OSSIR
Groupe Paris

Réunion du 13 novembre 2012

Revue des dernières vulnérabilités

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

Avis Microsoft

- **Octobre 2012**

  - **MS12-064 Failles dans Word (x2) [1]**
    - **Affecte: Word 2003 / 2007 / 2010 / Viewer / Compatibility Pack / SharePoint 2010 / Office Web Apps 2010**
    - **Exploit:**
      - **Exécution de code à l'ouverture d'un document Word malformé**
      - **Exécution de code à l'ouverture d'un document RTF malformé**
    - **Crédit:**
      - **Anonymous + ZDI**
      - **Anonymous + SecuriTeam**

  - **MS12-065 Faille dans Works [1]**
    - **Affecte: Works 9**
    - **Exploit: *heap overflow***
    - **Crédit: n/d**

Avis Microsoft

- MS12-066 XSS [1]
  - Affecte: InfoPath 2007 / 2010, SharePoint 3.0 / 2007 / 2010, Groove 2010, Office Web Apps 2010, Communicator 2007 R2, Lync 2010
  - Exploit: XSS
  - Crédit: Drew Hintz / Google

- MS12-067 Failles dans Oracle FAST Search Server (x13) [1]
  - Affecte: FAST Search Server for SharePoint 2010 SP1
  - Exploit: exécution de code lors de l'ouverture d'un document malformé
  - Crédit: Will Dorman / CERT/CC

Avis Microsoft

- **MS12-068 Faille noyau [3]**
  - **Affecte: Windows (toutes versions supportées sauf 8 et 2012)**
  - **Exploit: *integer overflow***
  - **Crédit: Anonymous + iDefense**

- **MS12-069 Déni de service dans Kerberos [1]**
  - **Affecte: Windows 7 & 2008R2**
  - **Exploit: pointeur NULL**
  - **Crédit: n/d**

- **MS12-070 XSS [1]**
  - **Affecte: SQL Server (toutes versions supportées … ou presque)**
  - **Exploit: XSS dans Server Report Manager**
  - **Crédit: n/d**

Avis Microsoft

- Advisories
  - Q2661254 Clés RSA < 1024 bits interdites
    - V2.0: le correctif a effectivement été déployé automatiquement
  - Q2737111 Exchange, FAST Search Server for SharePoint
    - V3.0: le correctif a été publié
  - Q2749655 Problème d'horodatage des correctifs
    - http://blogs.technet.com/b/srd/archive/2012/10/09/security-advisory-2749655-and-timestamping.aspx
    - V1.0: publication du bulletin
    - V1.1: mise à jour documentaire (Windows 8 et 2012)
  - Q2755801 IE 10 est livré avec une version vulnérable de Flash
    - V2.0: ajout de KB2758994
    - V3.0: publication du correctif KB2758994 pour Windows RT

Avis Microsoft

- Prévisions pour Novembre 2012
  - 6 bulletins (5 critiques)
  - Windows, IE, .NET, Office, et Windows RT affectés
- Failles antérieures
- Failles à venir
  - Des failles noyau à gogo …
    - http://j00ru.vexillium.org/?p=1169
    - http://j00ru.vexillium.org/?p=1393
  - … pas que théoriques
    - http://code.google.com/p/bypass-x64-dse/downloads/list
  - Faille IE9 (dans l'afficheur de source)
    - http://www.exploit-db.com/exploits/22401/

Avis Microsoft

- Révisions
  - MS12-043
    - V3.0: MSXML 4.0 est vulnérable si installé sur Windows 8 ou 2012
    - V3.1: précision pour les versions RC de Windows 8 et 2012
  - MS12-053
    - V2.0: problème d'horodatage *
    - V2.1: ajout d'une entrée de FAQ
  - MS12-054
    - V2.0: problème d'horodatage *
    - V2.1: ajout d'une entrée de FAQ
  - MS12-055
    - V2.0: problème d'horodatage *
    - V2.1: ajout d'une entrée de FAQ
  - MS12-058
    - V2.0: problème d'horodatage *
    - V2.1: ajout d'une entrée de FAQ
  - MS12-066
    - V1.1: correction documentaire (numéro de KB)
    - V1.2: correction documentaire (numéro de KB)
    - V1.3: SharePoint 3.0 SP3 est vulnérable

Infos Microsoft

- **Sorties logicielles**
  - **Windows 8**
    - **SMB 3.0 supporte nativement le chiffrement**
      - **http://www.lemagit.fr/technologie/stockage-technologie/san-nas/2012/10/18/ce-quil-faut-savoir-sur-smb-3-0-le-nouveau-protocole-de-partage-de-fichiers-de-microsoft/**
  - **Office 2013**
  - **Windows Server 2012 "Essentials"**
  - **Dynamics NAV 2013**
  - **Xbox Music**

Infos Microsoft

- **Autre**
  - **Lancement de Windows 8**
    - **"C'est la queue pour l'iPad mini" ?**
      - **http://www.zdnet.com/uk/windows-8-london-launch-is-this-a-queue-for-the-ipad-mini-7000006440/**
  - **Google vs. Windows 8**
    - **http://www.google.com/homepage/windows8/**
  - **Y aura-t-il un "Surface Phone" fabriqué par Microsoft ?**
    - **http://www.phonearena.com/news/Microsoft-possibly-testing-its-own-Windows-Phone-8-smartphone-evidence-suggests_id35283**

Infos Microsoft

- Que faisait Microsoft au lieu d'innover ?
  - Lutter contre la cybercriminalité …
    - http://www.gizmodo.fr/2012/11/07/cybercriminalite-retard-strategie-mobile-microsoft.html
- Microsoft pense qu'il y aura 100,000 applications dans son "Store" pour Windows 8 d'ici le 1er janvier 2013
  - Contre 3,500 actuellement
    - http://www.zdnet.com/microsoft-sales-exec-promises-100000-windows-8-apps-by-january-2013-7000005401/
- Steven Sinofsky quitte Microsoft
  - 23 ans de service
  - Patron de la division Windows

Infos Microsoft

- Security Intelligence Report, volume 13
  - Rise of the Keygen ☺
- MSN va être remplacé par Skype
- Skype aurait livré illégalement des informations à la police
    - http://thehackernews.com/2012/11/skype-illegally-handed-over-alleged.html
- Les résultats financiers de Microsoft
  - Les ventes de Windows chutent d'un tiers
    - http://www.linformaticien.com/actualites/id/26735/microsoft-publie-des-resultats-en-demi-teinte.aspx
- Pourquoi le Nigeria ?
    - http://research.microsoft.com/pubs/167719/WhyFromNigeria.pdf

Infos Réseau

- (Principales) faille(s)
  - Cisco
    - Contournement TACACS+
      - http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20121107-acs
  - Mac OS X, Windows XP et Windows 2012 vulnérables au "RA Flood"
      - http://samsclass.info/ipv6/proj/projL9-flood-router.htm

Infos Réseau

- **Autres infos**
  - **La saga Huawei et ZTE**
    - **Déclaré "Persona non grata" aux USA et au Canada**
      - **http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf**
    - **Cisco arrête son partenariat avec ZTE**
      - **http://www.linformaticien.com/actualites/id/26600/cisco-rompt-son-partenariat-avec-zte-qui-affirme-etre-transparent.aspx**
    - **Huawei propose aux australiens l'accès au code source**
      - **Après avoir fait de même avec les anglais en 2010**
    - **ZTE stoppe ses projets d'investissement à Poitiers**
      - **http://www.lanouvellerepublique.fr/Vienne/Actualite/Economie-social/n/Contenus/Articles/2012/10/29/Poitiers-ZTE-et-le-cyber-espionnage-selon-Jean-Marie-Bockel**
  - **Alcatel-Lucent licencie 15% de son effectif en France malgré tout**
    - **… mais c'est la faute à Free Mobile !**
      - **http://www.usinenouvelle.com/article/l-arrivee-de-free-a-place-alcatel-en-situation-de-grande-difficulte-selon-arnaud-montebourg.N185877**

Infos Réseau

- Une intervention sur les failles dans les routeurs HP et Huawei annulée (à la demande de HP)
  - Kurt Grutzmacher, Toorcon 2012
- 22 octobre 2012: panne d'Amazon EC2
  - Affecte: Reddit, Coursera, Flipboard, FastCompany, Heroku, Airbnb, Github, Vyou …
- The Pirate Bay version "Cloud"
    - http://torrentfreak.com/pirate-bay-moves-to-the-cloud-becomes-raid-proof-121017/
- NBS lance CerberHost
    - http://www.nbs-system.com/cerberhost-le-cloud-ultra-securise-de-nbs-system
- AT&T + IBM = encore un nouveau Cloud
  - Prévu en janvier 2013

Infos Réseau

- Seul 12% des sites de l'administration américaine sont compatibles IPv6
  - Objectif initial: 100% au 30 septembre 2012
    - http://www.zdnet.fr/services/mobile/actualites/ipv6-la-transition-prend-l-eau-aux-etats-unis-39783075.htm
- Verizon va loin
  - "Nous vendrons toutes les données sur nos clients mobiles"
    - http://news.cnet.com/8301-13578_3-57533001-38/verizon-draws-fire-for-monitoring-app-usage-browsing-habits/
- http://open-root.eu/
  - Une hiérarchie parallèle à celle de l'ICANN
- http://me.ga/
  - Pas encore sorti, déjà saisi …
- Stéphane Bortzmeyer sauve culturecommunication.gouv.fr et communication.gouv.fr
  - Le domaine n'avait pas été renouvelé à temps …

Infos Unix

- (Principales) faille(s)
  - Régression dans Ruby
    - open("/etc/passwd\0.txt")
      - http://www.ruby-lang.org/en/news/2012/10/12/poisoned-NUL-byte-vulnerability/
  - Drupal < 7.16
    - Exécution de code PHP
      - http://packetstormsecurity.org/files/117470
  - Exim
    - Faille dans le support DKIM
      - https://bugzilla.redhat.com/attachment.cgi?id=633222&action=diff
  - "systemd" a une dépendance avec "libmicrohttpd" et "qrencode-libs"
      - http://thread.gmane.org/gmane.linux.redhat.fedora.devel/169082

Infos Unix

- **Autre**
  - **"Address Sanitizer" pour GCC**
    - **Poussé par Google**
      - **http://gcc.gnu.org/ml/gcc-patches/2012-11/msg00088.html**
  - **Debian Code Search**
      - **http://codesearch.debian.net/**
  - **OpenBSD 5.2**
    - ***"OpenBSD 5.2 has been released and is available for download. One of the most significant changes in this release is the replacement of the user-level uthreads by kernel-level rthreads, allowing multithreaded programs to utilize multiple CPUs/cores."***

Failles

- **Principales applications**
  - **Java < 1.6.37, < 1.7.9**
    - **http://www.oracle.com/technetwork/topics/security/javacpuoct2012-1515924.html**
    - **Toutes les failles d'Adam Gowdiak ne sont pas corrigées**
      - **http://www.security-explorations.com/en/SE-2012-01-status.html**
    - **[0day]**
      - **http://weblog.ikvm.net/PermaLink.aspx?guid=23cced47-ccdb-460d-acc9-ce16154ab6a5**
  - **QuickTime < 7.3.3**
    - **Bravo à Kevin @ QuarksLab ☺**
      - **http://support.apple.com/kb/HT5581**
  - **Flash Player < 11.5**
    - **http://www.adobe.com/support/security/bulletins/apsb12-24.html**
  - **FireFox < 16.0.2**
    - **https://www.mozilla.org/security/announce/**
    - **La version précédente n'est restée que quelques heures en ligne**
      - **http://arstechnica.com/security/2012/10/firefox-16-vulnerability-attack-code-available-online/**
  - **Chrome < 23**

Failles

- Oracle Quaterly Patch
  - http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html
- Une faille Adobe vendue $50,000 par des russes
  - Non patchée, évasion complète de la sandbox …
  - … et utilisée dans une campagne d'infection massive
- [NGS00267] Compte "secret" dans Symantec Messaging Gateway
  - Accessible en SSH
    - http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=2012&suid=20120827_00

Failles 2.0

- Un "0day" dure en moyenne … 10 mois
  - http://www.forbes.com/sites/andygreenberg/2012/10/16/hackers-exploit-software-bugs-for-10-months-on-average-before-theyre-fixed/
- L'usage de SSL dans les applications Android
  - Un #fail …
    - http://www2.dcsec.uni-hannover.de/files/android/p50-fahl.pdf
- L'implémentation de SSL dans les librairies standard
  - Un #fail …
  - "CURL: this interface is almost perversely bad"
    - http://www.cs.utexas.edu/~shmat/shmat_ccs12.pdf
- Une faille VUPEN exploitée au Bahrain
  - https://citizenlab.org/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/
- Le "TOP 10" des failles détectées par Qualys
  - Mais d'où viennent ces statistiques ?
    - https://www.qualys.com/research/top10/
- Des terminaux de paiement backdoorés chez Barnes & Noble
  - 63 magasins concernés
    - http://www.barnesandnobleinc.com/press_releases/10_23_12_Important_Customer_Notice.html

Failles 2.0

- "Do Not Track", une information marketing comme les autres ?
  - http://www.zdnet.com/the-do-not-track-standard-has-crossed-into-crazy-territory-7000005502/
- Un employé Verizon volait les photos des clients sur leur portable
  - Lors des maintenances en magasin
    - http://updates.gawker.com/post/34998266352/verizon-employee-arrested-for-stealing-naked-pictures
- Jack Barnaby vs. Pacemakers
  - Accessibles via une transmission RF à 400MHz
  - … et piratés à 15m de distance
- Pour info: ventes de SmartPhones Q3 2012
  1. Samsung: 35%
  2. Apple: 16,6%
  3. Autre

Sites piratés

- **Les sites piratés du mois**
  - **Le site Euromillions.fr**
    - **La FDJ indique qu'elle est le seul opérateur de jeux en France à détenir la norme ISO27001, *"le plus haut standard en matière de sécurité informatique"* (sic)**
  - **GhostShell vs. Gouvernement russe**
    - **#OpBlackStar**
      - **http://pastebin.com/yXN7uc6r**
  - **Le registrar "punto.pe" (200 000 domaines)**
    - **Victime de Lulzsec Peru**
  - **Le registrar du ".gp" (Guadeloupe)**
      - **http://pastebin.com/gWdnzakx**
  - **ImageShack (et d'autres)**
    - **"*That being said, ImageShack has been completely owned, from the ground up. We have had root and physical control of every server and router they own. For years.*"**
      - **http://htp4.hack-the-planet.tv/htp4/HTP-4.txt**

Sites piratés

- **L'état de Caroline du Sud**
  - **3,6 millions de numéro de SS**
    - **http://www.theverge.com/2012/10/26/3560140/south-carolina-cyber-attack-3-6-million-social-security-numbers**
- **Un site de la NASA**
  - **http://pastebin.com/iDHbESD4**
- **La police italienne**
  - **http://hackmageddon.com/2012/10/25/anonymous-leaks-3500-private-docs-from-italian-police/**
  - **http://thehackernews.com/2012/10/anonymous-hackers-leaks-135gb-italian.html**
- **MoD (UK)**
  - **http://pastebin.com/vRFPQkzR**
- **L'armée du Bengladesh (www.army.mil.bd)**
  - **http://pastebin.com/Yk9bdaLj**
- **unescoetxea.org, www.mt.gov, www.la.gov, www.texas.gov, fhpr.osd.mil, etc.**
  - **http://thehackernews.com/2012/10/hacker-dump-database-from-us-government.html**

Sites piratés

- Anonymous
  - #OpDPB: des FAI qui bloquent TPB (ex. Tele2)
    - http://pastebin.com/QtPhg2Ru
  - #OpGreece
    - "Those funky IBM servers don't look so safe now, do they... We have new guns in our arsenal. A sweet 0day SAP exploit is in our hands and oh boy we're gonna sploit the hell out of it. Respectz to izl the dog for that perl candy."
      - http://www.anonpaste.me/anonpaste2/index.php?96dca2501712c2bd#7zC3Gk22bl9xGtQbWaaWEeEu46UElidVHWqL/lUNV+0=
  - #OpVendetta, #OpMayhem
    - 5 novembre
    - 48 sociétés (dont ATOS)
      - http://nopaste.me/paste/697739606507 72d611d34e

Sites piratés

- Faille sérieuse chez Paypal
  - http://www.scmagazine.com.au/News/321584,paypal-security-holes-expose-customer-card-data-personal-details.aspx
- Une liste de personnalités grecques ayant des comptes en Suisse
  - http://darkernet.in/list-of-greek-business-people-and-politicians-with-alleged-secret-swiss-bank-accounts/
- Le code source du noyau VMWare ESX disponible en torrent
  - Version de 2004
    - http://1337x.org/torrent/421062/VMware-ESX-Server-Kernel-LEAKED/
  - … et ça n'est pas bon
    - http://resources.infosecinstitute.com/vmware-esx-audit-analysis-part-1/
- Rapport final sur l'intrusion chez Diginotar
  - http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/08/13/black-tulip-update/black-tulip-update.pdf
- Facebook: panne DNS ou hack ?
  - http://www.mag-securs.com/News/tabid/62/articleType/ArticleView/articleId/29394/Panne-Facebook-probleme-de-DNS-ou-hack.aspx

Malwares, spam et fraudes

- Sophos #epic #fail
  - Fallait pas énerver Tavis Ormandy
    - https://lock.cmpxchg8b.com/sophailv2.pdf
  - Cisco Ironport est affecté en rebond
    - http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20121108-sophos
  - (Et probablement d'autres)

- Chevron infecté par Stuxnet
    - http://blogs.wsj.com/cio/2012/11/08/stuxnet-infected-chevrons-it-network/

- Malcon 2012
  - Présentation du 1er malware pour Windows Phone 8
    - http://www.malcon.org/
  - … ainsi que d'un malware capable d'utiliser une smartcard connectée

- Gh0st RAT est de retour
  - … derrière une Bbox ☺
    - http://blog.fireeye.com/research/2012/11/backdooraddnew-darkddoser-and-gh0st-a-match-made-in-heaven.html

Malwares, spam et fraudes

- Un auteur de malwares Android arrêté à Amiens
  - 17 000 victimes, 500 000 euros de revenus …
    - Il a 20 ans
      - http://www.01net.com/editorial/578167/un-hacker-francais-arrete-pour-avoir-cree-des-virus-pour-android/
- Le gouvernement allemand recrute … le développeur du Trojan fédéral
    - http://www.heise.de/newsticker/meldung/Zollkriminalamt-sucht-Trojaner-Programmierer-1742835.html
    - http://stellenanzeige.monster.de/GetJob.aspx?JobID=115736705
- McAfee va licencier
  - Accusés: les mauvaises ventes de PC, et l'antivirus gratuit de Windows 8 (?!)
      - http://www.reuters.com/article/2012/10/08/us-intel-mcafee-jobs-idUSBRE89718G20121008
- John McAfee recherché pour meurtre au Belize
    - http://www.wired.com/threatlevel/2012/11/threatlevel_1112_mcafee/

Actualité (francophone)

- CNIL vs. …
  - Google+
    - http://www.cnil.fr/nc/la-cnil/actualite/article/article/regles-de-confidentialite-de-google-une-information-incomplete-et-une-combinaison-de-donnees/
  - Drones
    - http://www.cnil.fr/la-cnil/actualite/article/article/usages-des-drones-et-protection-des-donnees-personnelles/
- ANSSI
  - Chez manufacturing.fr
    - http://www.ssi.gouv.fr/fr/menu/actualites/la-securite-des-systemes-industriels-s-invite-chez-manufacturing-fr.html
- Fusion de la DISIC et de la DGME
- Fusion du CSA et de l'ARCEP ?
  - Seulement si la neutralité des réseaux est abandonnée (pour le CSA)
    - http://www.csa.fr/index.php/Etudes-et-publications/Les-autres-rapports/Contribution-du-CSA-a-la-reflexion-sur-l-evolution-de-la-regulation-de-l-audiovisuel-et-des-communications-electroniques

Actualité (francophone)

- Il y aura un Conseil National du Numérique 2.0
  - http://www.latribune.fr/technos-medias/internet/20121009trib000723816/fleur-pellerin-va-presenter-un-grand-plan-numerique-.html
- Nouvelle idée: le Cloud doit payer la taxe sur la copie privée
  - http://www.culturecommunication.gouv.fr/content/download/49040/384519/file/AVIS%20Informatique%20dans%20les%20nuages.pdf
- Typosquatting: cnrs.fr -> crns.fr
  - https://aresu.dsi.cnrs.fr/IMG/pdf/alerte-11-10-2012.pdf
- Surcouf liquidé ☹
  - Ainsi que Joystick
  - Et bientôt Dane-Elec ?

Actualité (anglo-saxonne)

- AMD + Honeywell + Intel + Lockheed Martin + RSA + …
  - = Cyber Security Research Alliance
    - http://www.cybersecurityresearch.org/
- Le vote par fax et par email …
    - http://www.lemonde.fr/technologies/article/2012/11/06/le-new-jersey-autorise-le-vote-par-courriel-ou-par-fax_1786487_651865.html
- Facebook pour s'authentifier sur les sites du gouvernement UK ?
    - http://mobile.computerworlduk.com/news/security/3402273/facebook-id-will-give-access-to-govuk-websites/
- Le DHS va créer une "cyber réserve"
    - http://www.reuters.com/article/2012/10/31/net-us-usa-cybersecurity-reserve-idUSBRE89U16Z20121031
- Le GCHQ recrute chez les joueurs de jeux vidéos
    - http://securityaffairs.co/wordpress/9650/security/uk-recruits-xbox-generation-youngsters-for-cyber-war-games.html
- "Safe Online Surfing"
    - https://sos.fbi.gov/
- J-31 chinois == F-35 américain
    - http://french.ruvr.ru/2012_11_08/93961238/

Actualité (européenne)

- Le "reverse engineering" légal en Europe ?
  - http://pro.01net.com/editorial/577457/le-reverse-engineering-autorise-par-la-cour-de-justice-europeenne/
- "*Reducing terrorist use of the Internet*" (draft)
  - http://www.cleanitproject.eu/new-draft-document-for-vienna-workshop/
- Protection des données personnelles en Europe
  - http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fr.pdf
- 51 pannes de réseau en Europe en 2011
  - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2011/
- Mise à jour de la liste des CERT européens
  - http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

Actualité (Google)

- **Pwnium 2**
  - **Pinkie Pie 2 – Google 0**
    - **http://googlechromereleases.blogspot.fr/2012/10/stable-channel-update_6105.html**
  - **Une faille d'écriture de fichiers arbitraire …**
    - **http://src.chromium.org/viewvc/chrome/branches/1229/src/chrome/browser/renderer_host/chrome_render_message_filter.cc?r1=161037&r2=161036&pathrev=161037**
- **Google vs. Taxe sur le référencement de la presse**
  - **https://docs.google.com/file/d/0B92admnS83NKc3pULU5DZkdzQnM/edit?pli=1**
- **Les (mauvais) résultats de Google publiés une heure trop tôt**
  - **L'action chute de 10% (soit 20 Md$)**
- **Le Cloud n'empêchera pas le contrôle fiscal de Google en France**
  - **http://www.legalis.net/spip.php?page=breves-article&id_article=3505**

Actualité (Apple)

- Le plugin Java n'est plus installé par défaut sur Mac OS X 10.7 et 10.8
  - Effet du dernier patch
- Le nouveau câble de l'iPhone 5 déjà piraté
  - Malgré une authentification hardware
    - http://micgadget.com/30569/apples-authentication-chip-for-lightning-cable-has-been-successfully-cloned-video/
- OVH (hubic) vs. Apple (iCloud)
    - http://forum.ovh.com/showthread.php?t=83630
- Revenus Apple > somme(Google, Microsoft, Facebook)
    - http://www.nytimes.com/2012/10/26/technology/apple-profits-rise-24-on-iphone-5-sales.html
- Annonces
  - iPad Mini, iPad 4, …
  - Plus de lecteur de CD/DVD dans les MacBooks
- Pas encore annoncé
  - Une iRadio en ligne

Actualité (Apple)

- iOS 6: ce qu'Apple avait oublié d'annoncer …
  - IDFA: IDentifier For Advertising

Actualité (crypto)

- "Il n'y aura pas d'ordinateur quantique"
  - Source: le prix Nobel de physique 2012
    - http://www.larecherche.fr/content/recherche/article?id=21095
- Publication de la clé maitresse de la PS3
    - http://pastie.org/private/bevpt5jf9kdjg3vrrv05w
    - http://blogs.securiteam.com/index.php/archives/1928
- Les clés DKIM de Google (et d'autres ?) sont du RSA-512
    - http://www.wired.com/threatlevel/2012/10/dkim-vulnerability-widespread/all/
- Le "patent troll" qui tue
  - TQP a breveté la génération de clés de session en 1995
    - http://arstechnica.com/security/2012/11/patent-suits-target-google-intel-hundreds-more-for-encrypting-web-traffic/

Actualité (crypto)

- Vol de données entre VMs
  - Par une attaque "side channel" testée
    - http://blog.cryptographyengineering.com/2012/10/attack-of-week-cross-vm-timing-attacks.html
- Faille dans le client TOR
  - memset() est parfois "optimisé" par le compilateur …
    - http://www.h-online.com/open/news/item/Security-issue-discovered-in-TOR-client-Update-1746884.html
- Cryptocat est une blague
    - https://blog.crypto.cat/2012/11/security-update-a-follow-up/

Actualité (crypto)

- TrustedLabs fourni à Samsung un TPM EAL7
  - Evalué par le CEA LETI et l'ANSSI
    - http://bourse.lci.fr/bourse-en-ligne.hts?urlAction=bourse-en-ligne.hts&idnews=BNW121101_00005665&numligne=0&date=121101&source=BNW
- NIST: Guidelines on Hardware Rooted Security in Mobile Devices (Draft)
    - http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf
- Les mots de passe en image
    - http://xato.net/wp-content/xup/passwordscloud.png
- Le meilleur code PIN ?
  - 8068
    - http://www.datagenetics.com/blog/september32012/index.html

Actualité

- Conférences passées
  - HITB KUL
    - http://conference.hitb.org/hitbsecconf2012kul/materials/
  - Hack.Lu
    - http://archive.hack.lu/2012/
  - GreHack
    - http://grehack.org/
  - ASFWS
    - http://2012.appsec-forum.ch/
- Conférences à venir
  - JSSI de l'OSSIR
    - Le CFP est ouvert !
      - http://www.ossir.org/jssi/index/jssi-2013-appel-a-communications.shtml

Actualité

- **Sorties logicielles**
  - **Adobe Reader XI**
    - **http://blogs.adobe.com/adobereader/2012/10/adobe-reader-xi-now-available.html**
  - **Autopsy 3.0**
  - **Nessus 5.0.2**
    - **Avec interface HTML5 (beta)**

Actualité

- Kaspersky met au point son propre OS
  - Industriel et garanti sans faille (!)
    - http://eugene.kaspersky.com/2012/10/16/kl-developing-its-own-operating-system-we-confirm-the-rumors-and-end-the-speculation/
- Amazon pourrait acheter la division "OMAP" de TI
    - http://slashdot.org/story/12/10/15/143247/amazon-considering-buying-texas-instruments-chip-business
- Facebook ne paie pas assez d'impôts
    - http://www.guardian.co.uk/technology/2012/oct/10/facebook-uk-taxes
- Twitter filtre désormais la visibilité par pays
  - Après avoir perdu un procès en Allemagne
    - http://www.independent.co.uk/life-style/gadgets-and-tech/news/twitter-uses-new-countrywithheld-content-rule-to-block-neonazi-group-tweets-in-germany-8216260.html
- Qui est le premier constructeur mondial de PC ?
  - Lenovo pour Gartner
  - HP pour IDC
    - http://www.linformaticien.com/actualites/id/26632/lenovo-1er-constructeur-mondial-de-pc-devant-hp-oui-pour-gartner-non-pour-idc.aspx

Divers

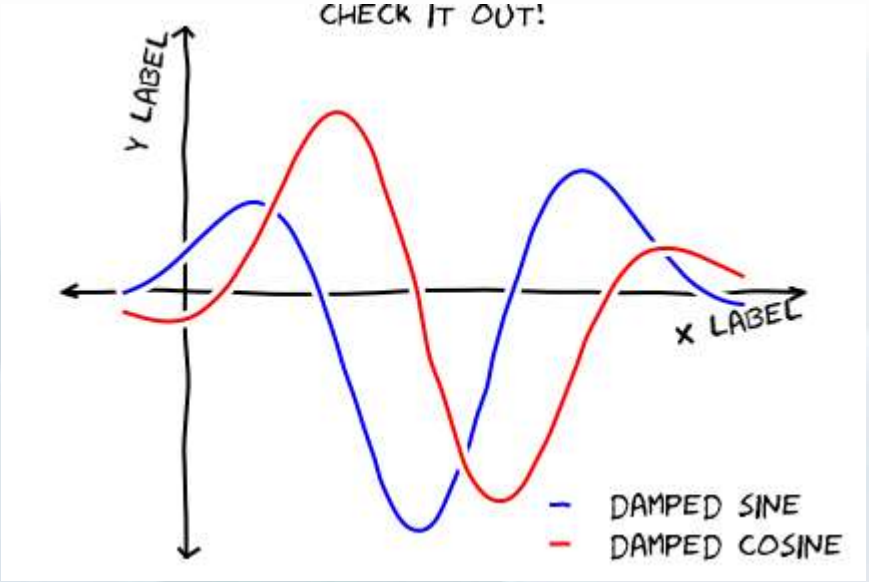
- **$500 si vous piratez votre TV Samsung sous Android**
  - **https://www.samsungtvbounty.com/**
- **Penser à son mot de passe peut être dangereux**
  - **https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final56.pdf**
- **Le Pape est sur Twitter**
  - **http://thenextweb.com/twitter/2012/11/09/benedict-xvi-reportedly-set-to-open-a-personal-twitter-account-by-the-end-of-the-year/**

Divers

- Dragos Ruiu joue … lui-même
  - http://www.imdb.com/title/tt2202700/

Divers

- Générer automatiquement des graphes "xkcd-like"
  - http://jakevdp.github.com/blog/2012/10/07/xkcd-style-plots-in-matplotlib/



Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 11 décembre 2012
- L'OSSIR sur Twitter
    - https://twitter.com/OSSIRFrance
- Conférence JSSI de l'OSSIR
  - Mardi 19 mars 2012
  - Le CFP est ouvert !
    - http://www.ossir.org/jssi/index/jssi-2013-appel-a-communications.shtml