la vente... sur son propre site Web. Il clame haut et fort qu'il n'est pas l'auteur du larcin mais risque tout de même jusqu'à 10 ans de prison et 250 000 dollars d'amende.



Microsoft estime que la sécurité interne de son réseau n'est pas en cause, mais que le pirate aurait obtenu ces éléments via des agences gouvernementales, de gouvernements étrangers ou d'universités qui possèdent des exemplaires "confidentiels" du code. L'auteur du vol n'a toujours pas été retrouvé.

SURVEILLER SA PETITE COPINE ? JUSQU'À 5 ANS DE PRISON

Le Loverspy ("Espion d'"amant") permettait d'envoyer cinq emails piégés à des personnes de son choix pour pouvoir mieux espionner ensuite leurs activités sur le Net (échanges de mails, chat, navigation, etc.) Payant (89 $!), ce service était édité par un jeune Salvadorien de 25 ans, poursuivi depuis par le FBI. D'autres plaintes ont été déposées contre quatre utilisateurs du programme : deux hommes (49 et 54 ans) et deux femmes (34 et 40 ans). Le créateur de Loverspy risque jusqu'à 175 ans de prison tandis que

ses "clients" peuvent encourir jusqu'à 5 ans d'emprisonnement. Le FBI aurait recensé plus de mille utilisateurs de Loverspy à travers le monde.

ClearSwift (société de surveillance et de filtrage des emails) avance que le message publicitaire de Lover Spy représente pas moins de 15 % du total des emails que ses logiciels de filtrage ont bloqué le mois dernier. Ses porte-parole indiquent aussi que les logiciels de la société ont récemment enregistré nombre de tentatives d'espionnage industriel reposant sur ce genre de spywares. Le marché est en plein boom !

>> BYE BYE TO THEREALWORLD

Le site allemand TheRealWorld.de, qui proposait le téléchargement de liens Torrent et eDonkey, a été fermé suite à une action de la MPAA (Motion Picture Association of America). L'association de défense des professionnels du cinéma américain reproche au site d'avoir permis l'échange de centaines d'émissions et de séries télévisées. Selon la société CacheLogic (www.cachelogic.com), plus de 60% des fichiers échangés et téléchargés par le biais du P2P sont des films et séries TV.

>> TISCALI ET LES P2PISTES

Selon Tiscali UK, 1% de ses 600 000 abonnés accaparent 30% de la bande passante. Pour mettre un frein à ceux qui font partie de cette minorité, le FAI anglais va mettre en place un système de restriction. Les P2Pistes n'auront que trois chances de rentrer dans le droit chemin. Après deux avertissements, les clients verront leur bande passante diminuer drastiquement pendant les heures de grande affluence . Ces restrictions ne font évidemment pas partie du contrat d'origine : voilà pour les FAI ce qui signifie la notion d'"offre illimitée"...

YUSUFALI, LE VER QUI FAIT DES VERS

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ كُتِبَ عَلَيۡكُمُ ٱلصِّيَامُ كَمَا كُتِبَ عَلَى
ٱلَّذِينَ مِن قَبۡلِكُمۡ لَعَلَّكُمۡ تَتَّقُونَ ١٨٣ أَيَّامٗا مَّعۡدُودَٰتٖۚ
فَمَن كَانَ مِنكُم مَّرِيضًا أَوۡ عَلَىٰ سَفَرٖ فَعِدَّةٞ مِّنۡ أَيَّامٍ أُخَرَۚ
وَعَلَى ٱلَّذِينَ يُطِيقُونَهُۥ فِدۡيَةٞ طَعَامُ مِسۡكِينٖۖ فَمَن تَطَوَّعَ
خَيۡرٗا فَهُوَ خَيۡرٞ لَّهُۥۚ وَأَن تَصُومُواْ خَيۡرٞ لَّكُمۡ إِن كُنتُمۡ
تَعۡلَمُونَ ١٨٤ شَهۡرُ رَمَضَانَ ٱلَّذِيٓ أُنزِلَ فِيهِ ٱلۡقُرۡءَانُ هُدٗى
لِّلنَّاسِ وَبَيِّنَٰتٖ مِّنَ ٱلۡهُدَىٰ وَٱلۡفُرۡقَانِۚ فَمَن شَهِدَ مِنكُمُ
ٱلشَّهۡرَ فَلۡيَصُمۡهُۖ وَمَن كَانَ مَرِيضًا أَوۡ عَلَىٰ سَفَرٖ فَعِدَّةٞ مِّنۡ
أَيَّامٍ أُخَرَۗ يُرِيدُ ٱللَّهُ بِكُمُ ٱلۡيُسۡرَ وَلَا يُرِيدُ بِكُمُ ٱلۡعُسۡرَ وَلِتُكۡمِلُواْ
ٱلۡعِدَّةَ وَلِتُكَبِّرُواْ ٱللَّهَ عَلَىٰ مَا هَدَىٰكُمۡ وَلَعَلَّكُمۡ تَشۡكُرُونَ ١٨٥

Parmi tous les vers se propageant par e-mail, Yusufali-A est plutôt original. Ce dernier se greffe dans la base de registre de votre ordinateur puis analyse les fenêtres que vous ouvrirez pendant vos surfs. Si celles-ci contiennent des mots à connotation sexuelle (il dispose d'un dictionnaire d'une dizaine de mots), le ver les bloque et affiche un message avec quelques vers du Coran ("Dieu sait ce qui se passe chez vous", etc.) Sophos souligne que Yusufali-A peut afficher plusieurs extraits du livre saint. Si l'utilisateur persiste dans ses recherches "coupables", il ouvre enfin une fenêtre qui le force à clore sa session, à fermer son PC ou à le redémarrer ! Difficile de savoir s'il s'agit d'une blague ou d'une véritable action militante. Même s'il est désagréable de choper ce genre de ver, au moins celui-ci ne détruira pas vos données et ne vous fera pas de chantage… À noter que le nom de ce ver est celui d'un éminent traducteur du Coran, Abdullah Yusuf Ali.

DES FAUX BILLETS SNCF ? C'EST POSSIBLE !

Un réseau de contrefaçon de billets SNCF a été démantelé à Paris. Resquiller, c'est dépassé ; maintenant la classe ce sont les faux billets ! La police a pu saisir 2000 titres de transport et les planches de billets vierges ayant servi à leur fabrication. Les malfaiteurs avaient scanné un billet de train émis en Allemagne qu'ils avaient reproduit. Les autorités parlent de 17 000 contrefaçons écoulées, ce qui représente une valeur de 100 000 €. Les quatre escrocs encourent cinq années de prison alors que les utilisateurs des billets ne risquent qu'une amende.

"Un réseau inédit par son ampleur et son audace."
SRPT (Service régional de la police des transports)

DVD JON NE S'ARRÊTE JAMAIS

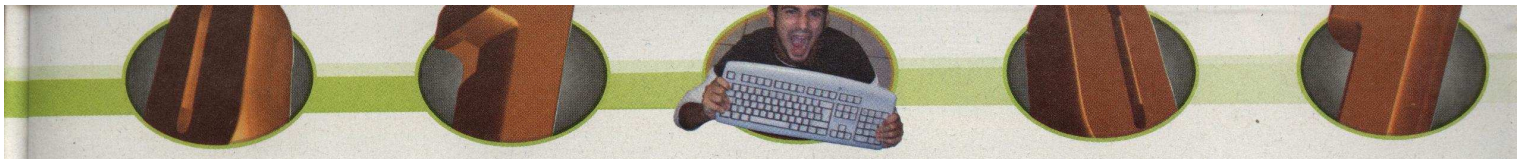
Le célèbre Norvégien Jon Lech Johansen, qui avait hacké en son temps la protection CSS des DVD, la plate-forme de musique en ligne iTunes et plus récemment le lecteur vidéo de Google, a encore frappé. Il vient en effet de faire sauter la protection NSC de Windows Media Player. Cette dernière crypte les informations inhérentes aux flux distribués en streaming. La protection masque l'adresse IP du serveur, le port, le format d'échange, etc. Dorénavant, il est possible de lire ce genre de flux avec d'autres logiciels, comme VLC Media Player. Comme le dit DVD Jon : "Windows Media Player n'est pas très bon, et les utilisateurs Windows et Mac ne devraient pas être forcés de l'employer pour visionner les flux NSC".

>> MICROSOFT CONTRE LA COMMISSION EUROPÉENNE

Microsoft dépose un recours devant la Cour européenne de justice. Cette action découle du jugement datant de mars 2004 pour "position dominante et concurrence déloyale". Microsoft avait été condamné à payer 497 millions d'euros et sommé de retirer Windows Media Player de ses systèmes d'exploitation en Europe. La commission avait aussi demandé à la firme au papillon de donner quelques informations sur le code source pour permettre à d'autres OS de cohabiter avec Windows sur une même machine. La sanction pourrait s'élever à 5 millions d'euros par jour de retard ! Microsoft ne l'entend pas de cette oreille et juge que la livraison d'une partie du code source atteint sa propriété intellectuelle, d'où le recours.

>> DES LYCÉENS PIRATENT LEURS NOTES

Comme dans le vieux film WarGames, des adolescents américains de 16 ans ont voulu faire les malins en piratant le système informatique de leur lycée. Ils y sont parvenus et se sont rendus coupables de manipulation de données en changeant les notes et diverses autres informations concernant leurs dossiers. Pour brouiller les pistes, ils ont aussi modifié certaines



ARNAQUE AUTOUR DE L'OURAGAN KATRINA

Après la vague d'émotion suscitée par le désastre de l'ouragan Katrina, le FBI met en garde les généreux donateurs. Beaucoup de faux sites se sont créés dernièrement avec les mots "katrina", "help" ou "disaster", etc. Le nombre de noms de domaine utilisant ces termes est en explosion ! Par exemple, pour le site katrinahelp.com personne ne sait où est passé l'argent. De plus,

les escrocs se servent d'e-mails pour leurs appels à la "générosité" et utilisent Paypal pour ne pas laisser de traces. Le même phénomène se produit aussi avec des propositions de reportages. Ces derniers sous couverts d'exclusivité vous incitent à updater votre OS ou votre logiciel de navigation. Bien sûr, il s'agit uniquement de manœuvres destinés à vous tromper. Si vous jouez leur jeu, vous pourriez bien vous faire inoculer des trojans, virus, etc. Le malheur des uns fait le bonheur des autres...

YAHOO COLLABORE AVEC LES AUTORITÉS CHINOISES

Le Yahoo de Hong Kong est accusé par Reporters sans Frontière d'avoir collaboré avec les autorités chinoises pour l'arrestation d'un journaliste dissident. Shi Tao,

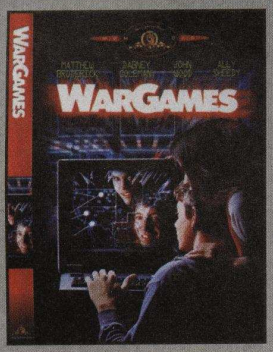
un homme de 37 ans, a en effet pris 10 ans de prison ferme pour "divulgation du secret d'État à l'étranger". Son seul crime est d'avoir fourni des messages, envoyés par le gouvernement chinois, à son journal économique.

HK Yahoo ! Holding apparaît dans le texte du verdict et a carrément piraté son e-mail et a permis la localisation de manière physique du journaliste ! "Déjà collaborateur zélé de la censure, Yahoo ! devient auxiliaire de la police chinoise", a déclaré dernièrement RSF. Pour sa défense, la société argue qu'elle se plie aux lois du pays où elle exerce... Certes, Yahoo est soumis à la législation hongkongaise mais celle-ci ne précise pas le régime de responsabilité des hébergeurs de mails dans ce type de situation ! Jusqu'où ira la société américaine pour s'attirer les faveurs du gouvernement de Pékin ?

UNE NOUVELLE CIBLE, PAS VRAIMENT NOUVELLE

Après avoir attaqué en justice des milliers d'internautes proposant des fichiers en téléchargement sur les réseaux peer-to-peer, la RIAA et ses équivalents européens ont trouvé une autre cible pour expliquer la chute des ventes de CD audio. En effet, s'attaquer uniquement au P2P devenait lassant et trop convenu ces derniers temps. Les majors se devaient de trouver un autre coupable vis-à-vis de l'opinion publique. Pas besoin d'aller chercher bien loin pour trouver la nouvelle tête de Turc, elle est connue depuis longtemps : c'est la gravure de CD ! Le président de la RIAA, Mitch Bainwol, a donc sorti des chiffres inquiétants lors d'une réunion à San Diego. Selon lui, l'année dernière, 29% de la musique dans le monde serait directement issue de la gravure alors que les réseaux P2P ne représenteraient que 16%. Voilà qui réjouira les P2Pistes qui ne seront plus désormais désignés comme les principaux meurtriers des artistes «Universal». Premièrement, on peut se demander comment la RIAA peut avancer des chiffres aussi précis. Il est aussi intéressant de noter que la RIAA semble littéralement redécouvrir le phénomène de la copie de CD. Heureusement pour Mitch et ses compères, il existe plusieurs protections qui n'autoriseront qu'un nombre limité de copies. Espérons tout de même que ces dernières ne seront pas de la même veine que celles qui sévissaient en France il y a quelques années...

informations de quelques-uns de leur camarade. Les personnes en charge de l'informatique s'en sont rendu compte et les apprentis Mitnick se sont fait attraper le plus



simplement du monde grâce aux logs serveur. Et comme le crime ne paie pas, les tricheurs se sont retrouvés en maison de redressement.

>> BUSH ET LE P2P

Scott McClellan, le porte-parole de la maison blanche a dernièrement annoncé que le président des Etats-Unis "*pense que les personnes qui produisent du matériel légal ne doivent pas être incriminés à la place des personnes utilisant ces produits à des fins criminelles*". Le président faisait-il allusion à l'affaire Grokster ? Est-il contre la position du tribunal qui a déterminé que le logiciel P2P encourageait le piratage ? Pas du tout, George parlait en fait des armes à feux ! Effectivement, cela n'a rien à voir : le P2P est bien plus dangereux !

DES FAILLES EN RAFALES

Une description complète de l'algorithme MD5 (Message Digest 5) se trouve à l'adresse www.faqs.org/rfcs/rfc1321. Cependant, quatre chercheurs chinois ont produit un document dans lequel ils démontrent que l'on peut contourner ce cryptage. Ainsi, d'après eux, il serait tout à fait possible d'obtenir, à partir de deux documents différents, deux signatures identiques. Ce qui, évidemment, jette le discrédit sur cette méthode cryptographique.
Que se passerait-il si nous parvenions à prouver, devant un juge par exemple, que notre signature a pu être contrefaite sur un document ? De même, imaginons que nous téléchargions un fichier sur Internet en pensant être protégés par une chaîne de caractères MD5 et qu'au lieu de cela nous récupérions un cheval de Troie ayant la même signature que le fichier recherché.

Si les chercheurs chinois ont raison, alors il serait préférable de retirer et vérifier les milliers, plus vraisemblablement les millions, de fichiers MD5 ainsi que leurs fichiers d'origine, et de les remplacer par un algorithme plus sécurisé. Difficile de s'y retrouver dans tout cela ! D'autant plus que deux autres chercheurs, israéliens cette fois (Eli Biham et Rafi Chen) ont démontré cette année que l'algorithme SHA-1, l'un des plus connus et des plus sûrs, présentait des failles jusqu'à présent inconnues. Ceci impliquerait, par exemple, que même les programmes PGP et SSL ne peuvent plus être considérés comme infaillibles. L'institut national des standards américains, quant à elle, a démontré que SHA-1 était un algorithme sûr, en générant une chaîne de caractères en sortie d'une longueur de 160 bits. Alors, vulnérable ou pas ?

Les algorithmes MD5 et SHA-1 étaient jusqu'à présent considérés à toute épreuve, parce qu'un seul changement dans le message d'origine doit normalement engendrer une empreinte numérique complètement différente, que l'on parte d'un courriel ou d'un fichier du système d'exploitation. Mais il semblerait

Le MD5 consiste en une sorte de synthèse qui convertit, grâce à un calcul mathématique, un message de longueur arbitraire en une empreinte numérique d'une longueur de 128 bits, que nous pensions unique... jusqu'à aujourd'hui.

que ce ne soit pas le cas. À l'heure actuelle, on ne peut plus affirmer que ces deux méthodes de cryptage assurent une parfaite sécurité.
En pratique, ces failles permettraient de cloner les signatures numériques avec une opération engendrant des " collisions ", c'est-à-dire un résultat erroné. Même si l'on sait qu'aucun algorithme n'est fiable à cent pour cent, on a toujours cru que cela pouvait être dû au temps nécessaire pour effectuer la fonction de hachage cryptographique. Dès le début, quelqu'un aurait pu savoir que le MD5 est basé sur des algorithmes mathématiques non sécurisés. Malgré tout, il reste populaire et il est encore très utilisé, notamment comme outil de vérification pour les téléchargements.

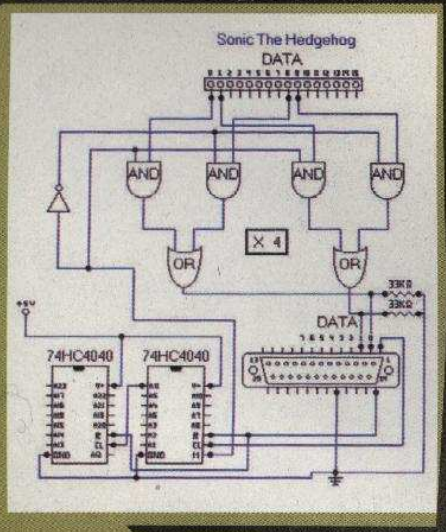
Le système SHA-1 (Secure Hash Algorithm) demande à l'ordinateur qui le calcule de faire tourner les routines dont il est constitué au moins 80 fois, jusqu'à créer une signature univoque. Biham, le chercheur israélien, a réussi à copier une signature numérique en seulement 30 passages sur les 80 prévus ! Si, en approfondissant les vulnérabilités de SHA-1, l'on découvrait des failles analogues à celles qui ont fait abandonner la précédente version, SHA-0, il suffirait d'un réseau restreint de PC pour déchiffrer en peu de temps n'importe quelle application basée sur l'algorithme en question.
D'autre part, les failles de MD5 pourraient impliquer énormément de serveurs, par exemple ceux qui se servent d'Apache Web Server, lequel utilise la fonction MD5 pour assurer aux utilisateurs que les codes sources des sites miroir renferment des fichiers identiques aux originaux et qu'ils peuvent donc être téléchargés en toute sécurité.

Un système tel que le " Solaris Fingerprint Database ", outil qui garantit la sécurité des fichiers du système d'exploitation Solaris, entièrement basé sur MD5, pourrait de ce fait se retrouver dans une situation embarrassante : celle d'avoir à expliquer à ses utilisateurs comment garantir l'aspect unique de leurs propres fichiers... à l'aide d'un algorithme réputé engendrer des clones assez facilement !
En ce qui concerne le MD5, aux dires des chercheurs, il suffit de quelques heures à un PC classique pour dupliquer n'importe quelle signature numérique. On savait déjà ne pas être en totale sécurité, mais à ce niveau-là les choses deviennent vraiment sérieuses. D'autant que les documents concernant la vulnérabilité des différents protocoles sont du domaine public, n'importe qui peut s'en servir pour lancer des attaques. C'est quelque chose qu'il faut désormais prendre en compte.

RESSUSCITER LES ANCIENS JEUX

L'émulation est la possibilité de faire tourner sur un PC des jeux conçus pour d'autres machines. La " copie " est tellement proche de l'original que l'on croirait presque jouer avec le jeu d'origine ; ceci grâce à l'émulateur, un programme imitant le fonctionnement de la machine en question, une GameBoy par exemple.. Développer un émulateur consiste à reproduire sur le disque dur d'un PC l'architecture d'une console de jeu. Lorsque nous chargeons sur notre PC l'émulateur d'une GameBoy, l'interface qui apparaît à l'écran est identique à celle d'une véritable GameBoy, et nous pouvons jouer comme nous le ferions avec la console elle-même. Pourtant, le " moteur " est tout autre.

Tous les ordinateurs actuels sont conçus pour que les instructions des programmes et les données soient conservées en mémoire pour ensuite être lues afin d'exécuter certaines fonctions. De même, la GameBoy, comme tout autre console, est



EST-CE AUTORISE

Pour les consoles qui ne sont plus produites, l'émulation est considérée comme un passe-temps inoffensif. Certains ont même essayé de vendre des émulateurs et des logiciels de consoles hors production (comme Sega l'avait fait). Comme pour les logiciels, on ne peut pas distribuer de copie d'émulateur, on peut juste posséder une copie de sauvegarde personnelle. Sony, Nintendo et Sega ont des opinions différentes, en fonction du succès de leurs produits, mais en règle générale, c'est illégal. Par contre, la copie d'un BIOS est strictement protégée par les droits d'auteur. Certains émulateurs exigent que l'on possède le BIOS d'origine... dont le désassemblage (reverse engineering) est toujours interdit.

Sur le site zsnes.com (en anglais), on trouve un des quatre éléments utilisés pour copier les ROMS. Celui-ci fonctionne convenablement, piloté par des machines DOS pour lesquelles il a été conçu. Avec la sortie de Windows, les programmes pour lire les ports sont devenus plus complexes.

Si beaucoup d'anciens jeux de console ont été reproduits sur PC, ce n'est pas un hasard. C'est que le plaisir de jouer à des jeux qui ont connu, en leur temps, leur heure de gloire est toujours intact. Cependant, l'émulation représente beaucoup de travail.

Un lecteur et un graveur de cartouches GameBoy. Si l'on n'est pas expert en circuits et en montages électroniques, mieux vaut ne pas s'y risquer ! Les choses ne sont plus aussi simples qu'avant.

dotée d'une mémoire renfermant des données et des programmes. Comme sur un PC, le BIOS contient les informations qui font fonctionner le système. Une autre mémoire, souvent amovible, renferme une série d'instructions et/ou de données qui permettent de jouer à un jeu bien précis : c'est la cartouche ou le CD-Rom du jeu. Donc, si nous voulons émuler une machine sur ordinateur, il nous faut la mémoire de cette machine. Par exemple, pour émuler un Mac sur PC, nous devons récupérer l'image du BIOS du Mac et élaborer autour de celle-ci un programme imitant le fonctionnement du Mac. Ensuite, lorsque l'émulateur est au point, nous pouvons nous procurer des images de logiciels tournant sur Mac, pour les utiliser sur PC. Pour les consoles plus complexes, comme la PlayStation, le support de mémoire externe est un CD. Donc, après avoir élaboré l'émulateur de PlayStation, nous devons nous procurer les images des CD, sous forme de fichiers ISO.

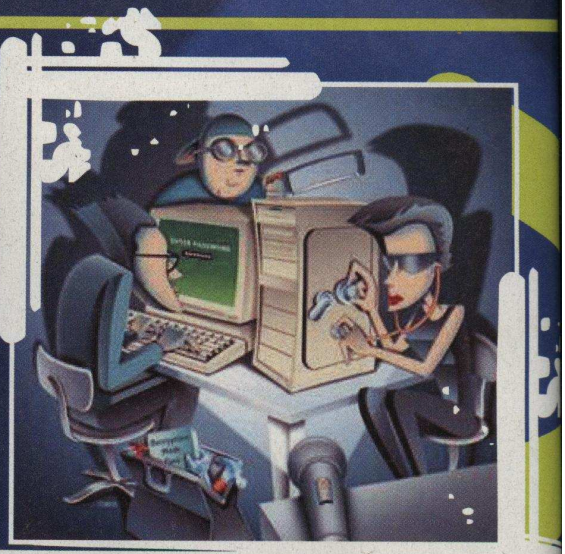
Pas si simple

Tout ceci semble facile, mais en pratique deux problèmes se posent : comment concevoir un émulateur ? Et comment se procurer l'image d'une mémoire ? Nous ne nous attarderons pas sur la première question, qui est vaste, sachez seulement qu'il s'agit d'un véritable travail de programmation qui demande du temps et de la patience, comme pour la création de n'importe quel logiciel. Toutes les informations matérielles de la console à émuler sont obtenues par désassemblage, et aussi par la récupération de données sur Internet. Dans la plupart des cas, surtout pour les machines de bar d'autrefois et pour les consoles les plus simples, les jeux sont contenus dans des ROMS interchangeables.

OU TROUVER LES EMULATEURS

Dans un ancien numéro de Hackers Magazine (N°5), pour plus de facilité, sur un CD sont regroupés les principaux émulateurs des consoles de jeu les plus connues. D'autres sont disponibles sur le Web.

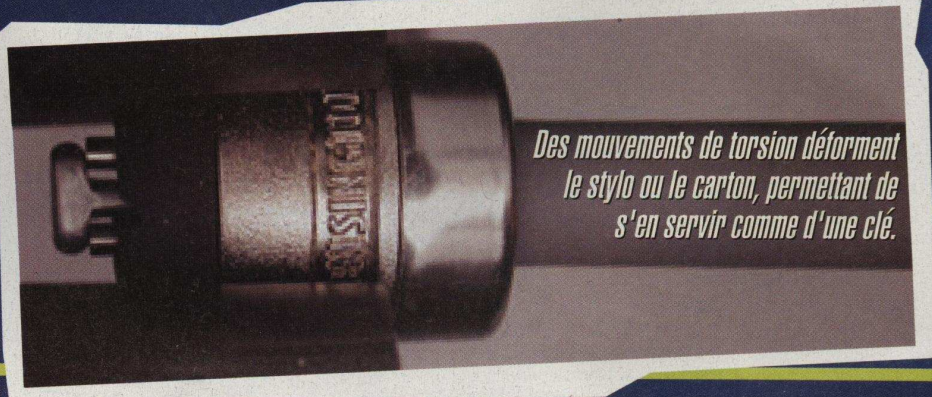
COMMENT OUVRIR UN CABLE DE SECURITE KENSINGTON ?



Très répandu, ce type de câble est utilisé contre le vol des ordinateurs portables et parfois même des ordinateurs de bureau. Il suffit de faire passer le câble en acier entre les pieds et le plateau du bureau et de le relier à l'encoche sécurité (ou slot antivol) de l'ordinateur par l'intermédiaire d'un cadenas à clé ou à combinaison. Les câbles Kensington (les plus connus) sont solides, mais le système de fermeture n'est cependant pas infaillible !

Cinquante secondes et un euro suffisent pour forcer un tel cadenas. On voit bien les cinq points du mécanisme.

Ceux qui utilisent ce type de cadenas doivent savoir qu'on peut l'ouvrir en trente secondes seulement. La serrure du cadenas a le même diamètre qu'un stylo à bille Flexgrip Papermate. Il suffit d'insérer le stylo selon un angle de quatre-vingt-dix degrés par rapport à la face avant du cadenas, puis de faire levier en appuyant vers l'intérieur du mécanisme. Ensuite, sans modifier la position du stylo à l'intérieur du cadenas, on fait levier dans la direction d'un autre point. En tout, il y a cinq points à aligner pour l'ouverture du cadenas. L'opération



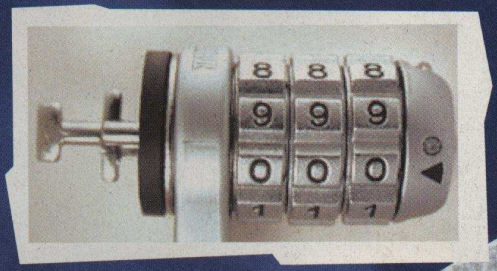
Des mouvements de torsion déforment le stylo ou le carton, permettant de s'en servir comme d'une clé.

Que peut-on faire avec un cylindre en carton ou un stylo à bille ? On peut ouvrir un antivol Kensington !

ComboSaver

Les cadenas à combinaison sont-ils plus sécurisés ? Non seulement ces cadenas s'ouvrent également rapidement et sans difficulté, mais en plus une main habile peut parvenir à changer de combinaison sans ouvrir le cadenas ! Dans ce cas, le cadenas reste fermé, mais le propriétaire de l'ordinateur ne peut plus l'ouvrir ; il devra deviner la nouvelle combinaison parmi les mille possibles...
Le ComboSaver de Kensington est programmable grâce à un levier situé sur l'arrière du cadenas.
Lorsqu'un point vert apparaît, c'est que le levier est en position fermée. Lorsque le point est rouge, le cadenas n'est pas fermé : les coulisses se déplacent légèrement vers l'avant ; c'est à ce moment-là qu'une effraction est possible.

À l'intérieur du mécanisme, deux disques s'alignent sur une barre mobile

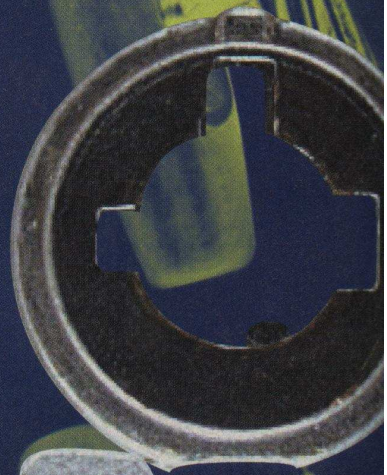


Un ComboSaver en position ouverte ou fermée.

reliée au verrou en forme de T connecté à l'ordinateur portable. Lorsque le ComboSaver est fermé, la barre coulisse vers le cadenas ; lorsqu'il est ouvert (levier faisant apparaître un point rouge), on peut pousser la barre légèrement en avant et la tourner, ce qui fait changer sa position à l'intérieur du mécanisme et bouger la molette correspondante. Après avoir positionné le levier sur le point vert, la nouvelle combinaison est activée !

Si la combinaison est, par exemple, 153 (chiffre lu dans le sens ordinateur-levier) : en regardant bien la position de la première molette (lorsque le levier est sur point vert), on parvient à distinguer le chiffre 3 et à la déplacer de sorte que ce chiffre soit indiqué également par la petite flèche. On met alors le levier sur le rouge et, en exerçant une pression, on déplace la molette du milieu jusqu'à ce que l'on trouve, au toucher, le deuxième chiffre de la combinaison. En faisant à nouveau pression sur le levier, on trouvera également le troisième chiffre. Si ce n'est pas le cas, il faut effectuer un tour de cinq chiffres.

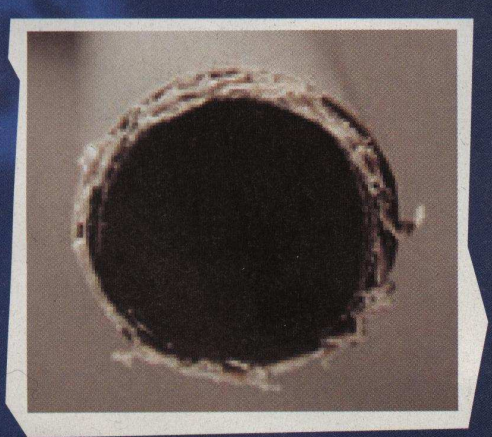
NeOkOn



L'intérieur du mécanisme : chaque chiffre de la combinaison est indiqué par le positionnement de la molette. Toutefois, on peut intervenir sur cette disposition... à l'insu du propriétaire.

permet d'imprimer ces cinq points sur le stylo qui, au final, a pris la forme exacte de la clé. Il ne reste plus qu'à ouvrir le cadenas.

Un autre système, toujours basé sur le même mécanisme. On enroule un carton assez solide autour d'un stylo bille, puis on procède aux mêmes mouvements de torsion que précédemment, afin de le déformer. Cette solution requiert de l'habileté manuelle, mais fonctionne tout aussi bien.



Des SIGNATURES utilisant la 3D

Les temps sont durs pour les faussaires. Bientôt, il ne suffira plus d'être capable d'imiter la signature des chèques, cartes bleues et papiers d'identité. Les faussaires devront aussi être à même de reproduire le profil 3D d'une signature.

Dans l'éternelle guerre entre la justice et les voleurs, la technologie est en train de porter un coup significatif aux faussaires, et surtout à ceux qui imitent les signatures afin de s'approprier l'identité d'autrui pour pirater les comptes en banque.
L'écriture n'est pas seulement bidimensionnelle, caractérisée par sa hauteur et sa largeur ; celui qui écrit exerce aussi une pression sur le papier. Cette pression laisse une trace qui est personnelle à chaque scripteur et dont la profondeur peut être mesurée. Cet aspect tridimensionnel de l'écriture est déjà largement pris en compte dans les analyses graphologiques, mais dans une perspective globale de compréhension de la personnalité du scripteur.
Grâce à la microprofilométrie, on pourra désormais reconnaître une écriture, et ainsi repérer les contrefaçons, en analysant la trace 3D du message.

La microprofilométrie

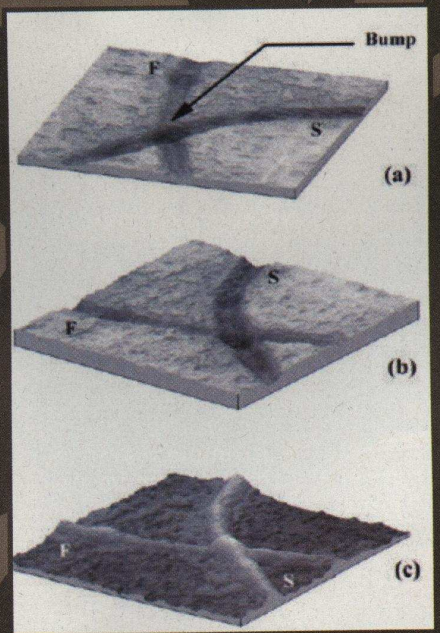
Cette nouvelle technique, appelée " microprofilométrie 3D ", est actuellement à l'étude à l'université italienne Rome3. Selon les chercheurs, elle pourrait avoir un rôle fondamental dans la lutte contre les faussaires. La première étape consiste à réaliser un modèle tridimensionnel de la pression exercée lors de l'écriture. En effet, une signature en trois dimensions donne davantage d'informations que son simple tracé encré (en deux dimensions). La troisième dimension, trace " en creux " de la signature, est donc une indication déterminante pour la reconnaissance de celle-ci. Le modèle 3D permet de la reproduire tout en garantissant de conserver intact le tracé au stylo.
Les applications de la microprofilométrie sont nombreuses. Elle peut être utile notamment lorsque l'on ne peut plus disposer de la signature de son auteur légitime : décès, voyage, maladie invalidante. Dans ce cas, le modèle 3D permet de conserver l'intégrité de l'échantillon.

Adieu calquage

Les faussaires qui imitent les écritures utilisent le calquage, et aussi d'autres méthodes évoluées de copie à main levée. Avec la 3D, leur mission devient impossible ! En règle générale, le faussaire dispose de peu de temps et de peu de moyens. Dans ces conditions, il arrive rarement à reproduire le profil 3D d'une signature. Dans le cas contraire, il pourrait suffire, à l'expert de la police, de quelques heures d'analyse pour obtenir un résultat incontestable et sans ambiguïté.
Les premières applications de la microprofilométrie 3D semblent assez prometteuses. En effet, le pourcentage de reconnaissance correcte dépasse déjà les 90%, sur un corpus expérimental de 126 lettres écrites par autant d'auteurs différents, avec divers instruments tels que stylo à bille ou feutre, et sur des supports allant du papier ordinaire au carton. La trace laissée par l'écriture au stylo à bille sur du carton étant la combinaison la plus simple, celle qui permet la reconnaissance avec une certitude quasi absolue.
En résumé, grâce à la signature 3D, on peut espérer qu'à l'avenir le vol de cartes de crédit ou d'autres documents sensibles causera moins de dégâts.

Reed Wright

Les technologies les plus avançées permettront de former une nouvelle race de faussaires plus évolués, qui maitriseront notamment la reproduction des signatures 3D.



Le matériel utilisé pour relever les traces 3D de l'écriture à main levée : entre autres, un laser et un module conoscopique. Les technologies les plus avancées permettront de vaincre les faussaires qui s'approprient la signature d'autrui.

Quelques conseils pour les espions et les espionnes

Comment vivre en toute tranquillité sans se faire remarquer

Qui peut bien avoir intérêt à nous épier ? Tout dépend de notre identité et de notre activité. Il existe plusieurs types d'espions potentiels : copain envieux, femme jalouse, collègue vexé ou maniaque. Les raisons peuvent être multiples, comme l'argent, le pouvoir ou le simple amusement. Sachez-le : on peut se protéger en raisonnant comme un véritable espion !

Certaines techniques d'espionnage semblent évidentes. Néanmoins, il faut bien y réfléchir : en connaissant à l'avance les méthodes utilisées pour nous espionner, nous serons en mesure de nous préparer.

Le dumpster diving

Notre corbeille contient des informations confidentielles : relevés de compte, reçus, billets de visite, vieux carnets de notes ou d'adresses, etc. La loi a tout à fait le droit d'aller y mettre son nez... et quiconque peut les récupérer et s'en servir. L'unique moyen de se protéger est donc de détruire ces documents.

Les puces espionnes

Combien de gens savent que l'on peut écouter à travers les murs avec du matériel approprié ? Le choix des micros espions est aussi varié que celui des micros téléphoniques. On peut en trouver quelques exemples à la page http://www.microspie.net/shopping/?id=9 : stylos, calculatrices, cendriers, pantoufles ou horloges murales, tout y est ! Seul un expert peut savoir s'il est surveillé ou pas. Les autres peuvent se procurer un détecteur, comme celui que l'on trouve à l'adresse http://www.micro-

GADGETS D'ESPION

Un des plus importants revendeurs italiens d'appareillages pour espionnage est "Endoacustica" à Bari. Ses produits se trouvent à l'adresse http://www.endoacustica.com et permettent aux espions d'opérer. C'est à ceux qui ne souhaitent pas être espionnés de réagir ! Les images de cet article se réfèrent à des produits qui sont tous disponibles sur le site d'Endoacustica.

Des lunettes pas comme les autres. Celles-ci sont équipées d'une caméra cachée, qui permet de transmettre les images par ondes radio vers un écouteur dissimulé.

spie.net/shopping/?id=13, et surtout rester sur leurs gardes…

À la pêche aux d'informations

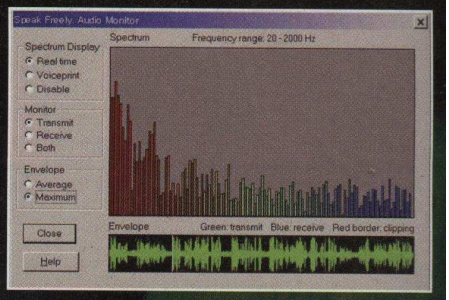
Il existe une technique insidieuse qui consiste à reconstituer un puzzle, information après information, pour mieux cerner un individu. Les gens aiment se donner de l'importance en racontant autour d'eux ce qu'ils savent. La règle d'or est de parler le moins possible de soi et de laisser parler les autres… voire de les y encourager. Celui qui parle à tort et à travers est un piégé en puissance, tandis que celui qui se tait ou ne parle qu'à bon escient donne peu de prise aux éventuels espions.

Se méfier de son ordinateur

Nous confions à notre ordinateur une grande partie de nos secrets. Par conséquent, il faut adopter une attitude responsable, afin de minimiser les risques d'espionnage. Les principes de base : faire preuve de bon sens, ne pas accepter de document ou programme si l'on ne connaît pas l'expéditeur, ne jamais cliquer à l'aveuglette sur tous les liens qui se présentent.
Si nos données sont confidentielles, cryptons-les avec PGP (http://www.pgp.org). Dissimulons nos dossiers et fichiers confidentiels avec un programme de type Hide Folders XP, http://www.fspro.net/hfxp/.
Il faut se méfier des keyloggers, ces programmes qui enregistrent nos frappes au clavier. Si l'on a des raisons de penser que l'on abrite un tel intrus, ne pas hésiter à installer un programme comme Anti-Keylogger (http://www.anti-keyloggers.com/).

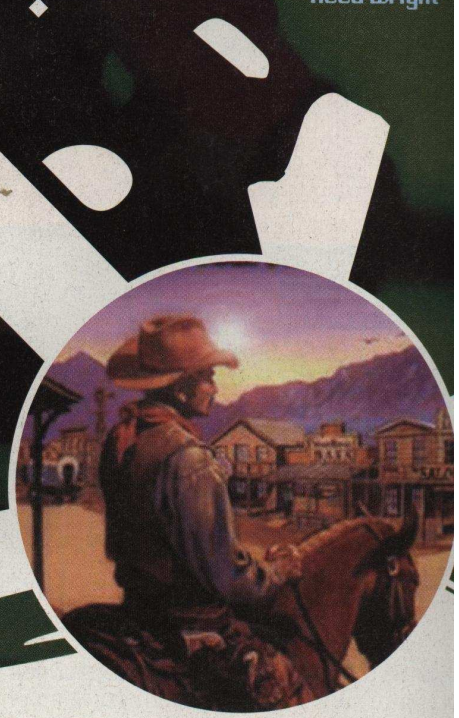
Les téléphones sur écoute

Contrairement à ce que l'on pourrait croire, les portables et les téléphones sans fil sont très facilement interceptables, grâce à des appareillages sophistiqués. Les communications se faisant par ondes radio, il suffit d'avoir la bonne antenne et le bon circuit. Le seul moyen de se protéger est d'acquérir un appareil qui, grâce à des processus de cryptage et de décryptage du signal, brouille la communication (pour les oreilles curieuses seulement). Il est très cher, mais efficace.



Sinon, nous pouvons téléphoner en passant par Internet et protéger nos conversations grâce à un logiciel de brouillage téléphonique tel que Speak Freely. (http://www.speakfreely.org/).
Le cas échéant, utilisons des téléphones filaires.

Reed Wright

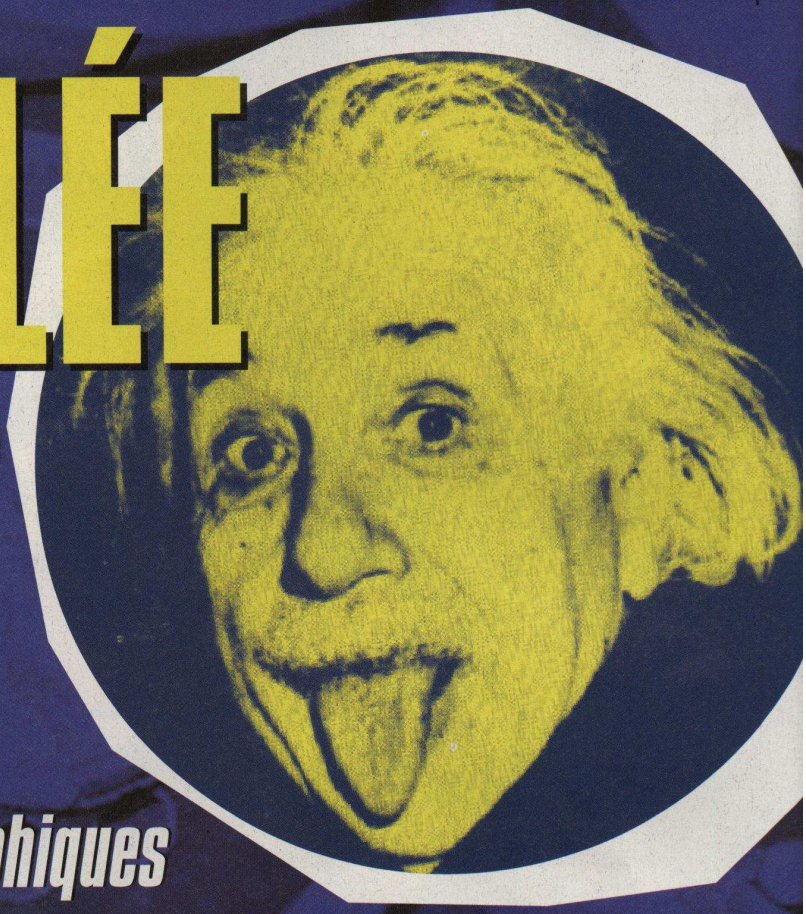


LA LOI DU PLUS FORT

En Italie, des lois sur l'espionnage électronique n'existent pas. Il y a seulement la ridicule loi 675/1996 sur l'intimité et la loi 98 de 1974, qui traite vaguement de l'utilisation d'appareillages à des fins de surveillance, mais l'on ne parle nulle part de manière explicite d'espionnage.

Ce qui est important n'est pas de connaître les moyens employés pour espionner, mais plutôt d'en connaître la raison. L'espion qui veut justifier ses opérations peut le faire librement, c'est à nous d'être vigilant.

LA CRYPTANALYSE DÉVOILÉE



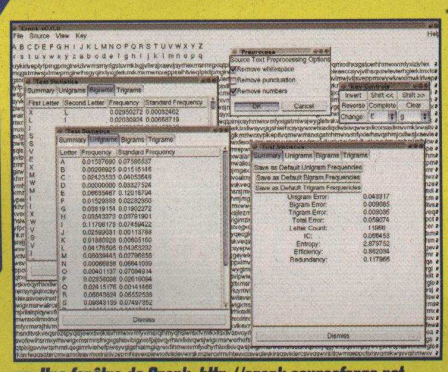
Comment s'approprier facilement la science du déchiffrage des algorithmes cryptographiques et des textes codés ?

Pendant la Seconde Guerre mondiale, les Anglais, aux prises avec les messages produits par la machine de cryptage allemande " Enigma " ont utilisé la cryptanalyse.

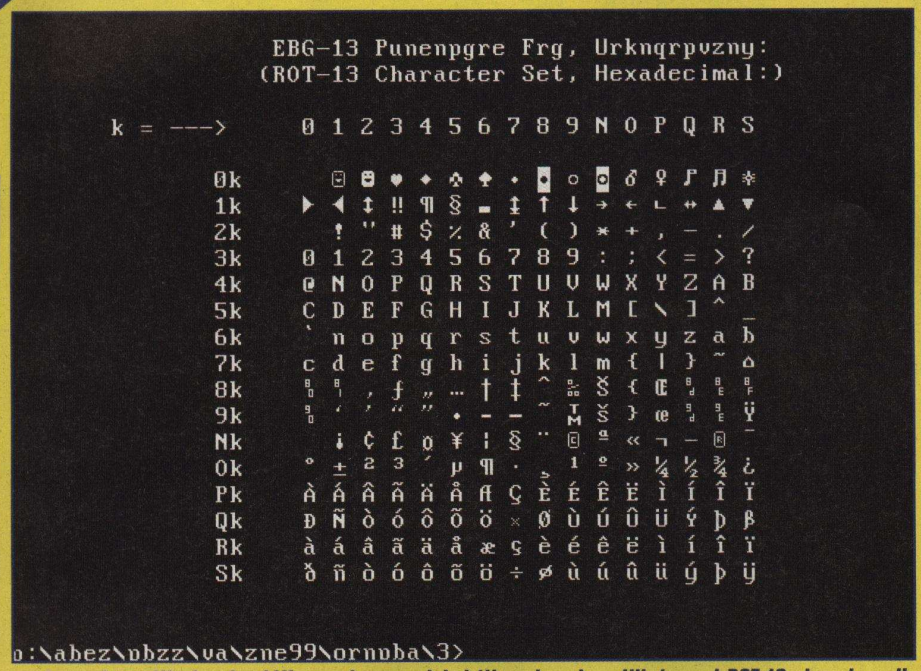
En français les voyelles sont les plus utilisées

La première étape dans la compréhension de la cryptanalyse consiste à saisir le concept de la fréquence de distribution des caractères dans un texte. Par exemple, en italien les lettres les plus utilisées sont les voyelles, excepté la lettre U. En anglais, les lettres les plus utilisées sont, par ordre décroissant, ETAOINSHRDLU. La fréquence d'apparition des caractères est à la base de la cryptanalyse : certaines lettres apparaissent plus souvent que d'autres et la situation diffère dans chaque langue. Si, dans un fichier chiffré, certaines lettres sont répétées plus souvent que d'autres, les fréquences deviennent un premier indice très précieux.

Un texte simplement chiffré avec un procédé de chiffrement par substitution mono alphabétique, dans lequel chaque lettre est



❑ *Une fenêtre de Crank, http://crank.sourceforge.net, logiciel open source pour Windows spécialisé dans la cryptanalyse.*



❑ *L'une des méthodes de chiffrement mono alphabétique les plus utilisées est ROT-13, dans laquelle chacun des caractères est codé par un déplacement de treize rangs dans l'alphabet.*

remplacée toujours par la même lettre, s'avère peu résistant face à l'analyse des fréquences. Plus le texte est long et plus l'analyse des fréquences sera précise. Bien évidemment, des procédés de chiffrement plus compliqués permettent de changer la donne.
La cryptanalyse de base peut également servir à étudier, non plus la fréquence des lettres individuelles, mais celle des suites de deux lettres (digrammes) et de trois lettres (trigrammes).
Voyons plus en détail quelques principes de base.

Exemple

Supposons que nous utilisions un simple procédé de chiffrement mono alphabétique et que nous remplacions chaque lettre de l'alphabet italien par celle qui se trouve dans le diagramme suivant :

Le texte PROVADICIFRATURA (TESTDECHIFFREMENT) est converti en GRPVEOCFCNREMZRE. Ce texte est très court, mais il est évident que l'on retrouve certaines lettres plus souvent que d'autres : A, E, I, O, T (en italien). C'est pour cette raison que la première chose à faire, lorsque l'on pense être confronté à un procédé de chiffrement mono alphabétique, est d'agir sur les lettres que l'on retrouve le plus souvent en espérant qu'elles puissent correspondre, dans le texte en clair, aux lettres les plus utilisées (en italien ou dans une autre langue).

Analyse approfondie

Les digrammes et les trigrammes servent à affiner l'analyse, les répétitions de suites de deux et trois lettres étant plus révélatrices. Par exemple, si les deux premières lettres en clair d'un trigramme sont S et T, il faut choisir la troisième parmi un choix restreint de possibilités. Cela ne peut pas être un Z, un Q, ni un C, etc., donc ce pourrait très bien être une voyelle, ou un R (par exemple).

À partir de là, comment procède-t-on pour élaborer une méthode de chiffrement plus simple et plus résistante, à même d'échapper à une simple analyse cryptanalytique ? Il faut, bien évidemment, faire en sorte que, dans le texte chiffré, la fréquence de répétition des lettres ne donne pas d'indices... Oui, mais comment faire ?

P. Mersenne

❑ *Jules César, indépendamment de conquérir la Gaule, a donné son nom à la plus simple des méthodes de chiffrement mono alphabétique.*

A B C D E F G H I L M N O P Q R S T U V Z
E S F O A N T B C Q U D P G H R I M Z V L

FREEBSD

CONNAISSEZ-VOUS FreeBSD ?

Linux est une galaxie importante dans l'univers du logiciel libre. C'est aussi une des plus intéressantes.

Pour ceux qui ne le sauraient pas encore : il existe des alternatives à Windows, et pas seulement Macintosh et Linux. Parmi tous les systèmes d'exploitation qui s'offrent à nous, FreeBSD est puissant, sûr, libre et gratuit.

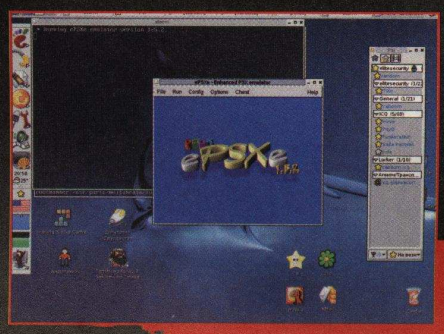
Il est issu d'Unix, comme Linux, mais il est sorti bien avant. Basé sur le système BSD, il a été créé en Californie à l'université de Berkeley, près de San Francisco.

Il fonctionne partout

FreeBSD fonctionne pratiquement sur n'importe quel processeur : Pentium, Athlon, AMD, Opteron, EM467, et même sur le PowerPC des Macintosh et Alpha, Itanium, PC-98, UltraSPARC, MIPS, et ainsi de suite. Il n'y a pas d'ordinateurs produits ces dix dernières années qui n'acceptent FreeBSD.

Comment l'utiliser ?

Étant un système de type Unix, FreeBSD peut être utilisé à partir de l'interface graphique ou bien en lignes de commande dans un interpréteur de commande (ou " shell "). Ceux qui ont



FreeBSD The Power to Serve
www.FreeBSD.org

testé Mac OS X ou Linux savent très bien de quoi il s'agit. Sur Windows également il existe un environnement similaire : l'invite de commande MS-DOS.

Que peut-on faire ? On peut tout faire avec FreeBSD (dont la devise est "the power to serve", le pouvoir de servir). Les plus célèbres programmes open source sont sur FreeeBSD : OpenOffice, qui peut lire tous les documents créés avec Office de Microsoft ; le navigateur Mozilla ; Gnome, par exemple, pour l'environnement de bureau, etc.

Des exemples de commande

En supposant que l'on utilise l'interpréteur de commande et non l'interface graphique, voici quelques exemples de commande à donner. Selon la tradition Unix, % indique ce qui est tapé par l'utilisateur lambda, et # correspond au root, c'est-à-dire au compte administrateur.

% adduser
Permet d'ajouter un nouvel utilisateur

% exit
Permet d'exécuter le logout, c'est-à-dire de quitter un système, de s'en déconnecter

% id
Permet de s'identifier au sein du système

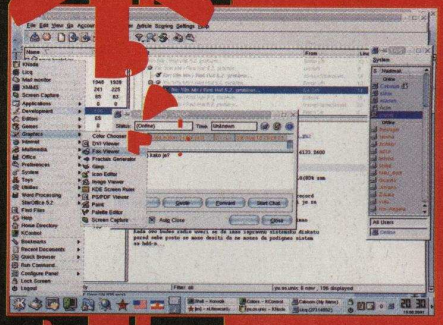
% pwd (print working directory)
Indique le répertoire de travail courant

% ls
Énumère les fichiers dans le répertoire courant

% cat
Fait apparaître le contenu d'un fichier sur l'écran

% apropos
Permet de consulter la base de données uhatis et indique les commandes qui ont une certaine fonction

% rm
Permet de supprimer les fichiers



Ceux qui connaissent Linux ou Mac OS X s'apercevront qu'il n'y a pas énormément de différences entre les deux, sinon pas du tout.

Mais alors, demanderont certains, pourquoi ne pas utiliser Linux ou Mac OS X ? Parce que la diversité favorise l'évolution, parce que FreeBSD a un moteur interne (le kernel) assez différent de Linux, ce qui le rend plus sûr. En outre, savoir utiliser plusieurs systèmes d'exploitation est comme de connaître plusieurs langues, cela permet de maintenir notre cerveau en forme. Pour nous, hackers, c'est fondamental !

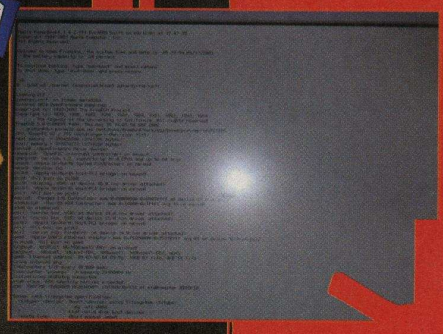
Nous reparlerons bientôt, plus en détail, de FreeBSD. Que ceux qui sont intéressés le fassent savoir !

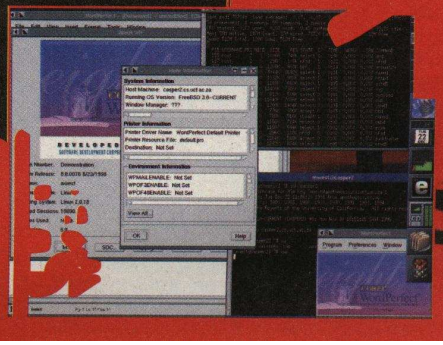
Beth i5b3773r@mac.com

L'ESSENTIEL SUR FREEBSD

Le site de référence de FreeBSD est bien sûr http://www.freebsd.org (que l'on peut consulter aussi en français !), On y trouve également la liste des plates-formes supportées et de nombreux liens vers les ressources les plus diverses, parmi lesquelles les programmes utilisables et les FAQ, en plus d'une liste de programmes déjà prêts (http://www.freebsd.org/applications.html) et supportés par d'autres plates-formes (http://www.freebsd.org/ports/index.html).
À l'adresse http://www.freebsd.org/projects/newbies.html, on trouve même un lien réservé aux nouveaux venus dans la galaxie Unix et FreeBSD.

Pour installer FreeBSD, il faut aller à l'adresse : http://www.freebsd.org/doc/en_US.ISO8859- 1/books/handbook/mirrors.html. Avec une connexion rapide, l'installation peut se faire avec plusieurs disquettes.





LES FAILLES DES KIOSQUES

Depuis quelques années, on trouve dans de nombreux lieux publics des terminaux, appelés " kiosques ", avec lesquels on peut accéder à différents services.

Ceux installés dans les bibliothèques, par exemple, sont très utiles pour accéder aux catalogues en ligne afin d'y trouver des livres et des produits multimédias.

Ces terminaux permettent de surfer sur Internet de manière très réglementée. Le gérant du kiosque a la possibilité d'autoriser l'accès uniquement à certains sites bien ciblés, généralement sur les sujets relatifs à l'utilisation du kiosque, ou bien à des services qui sont considérés utiles pour l'utilisateur. Dans le cas des bibliothèques, il est facile de parvenir à accéder à des sites d'organismes publics liés au lieu où le kiosque est installé. Autrement dit, il est possible de se rendre sur les sites institutionnels de la région, de la mairie, ou sur ceux de certains ministères et associations culturelles, par exemple.

Par contre, la navigation libre est presque toujours interdite. Par obligation légale (et comme pour tout autre point d'accès à Internet ouvert au public), le gérant du kiosque doit être en mesure d'identifier les utilisateurs. Ceci afin d'éviter, ou de décourager, les utilisations illégales telles que le spamming ou les téléchargements illégaux de fichiers.

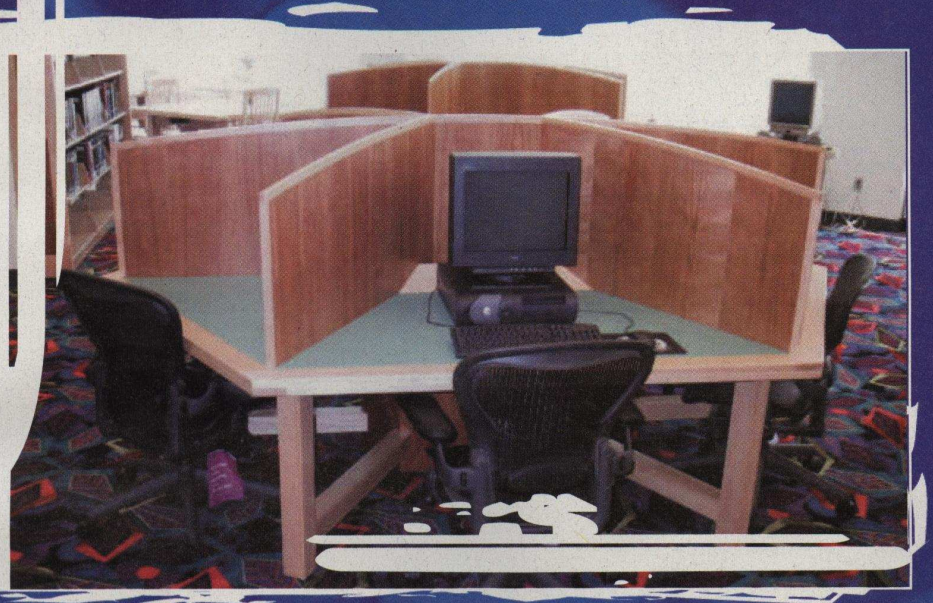
Un exploit imprévu

Beaucoup de ces systèmes autonomes installés dans les lieux publics sont basés sur SiteKiosk, un programme disponible à l'adresse www.sitekiosk.com, distribué également en version shareware, ce qui permet de le tester. Dans la pratique, il peut arriver que le programme en question soit mal configuré. En particulier, la configuration incorrecte du système utilisé pour

EN RESEAU AUSSI !

Les kiosques publics ont généralement la particularité de ne pas être de véritables PC " stand-alone ", mais sont configurés pour accéder au même disque dur en réseau. Par conséquent, il y a de grandes chances pour que notre configuration nouvellement créée ait été installée sur le disque dur du serveur central. De cette façon, lors de prochaines sessions, nous pourrons toujours l'utiliser, car elle sera présente sur n'importe quel terminal connecté au même serveur, quel que soit l'endroit où il se trouve.

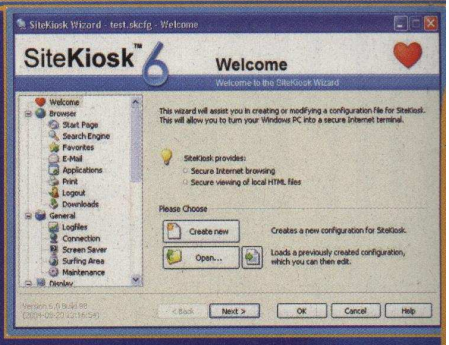
Les kiosques d'information publics sont des systèmes " blindés " qui ne permettent pas un accès libre à Internet. Mais en est-on aussi certain ? Parce qu'en pratique il est possible que ce ne soit pas toujours le cas...



blinder les terminaux vers l'extérieur et celle du système dans son ensemble permettrait de créer de nouvelles configurations, donc de lancer une fenêtre ayant sa propre configuration qui, évidemment, comprendrait la liberté de surfer sans restriction.

Une session alternative

Après avoir effectué quelques essais avec le logiciel, les choses pourraient se passer ainsi. Si, en réalité, nous nous apercevons qu'effectivement il est possible d'agir de cette manière, peut-être nous sentirons-nous tenus d'avertir le gérant du kiosque afin qu'il prenne les mesures nécessaires, en reconfigurant le système pour le sécuriser.
Voici la procédure. Assurons-nous d'abord que nous sommes sur la page d'accueil en cliquant sur " Start ", sur la barre en haut au centre. À partir de là, sélectionnons une des icônes affichées. Pour garder l'exemple de la bibliothèque, une icône serait probablement consacrée aux livres et une autre à la section multimédia. C'est le point de départ de la pénétration du système. Maintenant, sélectionnons un lien vers un site dont la visite est autorisée. Supposons que ce soit celui de la région dont dépend la bibliothèque : en général, ces systèmes sont souvent financés au niveau local ou régional. Lorsque nous avons atteint le site en question, cherchons n'importe quel document téléchargeable, par exemple un fichier PDF. Pour cela, nous pouvons utiliser la case de recherche, généralement toujours présente. Dans le champ " Rechercher ", il suffit de taper " pdf " ou " .pdf ", et ensuite de



sélectionner n'importe quel résultat parmi ceux obtenus, le but étant d'accéder au disque dur du terminal.
À la question " ouvrir le document ou le sauvegarder ? ", cliquons sur " Sauvegarder ", puis sur " c : \ " afin d'atteindre les répertoires " Programmes " et " SiteKiosk ". Dans le champ " Sauvegarder sous ", vérifions que soit précisé " Tous les fichiers ". Sélectionnons le fichier " Configure.exe " qui apparaît également, et choisissons " Ouvrir " avec un clic droit. Nous n'aurons évidemment pas l'autorisation de modifier les configurations existantes, mais rien ne nous empêche d'en créer une nouvelle qui répondra mieux à nos besoins !
Il ne nous reste plus qu'à configurer notre petite fenêtre pour le Web, sans oublier la barre pour saisir les adresses et la touche " Close " pour fermer. Donnons un nom à notre configuration et sauvegardons-la.
C'est terminé ! Pour ouvrir la nouvelle fenêtre, lançons SiteKiosk (dans C:\Programmes\SiteKiosk \, ouvrons le fichier sitekiosk.exe, de la même manière que nous avons exécuté configure.exe). Si des pop-up d'avertissement apparaissent, il suffit de cliquer sur OK jusqu'à ce que la fenêtre demande le nom du fichier de configuration à utiliser. Sélectionnons alors le fichier que nous venons de créer. Nous pouvons maintenant surfer en toute liberté à partir de ce terminal " reconfiguré ".

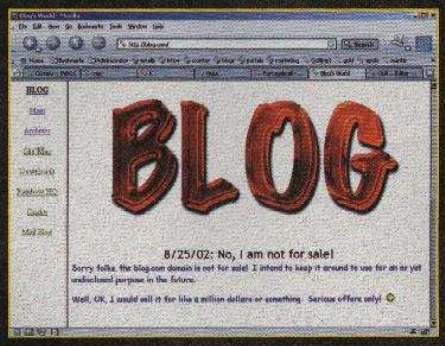
Francesco "EthMan" S.

UN BLOG VRAIMENT POU

ACCESSIBILITÉ : sur le Web, ce mot désigne tout ce qui peut faciliter l'accès des utilisateurs aux différents sites. Vous trouverez ici tout ce qu'il est nécessaire de savoir sur le sujet.

Nous avons vu dans un numéro précédent qu'il est toujours préférable de spécifier le DOCTYPE corrigé dans les documents HTML que nous écrivons. Cela vaut également pour les blogs.
Nous étudierons avant tout l'importance occupée par la langue. Même s'il peut sembler étrange de préciser la langue de notre site, blog, ou page Web, c'est pourtant fondamental, en particulier pour ceux, comme les non-voyants, qui utilisent un système de synthèse vocale, dont le logiciel doit s'adapter à la langue du site visité.

Selon Google Zeitgeist (http://www.google.com/press/zeitgeist.html), qui donne chaque mois un classement des recherches les plus populaires, la moitié des utilisateurs du



célèbre moteur fait ses recherches dans une langue autre que l'anglais. De fait, si notre programme d'authoring HTML insère une langue erronée ou n'en insère aucune, notre site risque de ne pas être trouvé par Google. Il est donc nécessaire de bien la préciser.
Il faut également prendre en compte le fait que beaucoup d'internautes paramètrent les " Préférences " de Google (http://www.google.fr/preferences?hl=fr) pour effectuer des recherches uniquement dans leur propre langue ou dans une langue spécifique.
Malgré tout, Google possède d'excellents algorithmes et pourrait probablement nous trouver, mais pourquoi lui compliquer la tâche ? Surtout lorsque l'on pense à toutes les pages faciles à atteindre… Donc, si nous voulons que notre site soit visité, soyons accessibles !

Configuration de la langue

L'identifiant de pays suffit pour configurer la langue de notre site. Par exemple : " en " pour l'anglais, " it " pour l'italien, " de " pour l'allemand, " fr " pour le français.

TOUS

Pour ceux que cela intéresse, la liste complète des identifiants de tous les pays du monde se trouve à cette adresse : http://www.oasis-open.org/cover/iso639a.html. On peut écrire ces codes en lettres majuscules ou minuscules, les deux fonctionnent. Où rentrer les codes de la langue ? À l'intérieur d'un tag <html> naturellement, mais la manière dépend du DOCTYPE. Voyons quelques exemples.

- **HTML ou sa variante**

Changeons le tag

```
<html> en <html lang= " fr ">
```

(il suffit de changer le code pour changer la langue)

- **XHTML 1.0 ou sa variante**

Changeons le tag

```
<html>  in  <html
xmlns="http://www.w3.org/1999/xhtm
l" lang="it" xml:lang="it">
```

- **XHTML 1.1 ou sa variante**

Changeons le tag

```
<html>  in  <html
xmlns="http://www.w3.org/1999/xhtm
l" xml:lang="it">
```

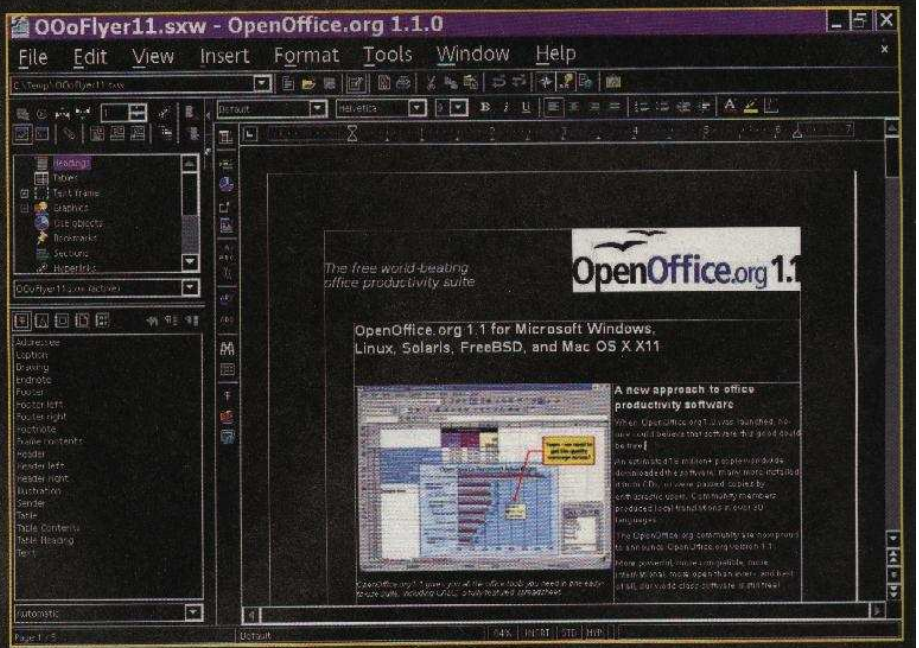
Il faut mentionner la langue sur l'ensemble des pages du site. Dans le cas où figurent plusieurs langues (par exemple, un blog en français contenant des citations en anglais), nous pouvons nous organiser de la manière suivante. L'exemple est valable pour des pages avec un DOCTYPE HTML.

```
<html lang="it">
 ...
 <blockquote lang="en">
 ...
 </blockquote>
```

Pour tout savoir sur le fonctionnement des propriétés lang, il faut étudier très soigneusement la page http://www.w3.org/TR/REC-html40/struct/dirlang.html#h-8.1.

Nommer les pages à l'aide de titres significatifs

Chaque page Web créée devrait avoir un titre significatif. Dans le cas d'un blog, la page d'accueil pourrait simplement porter le nom du blog. Seuls les lamers ne donnent pas de titres à leurs pages ou bien leur donnent des titres idiots ! Les pages d'archive, si elles sont classées par date, devraient comporter le



Lors de la création d'un blog ou d'un site, il faut tenir compte du fait que certaines personnes déficientes visuelles préfèrent changer les couleurs à l'écran.

FAIRE UN BLOG

Liens pour faire un blog comme il faut

MOVABLE TYPE
http://movabletype.org

GREYMATTER
http://www.noahgrey.com/greysoft/

BLOGGER
http://www.blogger.com

SPLINDER
http://www.splinder.com

USERLAND
http://www.userland.com

MANILA
http://www.userland.com

nom du blog, suivi de la date ou de l'intervalle de la date, par exemple Blogico/19 décembre 2004 ou bien Bloglob/décembre 2004. Une autre astuce utile pour archiver rapidement les pages est de les numéroter par année (quatre chiffres), par mois (deux chiffres) et par jour (deux chiffres). Par exemple, 4 décembre 2004 = 20041204. De cette façon, même dans l'ordre alphabétique, les fichiers seront classés par date.

Il serait également préférable d'inclure la catégorie dans le titre de la page, avec le nom du blog : Monblog/politique (si l'on parle de politique). Chaque page consacrée à un seul sujet devrait contenir dans son titre le nom du blog et le sujet en question. C'est la raison pour laquelle le langage Perl de Python convient mieux pour les blogs.

Comme pour la langue, les programmes de lecture pour non-voyants se basent sur le titre des pages. Google, quant à lui, privilégie les pages avec un titre. Autant de raisons de ne pas l'oublier ! D'autre part, les moteurs de recherche, en général, ne prennent en compte que les cinquante premiers caractères. Inutile, donc, d'aller au-là.

P. Greco

POUR LES NON VOYANTS

Pour surfer sur Internet même si l'on est non-voyant.

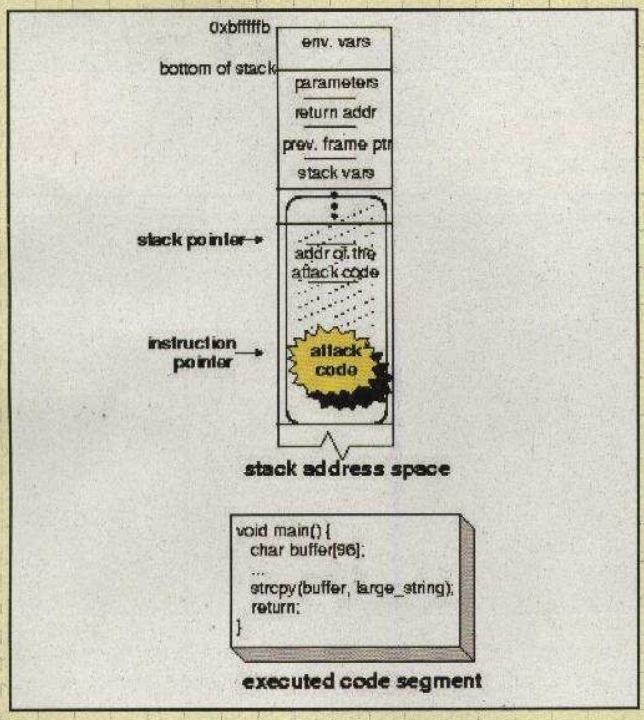
Des programmes tels que JAWS permettent aux personnes ayant des problèmes de vue de mener une vie tout à fait normale. Cependant, le logiciel ne pourra être d'aucune utilité si le site visité est inadapté. JAWS est destiné à Windows, mais il en existe de similaires pour tous les systèmes d'exploitation.

ENCYCLOPEDIE du hacking

Buffer Overflow

On dit qu'il y a buffer overflow (en français, littéralement " débordement de zone tampon ") lorsqu'un processus essaie de mémoriser plus de données que ce qu'il peut contenir, dans une zone de mémoire prévue pour les accueillir temporairement et appelée " buffer ". Les informations en excès débordent (c'est l'overflow) dans des zones de mémoire adjacentes. Les effets peuvent être dévastateurs pour les données en mémoire, car le surcroît de données peut contenir de véritables programmes à l'origine d'opérations spécifiques.

EXEMPLE



Un programme bien assemblé inséré dans un ordinateur à cause de la faille d'un système acceptant un buffer overflow pourrait altérer les fichiers, détruire des données, entrer en possession de mots de passe. Tout dépend de la zone de mémoire dans laquelle il réussit à s'introduire et des privilèges qu'il parvient à obtenir.
Il s'agit d'un buffer overflow lorsque, par exemple, à partir d'un formulaire sur Internet programmé pour accepter dix caractères (par l'intermédiaire d'un paramètre maxlenght=10), le serveur reçoit autre chose que la chaîne de caractères à laquelle il s'attend, à savoir quelque chose comme ça :

http://www.underflow.com/pubs/test.html?username=alessandro

Si, à la place, il reçoit ceci :

http://www.underflow.com/pubs/test.html?username=alessandrozzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz

et que le système n'est pas protégé contre les buffer overflow, alors il peut crasher, ou pire, laisser passer l'utilisateur car c'est une situation qui n'a pas été prévue par le système d'authentification.

Qualites requises

Il est souvent utile de connaître le langage C pour étudier les buffer overflow. Les programmes rédigés en C sont en effet généralement plus enclins à présenter des failles de ce type, parce que ce langage exige que le programmateur vérifie la longueur des buffers de mémoire. Les programmes rédigés dans des langages comme VisualBasic ou Java sont généralement moins vulnérables à ce type d'attaque.

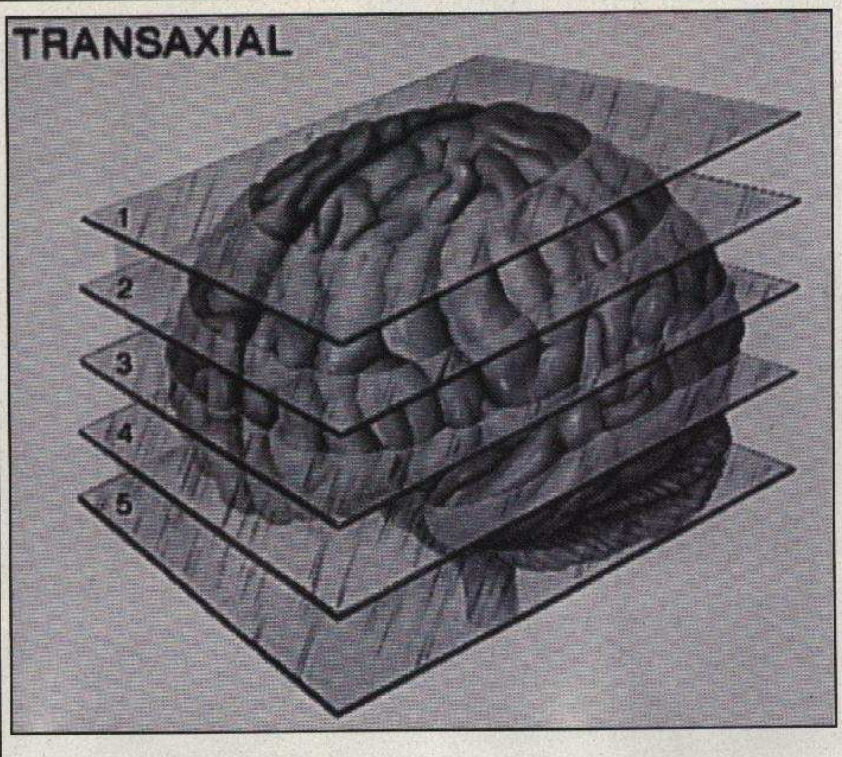
Securite

Très souvent, les attaques de buffer overflow se terminent bien parce que le système attaqué fait fonctionner ses processus réseau directement dans la root (niveau le plus bas), ou de toute façon au niveau de l'administrateur système. Pour cette raison, il est plus facile pour l'attaquant de faire tourner son programme néfaste à un niveau de privilèges élevé. Pour se protéger, la première précaution à prendre est donc de faire fonctionner les programmes utiles à des niveaux plus bas, c'est-à-dire sans les privilèges de l'administrateur système.

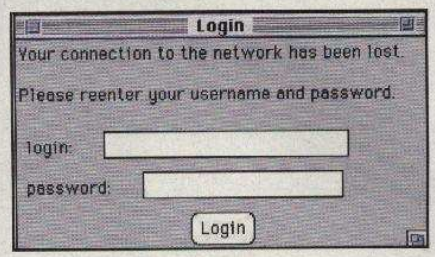
LIEN:
Exemple d'un buffer overflow constaté sur des systèmes d'il y a quelques années : http://project.honeynet.org/scans/scan25/sol/NCSU/main.html#b6
Possible buffer overflow récemment découvert par l'intermédiaire d'images PNG : http://scary.beasts.org/security/CESA-2004-001.txt

ENCYCLOPEDIE du hacking

L'ingénierie sociale (en anglais " social engineering ")



L'ingénierie sociale est une forme de hacking axé davantage sur la manière de penser de l'utilisateur d'un ordinateur que sur l'ordinateur lui-même. Le but est de soutirer le maximum d'informations sur l'utilisateur d'un système informatique pour identifier ses points forts et ses points faibles.



EXEMPLE

L'ingénierie sociale peut être mise en œuvre dans différentes situations. Par exemple, lorsque l'on essaie d'obtenir par téléphone les noms des employés d'une entreprise, ou bien, procédé passible de poursuites judiciaires, lorsque l'on se fait passer pour un employé de banque afin de récupérer un numéro de carte de crédit. Méfions-nous également des regards furtifs lorsque nous tapons notre code dans un magasin ou un restaurant. L'ingénierie sociale est souvent une question de psychologie, parfois d'adresse et presque toujours de ruse.

Un autre outil d'ingénierie sociale : la recherche dans les annuaires et les cartes routières. À partir d'un simple numéro de téléphone, les " ingénieurs sociaux " peuvent apprendre énormément de choses. De même, à partir d'un nom de particulier ou de société. On peut souvent déduire le statut social et le niveau de revenu d'un individu lorsque l'on connaît son adresse. Ce ne sont que quelques exemples, les occasions sont fréquentes d'enfreindre les lois protégeant la vie privée.

Qualites requises

Pour être un " bon " ingénieur social, il faut étudier le comportement des personnes et comprendre comment elles se comportent, quitte à se mettre dans des situations imprévues et incommodes. " Vous ne pouvez pas répondre à ma question, plutôt que d'avoir à passer par votre chef ?... " est une phrase qui dénote une connaissance profonde des faiblesses humaines. De plus, il est indispensable de connaître les moyens dont on dispose pour obtenir toutes sortes d'informations.

Securite

Avec du simple bon sens, on peut lutter contre l'ingénierie sociale. On peut aussi suivre scrupuleusement des procédures qui ont été testées. Au pire, une procédure peut être défectueuse, mais en aucun cas cela ne doit venir de nous. Il faut se servir des mêmes moyens qu'utilise l'ingénierie sociale pour la combattre.

PAGES BLANCHES ET JAUNES: www.pagesblanches.fr www.pagesjaunes.fr

CYBERÉNIGME EN SÉRIE !

PRENONS UN NOMBRE. SI CELUI-CI EST PAIR, DIVISONS-LE PAR DEUX. S'IL EST IMPAIR, MULTIPLIONS-LE PAR 3 ET AJOUTONS 1. COMMENÇONS PAR LE CHIFFRE 1 :

1 est un nombre impair, donc 1 * 3 + 1 = 4

4 est un nombre pair, donc 4/2 = 2

2 est un nombre pair, donc 2/2 = 1

La série aboutit à 1 en trois étapes.

POUR TOUS : En combien d'étapes parvient-on à 1 si l'on commence par le nombre 27 ? On peut le calculer soi-même ou bien trouver un site qui le fait à notre place. La série s'appelle 3n+1. C'est la fonction associée à la conjecture de Collatz.

À quoi cela sert-il ? On peut utiliser cette fonction pour communiquer un message chiffré. Prenons par exemple le nombre 6 et trouvons tous les nombres de la série générés : nous obtenons 63105168421 (6-3-10-5-16-8-4-2-1), qui peut être la clé d'un PAD, c'est-à-dire un logiciel d'assemblage/désassemblage. Seul le destinataire sait à quelle série correspond le chiffre 6 que nous lui avons communiqué.

POUR LES SPÉCIALISTES : Le message chiffré est GRWMHXFUSPVQNJJPJVWGFOFATL QRFR. La clé est 19. À chaque lettre correspond un nombre. Donc, sachant que chaque lettre du message est déplacée de zéro à neuf places en avant dans l'alphabet, quel est ce message ?
Nous pouvons envoyer une clé en générant une série de nombres avec une règle précise, mais pas facile à trouver.

POUR LES GÉNIES : La clé est 132113213 221133112132123222110. Pour y parvenir, nous avons procédé ainsi :

0
10
1110
3110
132110
1113122110
311311222110
13211321322110
1113122113121113222110
31131122211311123113322110

Quelle est la règle ?
Coup de pouce : le chiffre 4 n'apparaît pas et le zéro se trouve uniquement à la fin. Si au lieu de partir de 0, la série commençait à 1, à quoi ressemblerait-elle ?

POUR LES SUPER HACKERS : Écrire un programme qui accepte un nombre et qui en reproduise les étapes de la série 3n+1, en comptant les étapes nécessaires pour retourner à 1 (assez facile). Ou bien écrire un programme qui produise tout seul, jusqu'à l'infini ou en un nombre d'étapes arbitraires, une série pour génies, en appliquant la règle qui convient (demande davantage de concentration). Qui est capable de trouver une règle très simple qui produira une série intéressante, par exemple 01101001100101101001011001101001?

Courage et à la prochaine cyberénigme