OSSIR
Groupe Paris

Réunion du 13 septembre 2011

Revue des dernières vulnérabilités

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

Merci à Ary Paul Kokos

Avis Microsoft

- **Juillet 2011**
  - **4 bulletins, 22 failles**
  - **MS11-053 Faille dans la pile BlueTooth [2]**
    - **Affecte: Windows Vista & Seven**
    - **Exploit: corruption mémoire lors d'une communication BlueTooth avec un périphérique malveillant**
      - **http://blogs.technet.com/b/srd/archive/2011/07/12/ms11-053-vulnerability-in-the-bluetooth-stack-could-allow-remote-code-execution.aspx**
    - **Crédit: n/d**

Avis Microsoft

- **MS11-054 Failles dans WIN32K.SYS (x15) [1]**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit: élévation de privilèges locale**
  - **Crédit:**
    - **Tarjei Mandt / Norman (x14)**
    - **Mr. Liang Yin, Prof. Sihan Qing, Weiping Wen, Mr. Husheng Zhou / Department of Information Security, Beijing University**

- **MS11-055 Faille dans Visio [1]**
  - **Affecte: Visio 2003 SP3**
  - **Exploit: *DLL Preloading* à l'ouverture d'un document Visio**
  - **Crédit: n/d**

Avis Microsoft

- MS11-056 Faille dans CSRSS (x5) [1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: élévation de privilèges locale
    - http://blogs.technet.com/b/srd/archive/2011/07/12/ms11-056-vulnerabilities-in-the-client-server-runtime-subsystem-and-console-host.aspx
    - AllocConsole()
    - SrvSetConsoleLocalEUDC()
    - SrvSetConsoleNumberOfCommand()
    - SrvWriteConsoleOutput()
    - SrvWriteConsoleOutputString()
    - http://j00ru.vexillium.org/?p=893
    - http://j00ru.vexillium.org/?p=971
    - http://mysterie.fr/blog/2011/07/31/cve-2011-1281/
  - Crédit: Matthew 'j00ru' Jurczyk / Hispasec Virustotal

Avis Microsoft

- **Août 2011**
  - **13 bulletins, 22 failles**
    - **http://blogs.technet.com/b/srd/archive/2011/08/09/assessing-the-risk-of-the-august-2011-security-updates.aspx**
  - **MS11-057 Failles dans Internet Explorer (x8) [1]**
    - **Affecte: Internet Explorer (toutes versions supportées)**
    - **Exploit:**
      - **Exécution de code par corruption mémoire**
        - **ZDI-11-247, ZDI-11-248**
        - **http://lostmon.blogspot.com/2011/08/internet-explorer-6-7-and-8-windowopen.html**
      - **Evasion triviale de la sandbox**
        - **ZDI-11-249**
        - **Utilisée lors du concours pwn2own**
        - **Création d'un processus avec IL=0 => échec de la sandbox**
    - **Crédit:**
      - **Yngve N. Pettersen / Opera**
      - **Lostmon Lords**
      - **Makoto Shiotsuki / Security Professionals Network Inc.**
      - **Anonymous / ZDI**
      - **Stephen Fewer / Harmony Security + ZDI (x2)**
      - **Michal Zalewski / Google**

Avis Microsoft

- MS11-058 Failles dans le serveur DNS (x2) [3]
  - Affecte: Windows (toutes versions serveur)
  - Exploit:
    - Corruption mémoire sur une requête NAPTR malformée
    - Exécution de code à distance … dans certaines conditions
      - http://blogs.technet.com/b/srd/archive/2011/08/09/vulnerabilities-in-dns-server-could-allow-remote-code-execution.aspx
      - https://community.qualys.com/blogs/securitylabs/2011/08/23/patch-analysis-for-ms11-058
  - Crédit: Grischa Zengel / Zengel Medizintechnik GmbH

- MS11-059 Faille dans Windows Data Access Components [1]
  - Affecte: Windows Seven / 2008 R2
  - Exploit: *DLL Preloading*
    - Exploitable à l'ouverture d'un fichier Excel
  - Crédit: n/d

Avis Microsoft

- **MS11-060 Failles Visio (x2) [1]**
  - **Affecte: Visio (toutes versions supportées sauf Viewer)**
  - **Exploit: corruption mémoire à l'ouverture d'un document malformé**
  - **Crédit: Linlin Zhao / Baidu Security Team**

- **MS11-061 Faille dans Remote Desktop Web Access [1]**
  - **Affecte: Windows 2008 R2**
  - **Exploit: XSS**
  - **Crédit: Sven Taute**

Avis Microsoft

- **MS11-062 Faille dans le pilote NDISTAPI (service RAS)**
  - **Affecte: Windows XP / 2003**
  - **Exploit: élévation de privilèges locale**
  - **Crédit: Lufeng Li / Neusoft Corporation**

Avis Microsoft

- MS11-063 Faille dans CSRSS [1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: élévation de privilèges locale
  - Crédit: Alex Ionescu / Winsider Seminars & Solutions Inc
    - Cf. Recon 2011

- MS11-064 Failles dans TCP/IP (x2) [3]
  - Affecte: Windows Vista / 2008 / Seven / 2008 R2
  - Exploit: déni de service
    - Paquet ICMP malformé
    - Accès à une URL malformée (si "URL-based QoS" est actif)
      - http://technet.microsoft.com/en-us/library/dd637810(WS.10).aspx
  - Crédit: n/d

Avis Microsoft

- MS11-065 Faille RDP [3]
  - Affecte: Windows XP / 2003
  - Exploit: déni de service par un paquet RDP malformé
  - Crédit: n/d

- MS11-066 Faille dans le contrôle "Chart" [3]
  - Affecte: contrôle "Chart"
    - Disponible dans .NET Framework 4.0
    - Installable sur .NET Framework 3.5 SP1
  - Exploit: lecture de fichiers arbitraires dans une application ASP.NET
  - Crédit: Nico Leidecker, James Forshaw / Context Information Security

Avis Microsoft

- **MS11-067 Faille dans le contrôle "Microsoft Report Viewer" [3]**
  - **Affecte: Visual Studio 2005**
  - **Exploit: XSS**
  - **Crédit: Adam Bixby / Gotham Digital Science**

- **MS11-068 Faille noyau [?]**
  - **Affecte: Windows Vista / 2008 / Seven / 2008 R2**
  - **Exploit: déni de service lors de la lecture de métadonnées malformées**
  - **Crédit: Zheng Wenbin / Qihoo 360 Security Center**

Avis Microsoft

- **MS11-069 Faille .NET [?]**
  - **Affecte: .NET Framework (toutes versions supportées sauf 1.1SP1 et 3.5SP1)**
  - **Exploit: accès illimité au *namespace* System.Net.Sockets**
  - **Crédit: Michael J. Liu**

Prévisions pour septembre 2011

- **Les bulletins ont été publiés par erreur ☺**
  - **MS11-070: faille WINS**
  - **MS11-071: *DLL Preloading***
  - **MS11-072: failles dans Excel (x6)**
  - **MS11-073: failles dans Office (x2)**
  - **MS11-074: failles dans SharePoint (x6)**
  - **http://isc.sans.edu/diary.html?storyid=11551**

Avis Microsoft

- Advisories
  - Q2562937 Kill Bits
    - CheckPoint / SSL VPN On-Demand
    - IBM / ActBar
    - Honeywell / EBI R Web Toolkit
  - Q2269637 *DLL Preloading*
    - V9.0 : ajout du bulletin MS11-059
    - V8.0 : ajout du bulletin MS11-055
  - Q2607712 Suppression de l'autorité racine "DigiNotar"
    - V1.0: publication de l'avis
    - V2.0: correction documentaire
    - V3.0: publication d'un correctif dans Windows Update

Avis Microsoft

- **Révisions**
  - **MS11-068**
    - **V1.1: Server Core non affecté**
  - **MS11-063**
    - **V1.1: correction d'un lien**
  - **MS11-059**
    - **V1.1: précision sur la nécessité d'un redémarrage**
  - **MS11-056**
    - **V1.1: ajout d'un problème connu**
  - **MS11-052**
    - **V1.1: changement de la logique de détection**
  - **MS11-050**
    - **V1.1: ce bulletin corrige également un memory leak**
  - **MS11-049**
    - **V2.0: changement de la logique de détection**
  - **MS11-045**
    - **V1.1: suppression de 2 workarounds**
  - **MS11-043**
    - **V2.0: nouvel installeur du correctif, "plus stable"**
  - **MS11-027**
    - **V1.1: ajout du CLSID lié au contrôle WMITools dans les workarounds**
  - **MS11-025**
    - **V4.0: Visual Studio 2010 SP1 est également affecté**
  - **MS09-035**
    - **V3.1: changement de la méthode de détection pour les redistribuables VS**
  - **MS08-069**
    - **V4.0: ajout de MSXML 4.0 sur Windows 7 SP1 et Windows 2008R2 SP1 comme produits affectés**

Infos Microsoft

- **Sorties logicielles**
  - **Windows 2008 R2 HPC Edition**
  - **MDOP 2011 R2**

Infos Microsoft

- Autre
  - $200,000 pour stimuler la protection contre les corruptions mémoire
    - http://www.microsoft.com/security/bluehatprize/
  - $250,000 pour retrouver les auteurs de Rustock
    - http://blogs.technet.com/b/microsoft_blog/archive/2011/07/18/microsoft-offers-reward-for-information-on-rustock.aspx
  - Microsoft dévoile de nombreux détails sur Windows 8
    - http://blogs.msdn.com/b/b8/
    - http://blogs.msdn.com/b/b8_fr/
    - Windows 8
      - … aura un AppStore
      - … aura une application de virtualisation native et gratuite
      - … supportera l'UEFI pour assurer l'intégrité du démarrage
      - … démarrera en 3 secondes

Infos Microsoft

- *Mitigating Software Vulnerabilites*
  - http://go.microsoft.com/?linkid=9776900
- Microsoft ouvre un centre de recherche sur la sécurité en Allemagne
  - http://www.bulletins-electroniques.com/actualites/67465.htm
- Microsoft vs. Gmail
  - http://channelnomics.com/2011/07/29/microsoft-finds-sense-humor-%E2%80%98gmail-man%E2%80%99/
- La Xbox 360 victime d'une attaque hardware ?
  - http://www.h-online.com/security/news/item/Hackers-claim-to-have-beaten-Xbox-360-security-1333597.html
- Vendre Windows Phone …
  - http://www.youtube.com/watch?v=5hmaX2YCFWc

Infos Réseau

- (Principales) faille(s)
  - Cisco Unified Communication Manager
    - http://www.cisco.com/warp/public/707/cisco-sa-20110824-cucm.shtml
    - http://www.cisco.com/warp/public/707/cisco-sa-20110824-cucm-cups.shtml
  - Cisco Intercompany Media Engine
    - (Même faille que la précédente, mais dans un autre produit)
      - http://www.cisco.com/warp/public/707/cisco-sa-20110824-ime.shtml

Infos Réseau

- Autres infos
  - Il va être possible d'acheter nazi.fr
    - Et plein d'autres …
      - http://www.afnic.fr/obtenir/chartes/fondamentaux
  - Commotion, le réseau du futur
      - http://www.lemonde.fr/technologies/article/2011/08/30/commotion-le-projet-d-un-internet-hors-de-tout-controle_1565282_651865.html

Infos Unix

- (Principales) faille(s)
  - Déni de service Apache
    - http://archives.neohapsis.com/archives/fulldisclosure/2011-08/0203.html
    - Il s'agit d'une faille de 2007 qui n'a jamais été corrigée
      - http://seclists.org/bugtraq/2007/Jan/83
  - Ruby on Rails < 3.0.10
    - http://www.ruby-forum.com/topic/2373312
  - PHP < 5.3.7
    - http://www.php.net/archive/2011.php#id2011-08-18-1
    - Ne migrez pas, la crypto est cassée …
      - http://www.h-online.com/security/news/item/PHP-users-warned-not-to-upgrade-to-5-3-7-1327427.html
    - Entre temps la 5.3.8 est sortie
  - Note: PHP 5.2 n'est plus supporté

Infos Unix

- Autre
  - Kernel.org piraté
    - Les attaquants ont eu accès au système pendant au moins 3 semaines
      - http://pastebin.com/BKcmMd47
  - Linux Foundation et Linux.com (aussi) piratés
    - http://www.phoronix.com/scan.php?page=news_item&px=OTg5Ng
  - Linux 3.0 est sorti
    - Et Linux 3.1 est déjà en préparation
      - https://plus.google.com/102150693225130002912/posts/CJpyYdCqBL8
      - (Et oui, Linus Torvalds est sur Google+)
  - emacs viole la GPL
    - http://lists.gnu.org/archive/html/emacs-devel/2011-07/msg01155.html

Failles

- **Principales applications**
  - **Apple iOS < 4.3.4**
    - **Corrige le dernier *jailbreakme.com***
  - **Apple iOS < 4.3.5 #epic #fail**
    - **Ne valide pas la chaine de certification, mais seulement le dernier certificat (SSL/TLS)**
      - **http://support.apple.com/kb/HT4824**
      - **http://blog.recurity-labs.com/archives/2011/07/26/cve-2011-0228_ios_certificate_chain_validation_issue_in_handling_of_x_509_certificates/**
      - **https://www.trustwave.com/spiderlabs/advisories/TWSL2011-007.txt**
    - **Un correctif est aussi disponible pour les iPhone jailbreakés ☺**
  - **Apple Safari < 5.0.6, < 5.1**
    - **ZDI-11-239, ZDI-11-240, ZDI-11-241, ZDI-11-242, ZDI-11-243**
      - **http://support.apple.com/kb/HT4808**
  - **Apple QuickTime < 7.7**
    - **ZDI-11-250, ZDI-11-251, ZDI-11-252**
    - **ZDI-11-254, ZDI-11-255, ZDI-11-256, ZDI-11-257, ZDI-11-258, ZDI-11-259**
      - **http://support.apple.com/kb/HT4826**

Failles

- Adobe Flash Player < 10.3.183.5, AIR < 2.7.1
  - ZDI-11-253, ZDI-11-276
    - http://www.adobe.com/support/security/bulletins/apsb11-21.html
  - Plus de 400 failles de sécurité découvertes par Google (!)
    - http://googleonlinesecurity.blogspot.com/2011/08/fuzzing-at-scale.html
    - http://www.adobe.com/support/security/bulletins/apsb11-21.html
- Adobe Flash Player < 10.3.183.7
  - A priori pas un correctif de sécurité
    - http://forums.adobe.com/message/3883150
- Adobe ShockWave < 11.6.1.629
    - http://www.adobe.com/support/security/bulletins/apsb11-19.html
- Adobe Flash Media Server
    - http://www.adobe.com/support/security/bulletins/apsb11-20.html
- Adobe PhotoShop
    - http://www.adobe.com/support/security/bulletins/apsb11-22.html
- Adobe RoboHelp
    - http://www.adobe.com/support/security/bulletins/apsb11-23.html

Failles

- Oracle Quaterly Patches
  - http://www.oracle.com/technetwork/topics/security/cpujuly2011-313328.html
- Faille *conceptuelle* dans Java RMI
  - http://dev.metasploit.com/redmine/issues/4738
- Java 1.6.27
  - A priori pas un correctif de sécurité
    - http://www.oracle.com/technetwork/java/javase/6u27-relnotes-444147.html

Failles

- FireFox < 3.6.20
  - ZDI-11-270, ZDI-11-271
    - http://www.mozilla.org/security/announce/2011/mfsa2011-30.html
- FireFox 6.0 / ThunderBird 6.0
- Chrome < 13.0.782.215
    - http://googlechromereleases.blogspot.com/2011/08/stable-channel-update_22.html
- WireShark < 1.4.8, < 1.6.1
    - http://www.wireshark.org/news/20110718.html
- RealPlayer
  - ZDI-11-265 … ZDI-11-269
- HP Easy Printer Care (contrôle ActiveX … assez répandu)
  - ZDI-11-261

Failles

- Oracle "Secure" Backup
  - Injection de *commandes* dans le login
    - ZDI-11-238
- BlackBerry Administration API
    - http://btsc.webapps.blackberry.com/btsc/search.do?cmd=displayKC&docType=kc&externalId=KB27258
- Citrix Access Gateway
  - XSS
    - http://support.citrix.com/article/CTX129971
- Citrix XenApp & XenDesktop
  - Faille dans le service XML
    - http://support.citrix.com/article/CTX129430
- VMWare ESX
    - http://www.vmware.com/security/advisories/VMSA-2011-0010.html
- TeeChart Professional (contrôle ActiveX)
  - Utilisé dans certains systèmes SCADA
  - Pas de correctif
    - http://www.stratsec.net/Research/Advisories/TeeChart-Professional-Integer-Overflow

Failles 2.0

- Un journaliste fait fuir le mot de passe permettant de déchiffrer tous les contenus de WikiLeaks
  - Malgré ses engagements
    - http://www.wikileaks.org/Guardian-journalist-negligently.html
- THC vs. Vodafone
    - http://wiki.thc.org/vodafone
- Anonymous vs. Facebook
  - C'est pour le 5 novembre
    - http://www.20min.ch/ro/multimedia/stories/story/15170576
- Chine vs. Reste du monde
    - http://www.theepochtimes.com/n2/china-news/slip-up-in-chinese-military-tv-show-reveals-more-than-intended-60619.html
- TruePosition
    - http://www.wired.com/dangerroom/2011/07/global-phone-tracking/all/1/

Failles 2.0

- **Compromission en masse de sites osCommerce**
  - **http://twitter.com/#!/_MDL_/statuses/10214465333530816**
- **Les pratiques douteuses du *marketing* en ligne**
  - **http://www.theregister.co.uk/2011/08/24/comscore_privacy_lawsuit/**
- ***Phishing* contre les clients SecurID**
  - **http://www.net-security.org/malware_news.php?id=1783**
- ***Phishing* via un chat MSN**
  - **http://virtualabs.fr/spip.php?article52**

Sites piratés

- **Les sites piratés du mois**
  - **La plus grosse brèche de tous les temps au Pentagone**
    - **http://www.foxnews.com/politics/2011/07/14/pentagon-discloses-largest-ever-cyber-theft/**
    - **http://www.msnbc.msn.com/id/43757768/ns/technology_and_science-security/t/pentagon-discloses-largest-ever-cyber-theft/**
  - **Des données confidentielles de l'OTAN**
    - **Dérobées par #anonymous**
      - **https://twitter.com/#!/AnonymousIRC/status/94012787705122816**
  - **Les données personnelles de 35 millions de coréens**
    - **Via un opérateur télécom**
      - **http://slashdot.org/story/11/07/28/1810222/35-Million-SK-Telecom-Accounts-Stolen-By-Chinese-Hackers**
  - **Orange bénéficie d'un audit de tous ses sites en ligne gratuitement ☺**
    - **http://www.zataz.com/news/21521/HiddenTapz--orange--afai--Association-Francaise-de-l-Audit-et-du-Conseil-Informatiques.html**
    - **http://pastebin.com/GCH0r6f5**

Sites piratés

- DigiNotar … et d'autres ?
  - Une autorité de certification néerlandaise, reconnue par tous les navigateurs
  - Génération de faux certificats utilisés dans des attaques contre GMail en Iran
  - L'histoire complète:
    - http://www.vasco.com/company/press_room/news_archive/2011/news_diginotar_reports_security_incident.aspx
    - http://isc.sans.edu/diary.html?storyid=11500
    - http://blogs.technet.com/b/srd/archive/2011/09/04/protecting-yourself-from-attacks-that-leverage-fraudulent-diginotar-digital-certificates.aspx
  - L'histoire racontée par le pirate:
    - http://pastebin.com/SwCZqskV
    - http://pastebin.com/85WV10EL
    - http://pastebin.com/jhz20PqJ
    - http://pastebin.com/1AxH30em
  - L'autorité a été complètement supprimée des OS et/ou navigateurs …
    - Firefox 6.0.1, ThunderBird 6.0.1
      - http://support.mozilla.com/en-US/kb/deleting-diginotar-ca-cert
    - Windows (KB2607712)
    - Mac OS X
  - D'autres autorités également piratées ?
    - http://www.theregister.co.uk/2011/09/07/diginotar_hacker_proof/
    - http://www.mag-securs.com/News/tabid/62/articleType/ArticleView/articleId/28760/GlobalSign-cesse-d-etablir-des-certificats-suite-a-l-affaire-DigiNotar.aspx

Sites piratés

- CERN
  - Le mot de passe était dans la documentation en ligne …
    - http://reversemode.com/index.php?option=com_content&task=view&id=78&Itemid=0
  - Heureusement le pirate est un "gentil" …
- Vanguard
    - http://pastebin.com/PjiXmwNk
- Antisec shot the Sheriff
    - https://vv7pabmmyr2vnflf.tor2web.org/
- L'unité de police CNAIPIC
    - http://pastebin.com/r21cExeP
- Elysee.fr
    - http://www.telegraph.co.uk/news/worldnews/nicolas-sarkozy/8666800/Nicolas-Sarkozys-Elysee-Palace-website-hacked.html
- Le système de vote électronique en Floride
    - http://www.informationweek.com/news/security/attacks/231001248
- UPS, TheRegister, Acer, Telegraph, Vodafone, …
    - http://zone-h.org/news/id/4741

Sites piratés

- Google.gp (Guadeloupe)
  - http://www.zone-h.org/mirror/id/14877986
- Le ministère coréen de la réunification
  - http://french.yonhapnews.co.kr/techscience/2011/08/09/0700000000AFR20110809001400884.HTML
- Epson (Corée)
  - http://www.zdnet.fr/actualites/epson-pirate-350-000-clients-touches-en-coree-39763210.htm
- Nokia Developer
- Jouve
  - http://www.thehackernews.com/2011/07/jouve-group-hacked-by-inj3ct0r-team.html
- VKontakte
  - Par une intrusion … physique
    - https://twitter.com/#!/e_kaspersky/status/108272230437363712
- … et probablement plein d'autres

Malwares et spam

- Le ver Morto recherche les authentifiants triviaux via RDP
  - Personne n'avait automatisé RDP avant lui => gros carton
    - http://www.theregister.co.uk/2011/08/28/morto_worm_spreading/
- L'opération "Shady RAT"
  - Une vaste exfiltration de données analysée par McAfee
    - http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf
  - Attention aux effets d'annonce
    - http://www.symantec.com/connect/blogs/truth-behind-shady-rat
- Le matériel infecté en usine inquiète le DHS
    - http://technology.newsplurk.com/2011/07/dhs-imported-gadgets-possibly-include.html

Malwares et spam

- AVG sur Windows Phone 7 est-il lui-même un malware ?
  - En tout cas il a été retiré du Market
    - http://www.pcinpact.com/actu/news/65623-windows-phone-7-avg-antivirus-spyware.htm
- Kaspersky possède un brevet … sur le filtrage antispam
  - http://www.kaspersky.com/about/news/virus/2011/Kaspersky_Lab_Patents_Effective_Anti-Spam_Technology_in_the_USA
- Voler un code PIN … avec une caméra thermique ?
  - http://www.darknet.org.uk/2011/08/stealing-atm-pin-numbers-using-thermal-imaging-cameras/
- Voler un code de déverrouillage … avec un accéléromètre ?
  - http://www.theregister.co.uk/2011/08/17/android_key_logger/

Actualité (francophone)

- **Le retour du Grand Firewall**
  - **http://www.pcinpact.com/actu/news/65558-grand-firewall-chinois-france-blocage-dns.htm**
- **Nouvelle jurisprudence sur l'email en entreprise**
  - **http://www.pcinpact.com/actu/news/65356-cour-de-cassation-employeur-salarie-email-courrier.htm**
- **Un *serial hacker* s'attaque aux sites Web des préfectures**
  - **http://www.pcinpact.com/actu/news/65398-piratage-prefecture-internet-civilise.htm**
- **IPv6: le gouvernement français va donner l'exemple**
  - **http://www.itespresso.fr/ipv6-eric-besson-souhaite-que-l-etat-donne-l-exemple-45540.html**
- **Oberthur racheté par le fond d'investissement Advent**
  - **http://www.zdnet.fr/actualites/oberthur-sur-le-point-d-etre-cede-au-fonds-advent-pour-plus-d-1-milliard-d-euros-39762905.htm**
- **EdenWall en liquidation**
  - **http://www.societe.com/societe/edenwall-technologies-452215015.html**

Actualité (anglo-saxonne)

- Le problème avec les hackers
  - C'est qu'ils préfèrent travailler pour Google que pour l'état
    - http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8635959/Whizz-kids-deserting-the-spy-world-as-threat-of-attacks-increases.html

Actualité (européenne)

- **ENISA vs. HTML5**
  - **http://www.computerworld.com/s/article/358181/European_Group_Finds_HTML5_Security_Gaps**

Actualité (Google)

- Google rachète la division mobiles de Motorola
  - Pour $12 Mds
- Kees Cook passe d'Ubuntu chez Google
  - http://www.outflux.net/blog/archives/2011/09/12/5-years-with-canonical/
- Google fait comme les autres
  - Il donne les données aux américains dans le cadre du Patriot Act
    - http://news.softpedia.com/news/Google-Admits-Handing-over-European-User-Data-to-US-Intelligence-Agencies-215740.shtml
- Google+, c'est déjà fini ?
  - http://www.linformaticien.com/actualites/id/21440/google-lasserait-deja-les-internautes.aspx
- Google lance un magazine en ligne
  - Trimestriel
    - http://www.thinkwithgoogle.com/

Actualité (Apple)

- Steve Jobs démissionne
  - http://www.reuters.com/article/2011/08/24/us-apple-jobs-letter-idUSTRE77N86K20110824
- Comex (Jailbreakme.com) en stage chez Apple
- Corée: plainte collective pour géolocalisation abusive
  - http://french.yonhapnews.co.kr/techscience/2011/08/17/0700000000AFR20110817001800884.HTML
- Apple gagne la bataille du Flash
  - Flash Media Server est désormais compatible iOS
    - http://gigaom.com/apple/the-day-apple-won-the-flash-fight/
- A venir sous peu …
  - iOS 5 (avec iCloud)
  - iPhone 5 (le 7 octobre ?)
  - iPad 3 (en 2012)
  - iPhone "low cost"

Actualité (crypto)

- AES affaibli ?
  - Plus théorique que pratique pour le moment
    - http://www.computerworld.com/s/article/9219297/AES_proved_vulnerable_by_Microsoft_researchers?taxonomyId=17
- Le Pakistan veut interdire toute forme de chiffrement
    - www.techdirt.com/articles/20110729/03142715310/reports-claim-that-pakistan-is-trying-to-ban-encryption-under-telco-law.shtml

Actualité

- Conférences

  - BlackHat US / Defcon
    - Tavis Ormandy vs. Sophos
      - http://lock.cmpxchg8b.com/Sophail.pdf
    - Charlie Miller implante un malware dans la batterie des MacBooks
    - Grosse faille SAP/J2EE
    - "Wartexting" contre voitures connectées
    - Des failles et des *easter eggs* dans les SCADA Siemens
      - http://www.wired.com/threatlevel/2011/08/siemens-hardcoded-password/
    - Abus du service de géolocalisation Microsoft
      - Après celui de Google …
      - http://elie.im/blog/privacy/using-the-microsoft-geolocalization-api-to-retrace-where-a-windows-laptop-has-been/
      - http://blogs.technet.com/b/privacyimperative/archive/2011/08/01/microsoft-makes-change-to-geographic-location-positioning-service.aspx

Actualité

  - Concours de cassage de mots de passe
    - http://contest.korelogic.com/stats.html
  - ATM en rade (sans lien avec le contenu des conférences :)
    - http://twitpic.com/61issz
  - Supports BlackHat
    - http://blackhat.com/html/bh-us-11/bh-us-11-archives.html
  - Supports DEFCON
    - http://www.reddit.com/tb/jfqhj
    - http://good.net/dl/k4r3lj/DEFCON19/

- Usenix
  - Projet Telex
    - https://telex.cc

- Recon
  - Alex Ionescu vs. CSRSS

- Le programme du CCC commence à se construire
  - Cassage en direct du GPRS ?
    - http://www.h-online.com/security/news/item/GPRS-connections-easily-tapped-1321018.html

Actualité

- **Sorties logicielles**
  - **Mac OS X "Lion" (10.7)**
    - **Un système plus sûr … et qui converge avec iOS**
      - **http://arstechnica.com/apple/reviews/2011/07/mac-os-x-10-7.ars/1**
    - **Intègre les Push Notifications**
      - **TCP/5223**
    - **Déjà une faille dans le FireWire**
      - **http://www.lostpassword.com/pdf/pr-110726.pdf**
    - **… et dans l'authentification LDAP**
      - **http://www.h-online.com/security/news/item/Mac-OS-X-Lion-fails-to-check-passwords-when-authenticating-via-LDAP-1328704.html**
  - **Java 1.7**
    - **Avec des bogues connus …**
  - **VMWare vSphere 5**

Actualité

- smiasm *reverse engineering framework*
  - http://code.google.com/p/smiasm/
- Metasploit 4.0
- FireCat 2.0
  - http://www.firecat.fr/
- Putty 0.61
  - http://linux.slashdot.org/story/11/07/13/0530255/PuTTY-061-Released
- THC-Hydra 6.5
- Cain 4.9.42
- BackBox Linux 2.0
  - http://www.backbox.org/content/backbox-linux-2-released
- NFSpy
  - http://www.pentestit.com/2011/07/27/nfspy-idspoofing-nfs-client-tool/

Actualité

- Mozilla lance BrowserID
- Injection … dans la couche physique
  - http://travisgoodspeed.blogspot.com/2011/09/remotely-exploiting-phy-layer.html
- L'état des procès dans la téléphonie mobile
  - http://www.readwriteweb.com/mobile/2011/08/chart-of-the-day-who-is-suing.php
- PCI/DSS prend en compte la virtualisation
  - https://www.pcisecuritystandards.org/pdfs/pci_pr_20110614.pdf

Fun

- Le choix d'un bon mot de passe fait débat
  - http://xkcd.com/936/
- La solution aux problèmes d'archivage
  - Un DVD-R en pierre
    - http://actu.pcastuces.com/afficheactu.asp?Id=18836
- Sony va proposer une solution d'authentification forte pour l'accès aux comptes de ses joueurs
  - Fournisseur: Vasco
    - http://www.securityvibes.fr/marche-business/sony-authenticator/
- Faut-il afficher la version de Firefox ?
  - Le débat fait rage …
    - https://bugzilla.mozilla.org/show_bug.cgi?id=678775
- Mieux que le procès
  - Le duel
    - http://notch.tumblr.com/post/9038258448/hey-bethesda-lets-settle-this

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 11 octobre 2011
- N'hésitez pas à proposer des sujets et des salles
- L'appel à communications pour la JSSI 2012 est sorti
  - Thème: *L'intrusion, outil essentiel de la SSI ?*
  - Deadline pour les soumissions: 5 décembre 2011