OSSIR
Groupe Paris

Réunion du 15 juin 2010

Revue des dernières vulnérabilités

Nicolas RUFF
EADS-IW
nicolas.ruff (à) eads.net

Avis Microsoft

- **Correctifs de Mai 2010**
  - **2 bulletins, 2 failles**
  - **Avec [exploitability index]**
    - **http://blogs.technet.com/msrc/archive/2010/05/11/may-2010-security-bulletin-release.aspx**
  - **MS10-030 Faille dans Outlook Express [2]**
    - **Affecte: Outlook Express / Windows Mail / Windows Live Mail**
    - **Exploit: integer overflow dans le support des protocoles POP3/IMAP**
      - **http://www.exploit-db.com/exploits/12564**
      - **http://blogs.technet.com/srd/archive/2010/05/11/ms10-030-malicious-mail-server-vulnerability.aspx**
    - **Crédit: Francis Provencher / Protek Research Lab**
  - **MS10-031 Faille dans VBA [2]**
    - **Affecte: Office XP / 2003 / 2007**
      - **Mais pas les Viewer, les versions Mac, etc.**
    - **Exploit: corruption de la pile dans VBE6.DLL**
      - **Difficilement exploitable !**
      - **http://blogs.technet.com/srd/archive/2010/05/11/ms10-031-vbe6-single-byte-stack-overwrite.aspx**
    - **Crédit: NSFocus**

Avis Microsoft

- **Correctifs de Juin 2010**
  - **10 bulletins, 34 failles**
  - **Avec [exploitability index]**
    - **http://blogs.technet.com/b/msrc/archive/2010/06/08/june-2010-security-bulletin-release.aspx**
    - **http://blogs.technet.com/b/srd/archive/2010/06/08/assessing-the-risk-of-the-june-security-bulletins.aspx**
  - **MS10-032 Failles noyau [1,1,1]**
    - **Affecte: Windows (toutes versions supportées)**
    - **Exploit: élévation de privilèges locale**
      - **Composant affecté: win32k.sys**
      - **http://blogs.technet.com/b/srd/archive/2010/06/08/ms10-032-vulnerabilities-in-windows-kernel-mode-drivers-could-allow-elevation-of-privilege.aspx**
    - **Crédit:**
      - **Sébastien Renaud / VUPEN**
      - **Secunia Research**

Avis Microsoft

- MS10-033 Failles dans les codecs Windows Media [1,1]
  - Affecte: Windows (toutes versions supportées)
    - Sauf Windows 2000 si DirectX 9 / Windows Media 9 n'a pas été installé
  - Exploit: exécution de code à l'ouverture d'un flux MJPEG malformé
    - Composants affectés: quartz.dll / asycfilt.dll
  - Crédit:
    - Yamata Li / Palo Alto Networks

- MS10-034 Mise à jour des « kill bits » [1,1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: exécution de code depuis une page Web à l'aide de contrôles ActiveX vulnérables
    - Microsoft Data Analyzer
    - Microsoft IE8 Developer Tools
    - Danske Bank eSec
    - CA Pest Scan
    - Kodak Ofoto Upload Manager
    - Avaya CallPilot Unified Messaging
  - Crédit:
    - Shaun Colley / NGS Software
    - Chris Ries / Carnegie Mellon University

Avis Microsoft

- MS10-035 Failles dans Internet Explorer [2,3,1,?,?,1]
  - Affecte: IE (toutes versions supportées)
  - Exploit: exécution de code (ou fuite d'informations) à travers une page Web
    - http://blogs.technet.com/b/srd/archive/2010/06/08/ms10-035-cross-domain-information-disclosure-vulnerability.aspx
    - Inclut la faille utilisée lors du concours « pwn2own »
      - http://www.darknet.org.uk/2010/06/microsoft-patches-at-least-34-bugs-including-pwn2own-vulnerability/
      - http://www.zerodayinitiative.com/advisories/ZDI-10-102/
    - Protège contre le « stroke-jacking »
      - http://lcamtuf.blogspot.com/2010/06/curse-of-inverse-strokejacking.html
  - Crédit:
    - Chris Weber / Casaba Security
    - Takeshi Terada
    - Michal Zalewski / Google
    - Chris Rohlf / Matasano (x2)
    - Peter Vreugdenhil / ZDI

Avis Microsoft

- MS10-036 Faille dans le support COM [1]
  - Affecte: Office XP / 2003 / 2007
    - Introduit la notion de « kill bit » pour Office 2003 et 2007
    - Aucun correctif n'a été publié pour Office XP, mais un « workaround »
  - Exploit: exécution de code à l'ouverture d'un document Office
  - Crédit:
    - David Dewey / IBM ISS X-Force
    - Ryan Smith / Accuvant (anciennement VeriSign iDefense)

- MS10-037 Faille dans le support du format CFF (Compact Font Format) [2]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: élévation de privilèges locale
    - Composant affecté: « atmfd.dll »
  - Crédit: Chris Carton / Laserforce + Secunia

Avis Microsoft

- MS10-038 Failles Excel [2,1,2,1,1,1,1,1,1,1,2,2,1,1]
  - Affecte: Office XP / 2003 / 2004 (Mac) / 2007 / 2008 (Mac)
    - + Excel Viewer et Compatibility Pack
  - Exploit: exécution de code à l'ouverture d'un document malformé
  - Crédit:
    - Anonymous / ZDI (x2)
      - http://www.zerodayinitiative.com/advisories/ZDI-10-103/
      - http://www.zerodayinitiative.com/advisories/ZDI-10-104/
    - Nicolas Joly / VUPEN (x8)
    - Bing Liu / Fortinet
    - Carsten Eiram / Secunia (x2)
      - http://secunia.com/secunia_research/2009-54/
      - http://secunia.com/secunia_research/2009-59/
    - Rick Glaspie / Gilbert Public Schools

Avis Microsoft

- **MS10-039 Failles SharePoint et InfoPath [1,3,3]**
  - **Affecte: InfoPath 2003 / 2007, SharePoint 3.0 / 2007**
  - **Exploit:**
    - **XSS affectant « Help.aspx »**
    - **Fuite d'information via toStaticHTML()**
    - **Déni de service du serveur à travers « Help.aspx »**
  - **Crédit:**
    - **Chris Weber / Casaba Security**
    - **Rik Jones / Dallas County Community College District**

- **MS10-040 Faille IIS [2]**
  - **Affecte: IIS 6 / 7 / 7.5**
  - **Exploit: exécution de code à distance**
    - **Nécessite que *Extended Protection for Authentication* (KB973917) ait été installé et activé**
  - **Crédit: n/d**

Avis Microsoft

- MS10-041 Faille dans la vérification de signature XML [3]
  - Affecte: .NET Framework 1.1 / 2.0 / 3.5 sur Windows < Vista / 3.5.1
    - Ce qui exclut 3.0 / 4.0
    - Ainsi que 3.5 sur Windows >= Vista
  - Exploit: il est possible de falsifier la signature XMLDSig
    - En spécifiant longueur de la signature == 0
    - http://blogs.technet.com/b/srd/archive/2010/06/08/ms10-041-xml-signature-hmac-truncation-bypass-vulnerability.aspx
  - Crédit: Arian Evans / WhiteHat Security

Avis Microsoft

- Advisories
  - Q973811 *Extended Protection for Authentication*
    - V1.5: ajout du Framework .NET (sous forme de mise à jour optionnelle à télécharger)
  - Q980088 Fuite d'informations dans Internet Explorer
    - V1.2: cette faille est partiellement corrigée par MS10-035
  - Q983438 XSS dans SharePoint
    - V2.0: cette faille est corrigée par MS10-039
  - Q2028859 Faille dans CDD.DLL
    - Affecte: Windows Seven et 2008 R2
      - Nécessite l'interface Aero
    - Exploit: exécution de code à l'affichage d'une image
      - Difficile, plus probablement un DoS
        - http://blogs.technet.com/msrc/archive/2010/05/18/security-advisory-2028859-released.aspx
        - http://blogs.technet.com/srd/archive/2010/05/18/cdd-dll-vulnerability-difficult-to-exploit.aspx

Avis Microsoft

- Q2219475
  - Exécution de commandes à travers Internet Explorer
    - Grâce à une URL de type « hcp:// »
    - http://blogs.technet.com/b/srd/archive/2010/06/10/help-and-support-center-vulnerability-full-disclosure-posting.aspx
    - http://blogs.technet.com/b/msrc/archive/2010/06/10/windows-help-vulnerability-disclosure.aspx
    - http://blogs.technet.com/b/msrc/archive/2010/06/10/security-advisory-2219475-released.aspx
    - http://secunia.com/blog/103/
  - Publié de manière « irresponsable » par Tavis Ormandy …
    - http://seclists.org/fulldisclosure/2010/Jun/205
  - V1.1: un « FixIt » est disponible

Avis Microsoft

- **Révisions**
  - **MS09-061**
    - **V1.3: changement de la logique de détection**
  - **MS10-011**
    - **V1.2: problème connu (KB978037)**
  - **MS10-020**
    - **V1.1: problème connu (KB980232)**
  - **MS10-030**
    - **V1.1: nécessité d'un redémarrage ... ou pas**
    - **V1.2: Windows Mail n'existe pas sous Seven / 2008R2**
  - **MS10-031**
    - **V1.1: mise à jour de la FAQ**
  - **MS10-033**
    - **V1.1: mise à jour documentaire**
  - **MS10-038**
    - **V1.1: plus aucun problème connu**

Infos Microsoft

- **Sorties logicielles**
  - **Version beta du SP1 pour Seven/2008R2 prévue en juillet**
  - **ACT 5.6**
  - **Microsoft installe silencieusement une extension FireFox avec les mises à jour du mois de Juin 2010**
    - **http://arstechnica.com/microsoft/news/2010/06/microsoft-slips-ie-firefox-add-on-into-toolbar-update.ars**
- **Autre**
  - **Les gouvernements auront les failles avant les autres**
    - **Pour protéger les « infrastructures critiques »**
      - **http://threatpost.com/en_us/blogs/microsoft-share-vulnerability-details-governments-051810**
  - **Un showcase pour le Cloud Computing**
    - **http://www.modelingtheworld.com/**
  - **Microsoft Office 2010 supporte la signature XAdES**
    - **http://blogs.technet.com/b/office2010/archive/2009/12/08/digital-signitures-in-office-2010.aspx**

Infos Réseau

- (Principales) faille(s)
  - WebSense 6.3.3
    - L'ajout d'un entête « Via: » permet de contourner entièrement la politique de filtrage
      - http://archives.neohapsis.com/archives/fulldisclosure/2010-05/0376.html
  - Litespeed Web Server
    - Accès au code source en utilisant un caractère « NUL »
      - http://archives.neohapsis.com/archives/fulldisclosure/2010-06/0280.html
  - UnrealIRCd « backdooré »
    - Depuis quelques temps …
      - http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt
  - Snort
    - La clé privée SSL est la même sur toutes les instances du produit
      - http://www.zerodayinitiative.com/advisories/ZDI-10-107/

Infos Réseau

- **Autres infos**
  - **Panne générale du « .de » pendant une heure**
    - **http://cert.lexsi.com/weblog/index.php/2010/05/12/385-panne-internet-geante-en-allemagne-et-en-Autriche**
  - **Une application ZRTP pour Android**
    - **http://whispersys.com/**

Infos Unix

- (Principales) faille(s)
  - Samba <= 3.4.7, <= 3.5.1
    - Laurent Gaffié continue de frapper ☺
  - MySQL < 5.1.47
    - http://dev.mysql.com/doc/refman/5.1/en/news-5-1-47.html
  - PostgreSQL
    - http://www.postgresql.org/about/news.1203
  - FreeBSD 8.0
    - http://security.freebsd.org/advisories/FreeBSD-SA-10:04.jail.asc
    - http://security.freebsd.org/advisories/FreeBSD-SA-10:05.opie.asc
    - http://security.freebsd.org/advisories/FreeBSD-SA-10:06.nfsclient.asc
  - OpenSSL < 0.9.8o, < 1.0.0a
    - 2 failles corrigées
      - http://www.openssl.org/news/secadv_20100601.txt

Infos Unix

- Quelques failles dans Solaris
  - Affecte: Solaris 10
  - Exploit: failles dans « find » et « rm » (!)
    - http://securityreason.com/achievement_securityalert/85

- rpc.pcnfsd
  - Affecte:
    - AIX 5.1, 6.0
    - HP-UX 11.11, 11.23, 11.31
    - IRIX 6.5
  - Exploit:
    - Et en plus c'est une chaine de format dans syslog() ...
    - http://www.checkpoint.com/defense/advisories/public/announcement/2010/052010-syslog-format-string-vulnerability.html

Infos Unix

- Autre
  - Sortie d'OpenBSD 4.7
    - http://openbsd.org/47.html
  - Un port natif d'OpenSSH pour Windows
    - http://www.nomachine.com/contributions.php
  - Le support xt_TEE ajouté à NetFilter
    - http://permalink.gmane.org/gmane.linux.network/160668

Failles

- **Principales applications**

  - **Adobe ShockWave < 11.5.7.609**
    - **http://www.adobe.com/support/security/bulletins/apsb10-12.html**
    - **Crédits**
      - **Chaouki Bekrar / VUPEN (x4)**
      - **Sebastien Renaud / VUPEN**
      - **Code Audit Labs (x3)**
      - **Nahuel Riva / Core**
      - **Gjoko Krstic / Zero Science Lab**
      - **Chro HD / FortiGuard (x7)**
      - **Anonymous / iDefense**
        - **http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=869**
      - **Alin Rad Pop / Secunia (x6)**
      - **Anonymous / ZDI (x3)**
        - **ZDI-10-087, ZDI-10-088, ZDI-10-089**

Failles

- Flash < 10.1.53.64
  - Faille critique, non patchée, exploitée dans la nature
    - http://www.adobe.com/support/security/advisories/apsa10-01.html
    - http://blog.zynamics.com/2010/06/09/analyzing-the-currently-exploited-0-day-for-adobe-reader-and-adobe-flash/
    - http://community.websense.com/blogs/securitylabs/archive/2010/06/09/having-fun-with-adobe-0-day-exploits.aspx
  - Correctif pour Flash Player
    - Disponible depuis le 10 juin
    - Corrige 32 (!) failles
      - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=871
      - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=872
      - Dont une exploitable uniquement si les VMWare Tools sont installés
    - http://www.adobe.com/support/security/bulletins/apsb10-14.html
  - Correctif pour Acrobat Reader ?
    - Sera corrigée le 29 juin …

Failles

- Crédits
  - Anonymous + Dionysus Blazakis / ZDI
  - Anonymous / iDefense (x2)
  - Damian Put / ZDI (x2)
  - Anonymous + Tielei Wang / ZDI

  - Tielei Wang / ICST-ERCIS (Engineering Research Center of Info Security, Institute of Computer Science & Technology, Peking University / China)
  - Will Dormann / CERT (x2)
  - Lockheed Martin CIRT / Members of the Defense Security Information Exchange (DSIE)
  - Ralph Loader / Innaworks Development Limited
  - Nicolas Joly / VUPEN (x3)
  - Manuel Caballero / Microsoft Vulnerability Research (MSVR)
  - Red Hat Security Response Team
  - Ezio Anselmo Mazarim Fernandes
  - Tavis Ormandy / Google Security Team (x9)

  - Megumi Yanagishita / Palo Alto Networks
  - Bo Qu / Palo Alto Networks (x4)

  - Bing Liu / Fortinet (x2)
  - Haifei Li / Fortinet

Failles

- Google Chrome < 5.0.375.70
  - Note: la 6.0 est déjà en beta
    - http://googlechromereleases.blogspot.com/2010/05/stable-channel-update.html
    - http://googlechromereleases.blogspot.com/2010/06/stable-channel-update.html
- Safari < 4.1, < 5.0
    - http://support.apple.com/kb/HT4196
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=870
    - Ainsi que ZDI-10-091 ... ZDI-10-101 (!)
  - Corrige également une faille « amusante »
    - « http:google.com » est considéré comme une URL valide sans domaine
      - Ce qui permet de contourner la Same Origin Policy
    - APPLE-SA-2010-06-07-1
    - http://lcamtuf.blogspot.com/2010/06/safari-tale-of-betrayal-and-revenge.html

Failles

- Mise à jour de Java sur Mac OS X
  - http://support.apple.com/kb/HT4170
  - http://support.apple.com/kb/HT4171
- Comment exploiter une faille dans Java < 1.6.0_19
  - Une explication très détaillée !
    - http://vreugdenhilresearch.nl/2010/05/java-midi-parse-vulnerabilities/
- OpenOffice < 3.2.1
  - Failles corrigées
    - « Renégociation SSL/TLS »
    - Exécution de macros Python sans confirmation lors de l'ouverture de l'éditeur de macros
    - http://www.openoffice.org/security/bulletin.html
  - A cette occasion, tout a été « Oraclisé »

Failles

- WireShark < 1.2.8
  - http://www.wireshark.org/security/wnpa-sec-2010-03.html
  - http://www.wireshark.org/security/wnpa-sec-2010-04.html
- WireShark < 1.2.9
  - http://www.wireshark.org/security/wnpa-sec-2010-05.html
  - http://www.wireshark.org/security/wnpa-sec-2010-06.html
- Foxit 3.3.1 bloque « LaunchAction »
  - http://www.foxitsoftware.com/pdf/reader/whatsnew331.htm
- Sortie de SumatraPDF 1.1
  - Correction de bogues
  - Durcissement de la chaine de compilation

Failles

- Une faille dans l'iPhone ?
  - Contournement du verrouillage de l'écran d'accueil
  - Apple « n'arrive pas à reproduire »
    - http://marienfeldt.wordpress.com/2010/03/22/iphone-business-security-framework/

- Cisco IronPort plugin for Outlook
  - « *If multiple email messages are being composed simultaneously and the Send Secure button is used to send more than one of the email messages, an error condition may occur where only the first email message sent is successfully encrypted.* »
    - http://www.cisco.com/en/US/products/products_security_response09186a0080b2c505.html

- Un nouveau « pack » pour le produit Immunity Canvas
    - http://www.immunityinc.com/products-whitephosphorus2.shtml

Failles 2.0

- Nouvelle attaque: le « tabnabbing »
  - http://www.azarask.in/blog/post/a-new-type-of-phishing-attack/
- Le « clicjacking » utilisé pour de vrai contre Facebook
  - http://isc.sans.edu/diary.html?storyid=8893
- 1,5 million de comptes Facebook à vendre
  - Source: iDefense
    - http://www.zdnet.com/blog/security/15-million-facebook-accounts-offered-for-sale-faq/6304
- Facebook renforce la sécurité du login
  - Il est possible de spécifier ses adresses IP « préférées »
    - http://blog.facebook.com/blog.php?post=389991097130
- De nombreux vers Twitter et/ou Facebook
  - Ex. FBHole
  - Pas la peine de tous les lister ici …

Failles 2.0

- ATT « perd » les coordonnées complètes des 114 000 utilisateurs qui ont précommandé l'iPad
  - http://gawker.com/5559346/apples-worst-security-breach-114000-ipad-owners-exposed
- « Skyrock » (ex. « Skyblog ») piraté
  - Via l'application publicitaire d'un partenaire
    - http://www.zataz.com/news/20256/skyrock--skyblog--piratage.html
    - http://www.zataz.com/news/20282/skyblog--enquete-piratage.html
- Attaques en saturation téléphonique
  - Pour empêcher les banques de joindre leurs clients lors de transaction frauduleuses
    - http://www.wired.com/threatlevel/2010/05/telephony-dos/
    - http://njtoday.net/2010/05/12/phony-phone-calls-distract-consumers-from-genuine-theft-%E2%80%94-fbi-partners-warn-public/

Malwares et spam

- Le forum « carders.cc » piraté
  - Et les données publiées dans la nature
    - http://krebsonsecurity.com/2010/05/fraud-bazaar-carders-cc-hacked/
    - http://j0hnx3r.org/?p=606
    - http://nopaste.info/81779e1129_nl.html
- Infection en masse de sites ASP.NET
  - Via des injections SQL « basiques »
  - Et combinée avec la dernière faille Acrobat (non patchée)
    - http://blog.sucuri.net/2010/06/mass-infection-of-iisasp-sites-robint-us.html
- Le nombre de « malwares » pour mobiles explose
  - D'après une société qui distribue un anti-malware …
    - http://www.darkreading.com/insiderthreat/security/attacks/showArticle.jhtml?articleID=225402185

Malwares et spam

- IBM distribue des clés USB infectées
  - Lors d'une conférence de sécurité … (AusCERT)
    - http://www.gizmodo.com.au/2010/05/ibm-gifts-computer-security-expo-attendees-with-virus-filled-usb-sticks/
- Un nouveau type d'adware (sous forme de recherche universitaire)
  - Principe: injecter de la publicité dans du trafic WiFi non protégé
    - http://en.wikipedia.org/wiki/Typhoid_adware
- Un spyware pour Mac OS X détecté dans la nature
    - http://www.zdnet.fr/actualites/un-spyware-pour-mac-s-invite-dans-des-logitheques-en-ligne-39752099.htm

Actualité (francophone)

- Le RGS officiellement publié
  - http://www.ssi.gouv.fr/rgs
- Actualité ANSSI
  - Sécurité du langage Java
    - http://www.ssi.gouv.fr/site_article226.html
  - Effacement des supports de stockage de masse
    - http://www.ssi.gouv.fr/site_article172.html
- La CNIL épingle le ministère de la Justice
  - http://www.cnil.fr/la-cnil/actu-cnil/article/article/2/les-conclusions-des-controles-de-la-cnil-dans-laffaire-de-m-ali-soumare/
- 8 juin 2010
  - Ouverture officielle des sites « légaux » de paris en ligne
    - Sous contrôle de l'ARJEL

Actualité (francophone)

- Un logiciel de « protection » contre le P2P
  - … ou pas !
    - http://bluetouff.com/2010/06/13/orange-vous-securise-ayez-confiance/
- (Encore) une panne informatique à la SNCF
  - Mais cette fois-ci il n'y a pas que Voyages-Sncf.com qui est touché !
    - http://www.google.com/hostednews/afp/article/ALeqM5hzBIL1gZHMNb73RfqqU7JyC72mAw
- Quand l'administration utilise des webmails (étrangers)
    - http://bugbrother.blog.lemonde.fr/2010/05/14/55-000-webmails-piratables-sur-les-sites-gouvfr/
- Dassault Systèmes rachète Exalead
- Après IsEncryptionPermitted() ...
  - IsSchEncryptionPermitted() !
    - http://expertmiami.blogspot.com/2010/05/exception-culturelle.html

Actualité (anglo-saxonne)

- Symantec rachète la branche « certificats » de VeriSign
  - Le certificat n'est plus assez rentable (?)
- Un outil de surveillance des étudiants se retourne contre eux
  - Des failles inexcusables ont été exploitées
    - http://www.wired.com/threatlevel/2010/05/lanrev-security-holes/
- La guerre du NAC est terminée chez Cisco
    - http://news.idg.no/cw/art.cfm?id=C8DE2975-1A64-6A71-CE4E0A7BD2C51E0E
- La valeur des vulnérabilités
  - Attention: une étude probablement sans valeur statistique !
    - http://cyber-son.blogspot.com/2010/05/vulnerability-market-numbers.html
    - http://unsecurityresearch.com/index.php?option=com_content&view=article&id=52&Itemid=57
- Le Canada veut renforcer la sécurité du « cybermarché »
  - Protection des données personnelles
  - Lutte contre le spam
    - http://www.ic.gc.ca/eic/site/ic1.nsf/fra/05596.html

Actualité (européenne)

- Une campagne originale au Luxembourg
  - « Un mot de passe, c'est comme une brosse à dents: il faut en changer régulièrement »
    - http://www.cases.public.lu/fr/actualites/actualites/2010/05/31_password/index.html

- Une amende de 100€ pour défaut de sécurisation du WiFi en Allemagne
  - Une décision largement commentée …
    - http://www.itespresso.fr/p2p-une-amende-pour-defaut-de-securisation-du-wi-fi-en-allemagne-35075.html

Actualité (Google)

- httpS://www.google.com/
  - Est-ce vraiment plus sûr ?
- Le TOP 1000 du Web (d'après Google)
  - http://www.google.com/adplanner/static/top1000/#
- Google propose une extension pour désactiver Google Analytics
  - http://tools.google.com/dlpage/gaoptout
- Google Maps Navigation disponible en France
- Google recommande à ses employés d'abandonner Windows
  - Attention: non confirmé officiellement
    - http://www.ft.com/cms/s/2/d2f3f04e-6ccf-11df-91c8-00144feab49a.html
  - Mais commenté par Microsoft
    - http://windowsteamblog.com/windows/b/bloggingwindows/archive/2010/06/01/windows-and-security-setting-the-record-straight.aspx

Actualité (Google)

- Google fête les 10 ans de PacMan
  - http://www.google.com/pacman/
  - Cela aurait coûté 120 millions de dollars de productivité aux USA
    - http://www.solutions-logiciels.com/actualites.php?actu=7550

- Google pratique le wardriving « par erreur »
  - http://finance.yahoo.com/news/Google-grabs-personal-info-apf-2162289993.html?x=0&sec=topStories&pos=7&asset=&ccode
  - Du coup la CNIL engage un contrôle
    - http://www.cnil.fr/la-cnil/actu-cnil/article/article/2/streetview-la-cnil-vient-dengager-un-controle-de-google/

Actualité

- Un système de cryptographie quantique commercial « cassé »
  - Lors de la phase d'échange des clés
    - http://arxiv.org/abs/1005.2376
- HyperSafe: un hyperviseur « garanti »
  - Par qui / quoi ???
    - http://www.csc.ncsu.edu/faculty/jiang/pubs/OAKLAND10.pdf
- webOS vulnérable à une attaque par SMS
    - http://intrepidusgroup.com/insight/2010/04/webos-examples-of-sms-delivered-injection-flaws/
- Sorties
  - Metasploit 3.4.0
    - http://www.metasploit.com/framework/download/
  - OllyDbg 2.0
    - http://www.ollydbg.de/

Actualité

- SAP rachète Sybase
  - http://www.sap.com/press.epx?pressid=13202
- EFF: chaque navigateur est unique
  - En combinant tous les paramètres accessibles à un serveur Web
    - https://panopticlick.eff.org/browser-uniqueness.pdf
- Une homme s'inocule un « virus RFID »
  - Cela tient plus de la performance artistique … pour le moment
    - http://www.lefigaro.fr/sciences-technologies/2010/05/26/01030-20100526ARTFIG00686-le-premier-homme-contamine-par-un-virus-informatique.php

Fun

- « Man in the Middle » sur IRC
  - Capable de soutenir la conversation avec un être humain !
    - http://seclab.tuwien.ac.at/papers/autosoc-leet2010.pdf
- Le « Quit Facebook Day »
  - A rassemblé environ 30,000 personnes
    - http://www.quitfacebookday.com/
- Verizon vs. « Narcissistic Vulnerability Pimps »
    - http://www.theregister.co.uk/2010/04/23/verizon_narcissistic_vulnerability_pimps/
- Une entreprise attaque son fournisseur antivirus en justice pour « inefficacité »
  - Et perd son procès car les employés avaient été infectés par un site pornographique
    - http://www.securityvibes.com/entreprises-juridique-proces-fournisseur-jsaiz-news-3003648.html

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 13 juillet 2010
- N'hésitez pas à proposer des sujets et des salles