

0-Days ACL Analyse **Audit** **Autorité** **Awareness** Botnets **Buffer** **CERT**

Certificats **Code** Conception Cryptographie Cyber-Attacks DCSSI Defacement

Détection Disclosure **DNS** **DNS**Sec **Education** eID ENISA

Firewall **FIRST** Forensic **Guidance** Hacker ICANN Identity IDS IETF

IFRAME Incidents Internet Intrusion IP **IPSec** **IPV6** ISO ISO27001 ISOC IT

LINUX Mail MD5 **Menaces** Méthodologies **MITM** Mobile-Devices NET PDA

Phishing **Planification** Privacy Proxy RBAC **RFC** RFID **Risques** Rootkits

Sécurité Security **Sensibilisation** SHA1 SmartPhones SPAM **SQL** SSH SSL

TCP Technologies Terrorisme Virtualité Virus **VoIP** WEB2 **WEP** Windows WPA

Veille Technologique Sécurité

Rapport Mensuel N°136

NOVEMBRE 2009

Les informations fournies dans ce document ont été collectées et compilées à partir de sources d'origines diverses et publiquement accessibles: listes de diffusion, newsgroups, sites Web, ...

Ces informations sont fournies pour ce qu'elles valent sans garantie d'aucune sorte vis à vis de l'exactitude, de la précision ou de la qualité de l'information. Les URL associées à certains thèmes sont validées à la date de la rédaction du document.

Dans ce numéro:

COFEE selon Microsoft

Chrome OS

Cloud Computing, les risques

AntiVirus LiveCD

OWASP Top Ten List 2010

RFC5702

Les marques et les produits cités dans ce rapport sont la propriété des dépositaires respectifs.

CONNECTING BUSINESS & TECHNOLOGY

DEVOTEAM – BU Sécurité
1, rue GALVANI
91300 Massy Palaiseau

Pour tous renseignements:
Offre de veille <http://www.devoteam.fr/>
Informations vts-info@veille.apogee-com.fr

©DEVOTEAM Solutions - Tous droits réservés

Au sommaire de ce rapport...

ACTUALITES SECURITE

COFEE SELON MICROSOFT	2
KIT FAMILIAL DE LA SECURITE EN LIGNE	4
CHROME OS DEVOILE	4
MC COLO, UN AN APRES	5

ANALYSES ET COMMENTAIRES

ETUDES

SC2009 – 34 ^{IE} ME TOP 500	7
UNE ETUDE COMPARATIVE DES PERFORMANCES DES ANTI-VIRUS	8
ENISA – SUR LA DISTRIBUTION QUANTIQUE DE CLEFS	9
ENISA – SUR LES RISQUES LIES AU CLOUD COMPUTING	9
ENISA – CARTES D'IDENTITE ELECTRONIQUES ET INTERNET	12

LOGICIELS

OUTILLAGES ANTI-VIRUS	13
-----------------------	----

METHODOLOGIES ET STANDARDS

METHODES

ENISA - COMMENT AMELIORER LA SENSIBILISATION A LA SECURITE DE L'INFORMATION	16
OWASP – LA PROCHAINE TOP TEN LIST	16

RECOMMANDATIONS

NIST - SP800-126 'THE TECHNICAL SPECIFICATION FOR THE SECURITY CONTENT AUTOMATION PROTOCOL'	18
NIST – IR7657 / PRIVILEGE MANAGEMENT	19

STANDARDS

RFC5702 / USE OF SHA-2 ALGORITHMS WITH RSA IN DNSKEY AND RRSIG RESOURCE RECORDS FOR DNSSEC	20
--	----

TABLEAUX DE SYNTHESE

CONFERENCES

OARC 2009	22
OWASP APPSEC 2009 – BRESIL	22
HACK.LU - 2009	23

GUIDES

NIST – ETAT DES GUIDES DE LA SERIE SPECIALE 800	23
CIS - CATALOGUE DE PROCEDURES ET DE TESTS	25
DISA – GUIDES ET CHECK LISTES DE SECURISATION	26

INTERNET

LES DECISIONS DE L'OMPI	27
-------------------------	----

STANDARDS

IETF – LES RFC TRAITANT DIRECTEMENT DE LA SECURITE	28
IETF – LES RFC LIES A LA SECURITE	28
IETF – LES NOUVEAUX DRAFTS TRAITANT DE LA SECURITE	28
IETF – LES MISES A JOUR DE DRAFTS TRAITANT DE LA SECURITE	28

Le mot du rédacteur

Ce mois de novembre aura été plus particulièrement marqué, de notre point de vue, par quatre nouvelles:

Pour la première, la découverte d'un problème dans la conception des protocoles TLS et SSL qui, s'il ne donne pas lieu à une vulnérabilité aisément exploitable, aura une fois de plus mis en évidence « la course à l'annonce » qui règne dans le domaine de la sécurité comme dans bien d'autres domaines.

En deux mots, et au risque de trop simplifier peut être, deux chercheurs travaillant à la résolution d'un problème découvert par l'un d'eux – Marsh Ray – divulguent en urgence leurs travaux pour couper l'herbe sous le pied d'un troisième chercheur – Martin Rex – qui vient d'annoncer sur une liste de l'IETF avoir découvert un problème similaire.

<http://www.ietf.org/mail-archive/web/tls/current/msg03928.html>
http://extendedsubset.com/Renegotiating_TLS.pdf

Pour la seconde, la publication en tant que norme internationale de la norme **ISO 31000:2009** 'Risk management -- Principles and guidelines' et de la révision 2009 du guide **ISO/IEC Guide 73** 'Vocabulaire'. Deux documents dont l'accès est payant comme cela est le cas de la majorité des documents publiés par l'ISO. Ceci est peut être regrettable dans le cas du Guide 73 dont la mise à disposition gratuite aurait peut être contribué à l'harmonisation du vocabulaire en usage dans notre métier.

http://www.iso.org/iso/catalogue_detail.htm?csnumber=43170
http://www.iso.org/iso/catalogue_detail.htm?csnumber=44651

Pour la troisième, la prochaine entrée en vigueur de la directive Européenne '**Vie privée et Communications électroniques**' qui vient compléter la directive de juillet 2002 en imposant notamment la notification des failles de sécurité. Une fois le texte adopté, les Etats membres de l'UE auront 18 mois pour transposer dans leurs législations la directive modifiée par le Parlement européen et validée par le Conseil.

<http://europa.eu/rapid/pressReleasesAction.do?reference=EDPS/09/13&language=FR>

Et pour la dernière, la création de l'observatoire zonal de la sécurité des systèmes d'information – **OzSSI** - de la zone de défense de Paris. Avec celui-ci, l'ANSSI dispose d'un relais dans les sept zones de défense métropolitaines: Paris, Lille, Rennes, Bordeaux, Marseille, Lyon et Metz.

http://www.ssi.gouv.fr/IMG/pdf/ANSSI_Communique_de_presse_lancement_OZSSI.pdf
http://www.ssi.gouv.fr/site_rubrique50.html

Bonne lecture

BERTRAND VELLE

ACTUALITES SECURITE

COFEE SELON MICROSOFT



Il y a un peu plus d'un an, Microsoft annonçait, à grand renfort de publicité, la fourniture à titre gracieux d'un outil d'investigation aux agences gouvernementales qui en feraient la demande. Cet outil dénommé **COFEE** - Computer Online Forensic Evidence Extractor - avait été développé en collaboration avec **Interpol** et le **NW3C** Américain (National White Collar Crime Center).

To help combat the growing number of ways that criminals use computers and the Internet to commit crimes, Microsoft is working with INTERPOL and the National White Collar Crime Center (NW3C) to provide COFEE at no cost to law enforcement agencies in 187 countries worldwide. INTERPOL and NW3C are also working with Florida State University and University College Dublin to continue the research and development that will help ensure that COFEE serves the needs of law enforcement, even as technology evolves.

Beaucoup de choses auront été dites, ou écrites, sur ce mystérieux outil que bien peu de gens auront eu l'occasion d'avoir entre les mains et d'utiliser, chacun lui attribuant des possibilités extraordinaires: capable de court-circuiter les mécanismes de sécurité de Windows selon certains, susceptible d'extraire les données les mieux cachées voire de casser les mots de passe des utilisateurs même selon d'autres...

Les rumeurs auront couru jusqu'à ce début novembre quand un individu bien peu scrupuleux a fini par télécharger cet outil sur un serveur privé dans la seule optique de gagner des crédits lui permettant d'augmenter son plafond de téléchargement, à quelques 1.6To d'après certaines sources...

Les administrateurs du serveur ont rapidement réagi en détruisant le fichier mais le mal était fait et '**COFEE**' s'est vite retrouvé distribué dans le monde entier, partagé sur 'torrent' où nous l'avons trouvé à la seule fin de le tester. Deux distributions étaient accessibles le jour même de l'annonce de la disponibilité du paquetage sur 'torrent', l'un annoncé être l'original chargé sur le serveur privé '**What.Cd**' mais dont le fichier d'installation n'est pas fonctionnel, l'autre contenant l'original et une copie de la distribution déjà installée. Les quelques tests que nous avons mené sur ces deux paquetages montraient qu'à ce moment aucun des deux n'étaient porteur d'un virus connu.

Le paquetage original contient deux répertoires, l'un regroupant les documentations des outils au format Excel, l'autre les résultats de la campagne de validation fonctionnelle de l'outil menée par une équipe du **NW3C**. Quatre fichiers sont présents à la racine du paquetage: le fichier d'installation au format 'msi', deux fichiers au format 'pdf' décrivant les évolutions et l'utilisation de l'outil et enfin un fichier inséré par l'auteur de la fuite contenant le texte suivant:

```
THIS IS A WHAT.CD EXCLUSIVE RELEASE! IF CAUGHT UPLOADING THIS ANYWHERE ELSE, YOU WILL BE DISABLED!!
Microsoft COFEE v1.1.2 (Computer Online Forensics Evidence Extractor)
Release Date.....Sept 2009
Author.....www.nw3c.org
Released By.....DrWeird of Etiv.in
Much love to all my Pirates
//DrWeird
```

Le manuel d'utilisation décrit en détail le fonctionnement de l'outil, lequel est constitué de deux utilitaires complémentaires:

- un installateur, **Cofee.exe**, qui permet dans un premier temps de générer à façon l'environnement d'analyse sur un support amovible de type clef **USB**, puis l'analyse ayant été effectuée, d'assembler un rapport au format XML,
- un client, **Runner.exe** qui, lancé via un fichier autorun.inf, ordonnancera l'ensemble des tâches d'analyse et collectera les résultats.

Deux profils d'analyses ont été définis par le **NW3C** et sont proposés par défaut: un profil permettant la collecte des **données volatiles** et un profil permettant l'acquisition des informations déterminantes dans le cas d'**une réponse à un incident**. Ces profils dictent le choix des outils d'analyse et des options associées. On notera que le document '**NW3C - Validation - Cofee 1.1.2**' présent dans le répertoire '**Validation Studies**' du paquetage original précise que le premier profil n'écrit aucune donnée sur le système de fichiers de la cible à l'exception de quelques modifications de la base de registre. L'utilisation du second profil conduit par contre à la création d'un nouveau fichier, un gestionnaire de périphérique utilisé par l'utilitaire 'handle.exe'.

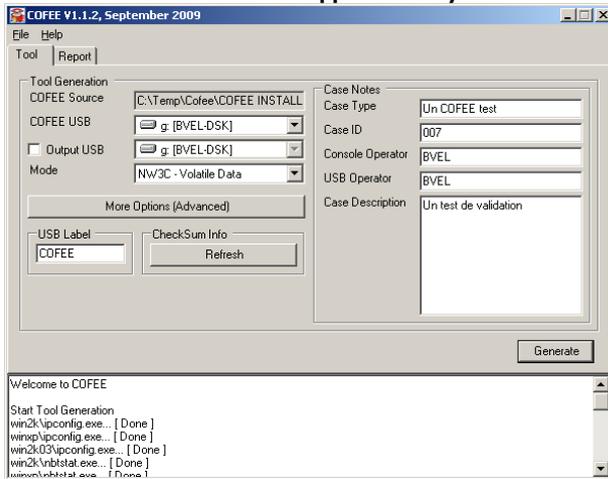
L'étude de la constitution de **Cofee** montre que celui-ci s'appuie sur des utilitaires on ne peut plus classiques pour toute la phase de collecte des informations quand on pouvait s'attendre à l'utilisation d'utilitaires développés sur mesure.

at	Microsoft	Accès à l'ordonnanceur	5.2.3790
arp	Microsoft	Accès à la table ARP	5.2.3790

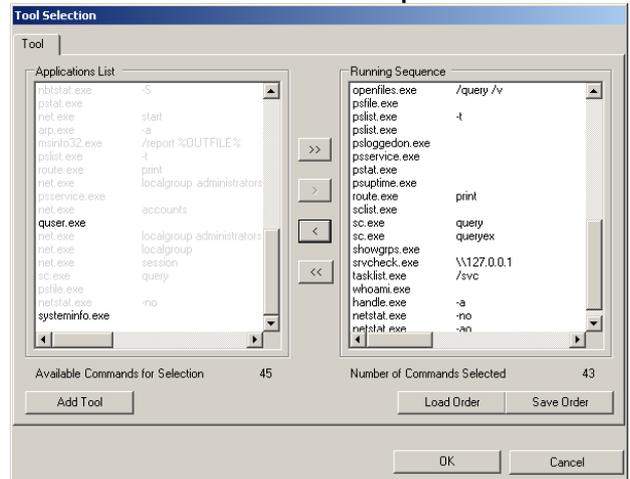
autorunsc	SysInternals	Liste les paramètres de configuration des services	8.53
getmac	Microsoft	Affiche les adresses MAC des interfaces	5.2.3790
handle	SysInternals	Liste les fichiers ouverts sur le système	3.2
hostname	Microsoft	Affiche le nom du système	5.1.2600
ipconfig	Microsoft	Accès aux paramètres de configuration réseau IP	5.2.3790
ipxroute	Microsoft	Accès aux paramètres de configuration réseau IPX	5.1.2600
msinfo32	Microsoft	Liste les informations relatives au système	5.1.2600
nbtstat	Microsoft	Accès aux paramètres de configuration réseau NetBios sur IP	5.2.3790
net	Microsoft	Interpréteur de commande réseau	5.2.3790
netdom	Microsoft	Accès aux paramètres de configuration du domaine	5.0.2184
netstat	Microsoft	Liste les informations concernant les sessions réseau IP	5.2.3790
openfiles	Microsoft	Liste les fichiers ouverts	5.2.3790
psfile	SysInternals	Liste les fichiers ouverts par un système distant	1.01
pslist	SysInternals	Liste les applications et processus en cours d'exécution	1.22
psloggedon	SysInternals	Liste les utilisateurs authentifiés	1.21
pservice	SysInternals	Liste les services	1.01
pstat	SysInternals	Liste tous les processus du système	0.3
psuptime	SysInternals	Affiche la durée de mise sous tension du système	1.1
quser	Microsoft	Liste les utilisateurs	5.2.3790
route	Microsoft	Liste les informations concernant les routages réseau IP	5.1.2600
sc	Microsoft	Accès aux services	5.1.2600
sclist	Microsoft	Liste l'état de tous les services	5.0.14.12
showgrps	NA	Liste les groupes d'appartenance de l'utilisateur	NA
systeminfo	Microsoft	Liste les caractéristiques du système d'exploitation, et les correctifs	5.1.2600
tasklist	Microsoft	Liste les applications et processus en cours d'exécution	5.2.3790
uptime	Microsoft	fiche la durée de mise sous tension du système	1.0.0.1
whoami	Microsoft	Affiche l'identité du propriétaire de la session courante	2.0

Le support d'analyse généré à la demande de l'utilisateur contiendra les seuls outils correspondant au profil sélectionné ainsi qu'une version dédiée au système d'exploitation s'il y a lieu: Windows XP, 2000, 2003 ou Vista.

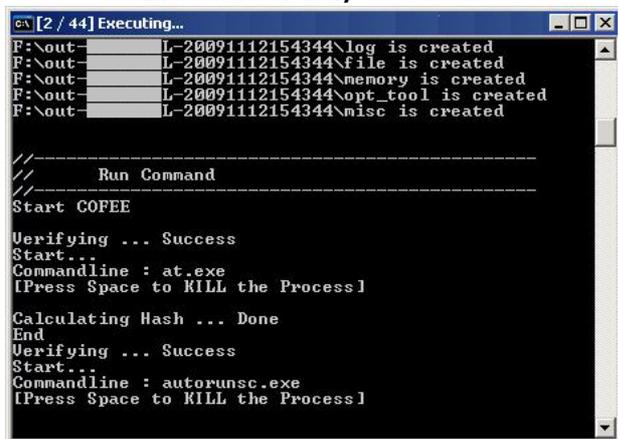
Génération du support d'analyse



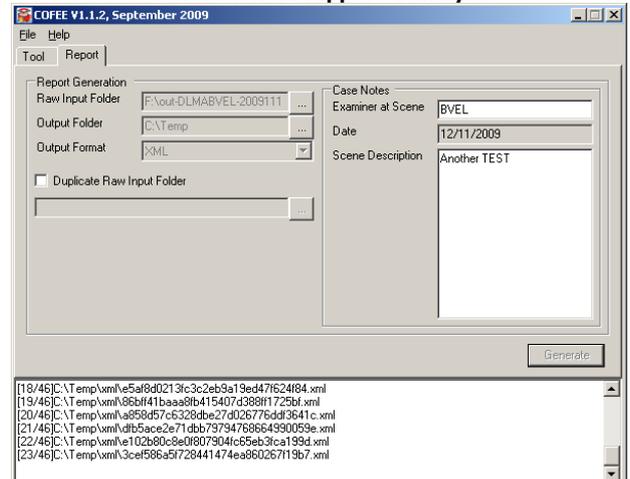
Sélection des utilitaires hors profil de base



Exécution de l'analyse sur la cible



Génération du rapport d'analyse

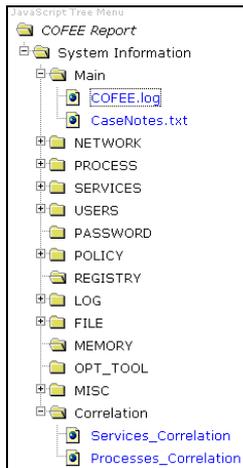


Au final, **COFEE** s'avère être une boîte à outils tout ce qu'il y a de plus classique.

COFEE permet d'automatiser les tâches de collecte d'informations sur un poste de travail Windows, comme bien d'autres applications d'analyses, ni plus ni moins.

Nous devons avouer avoir été déçus par cet outil que nous pensions être bien plus évolué.

Rien ne permet d'affirmer que le packaging diffusé sur Internet soit identique à celui fourni aux agences gouvernementales mais tout laisse à penser que cela est bien le cas.



Rapport d'analyse

Correlate Different Commands among Services

Description				
--Command dumpsec.exe /computer=%COMPUTERNAME% /rpt=services /saveas=tsv /outfile=%Outfile% pservice.exe sclist.exe sc.exe query --Tool Vendor Company -- --Description Correlate Different Commands among Services				
Output				
	PsService	ScList	ScQuery	
Adobe LM Service (Adobe LM Service)	✓	✓	✗	
Alerter (Avertissement)	✓	✓	✗	
ALG (Service de la passerelle de la couche Application)	✓	✓	✓	
AppMgmt (Gestion d'applications)	✓	✓	✗	
aspnet_state (Service d'état ASP.NET)	✓	✓	✗	
Ati HotKey Poller (Ati HotKey Poller)	✓	✓	✓	
AudioSrv (Audio Windows)	✓	✓	✓	
BITS (Service de transfert intelligent en arrière-plan)	✓	✓	✓	
Browser (Explorateur d'ordinateur)	✓	✓	✓	

POUR PLUS D'INFORMATION

<http://arstechnica.com/microsoft/news/2009/04/microsoft-gives-interpol-free-cofee.ars>

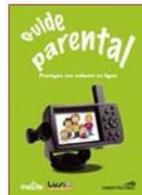
KIT FAMILIAL DE LA SECURITE EN LIGNE



Le projet **Luxembourg Safer Internet**, ou **LUSI**, a pour objectif d'aider les jeunes à mieux utiliser l'Internet par des actions de sensibilisation et l'implication des acteurs nationaux.

C'est dans ce cadre que vient d'être mis à disposition le **'kit familial de sécurité en ligne'**. Celui-ci est constitué des quatre documents suivants:

- un guide de 36 pages à l'attention des jeunes, et des moins jeunes, intitulé 'Brochure ludique pour toute la famille',
- un guide de 39 pages à l'attention des parents intitulé 'Guide parental',
- un quizz proposant 12 situations types sous la forme des cartes qu'il faudra découper,
- un certificat familial qu'il faudra imprimer et signer après avoir décidé des règles d'or qu'il conviendra d'appliquer.



Abondamment illustré, et rédigé en termes simples, ce kit disponible en Français et Allemand doit permettre d'échanger au sein même de la structure familiale en impliquant parents et enfants.

POUR PLUS D'INFORMATION

<http://www.lusi.lu/index.php?id=efamilykit&L=0>

CHROME OS DEVOILE



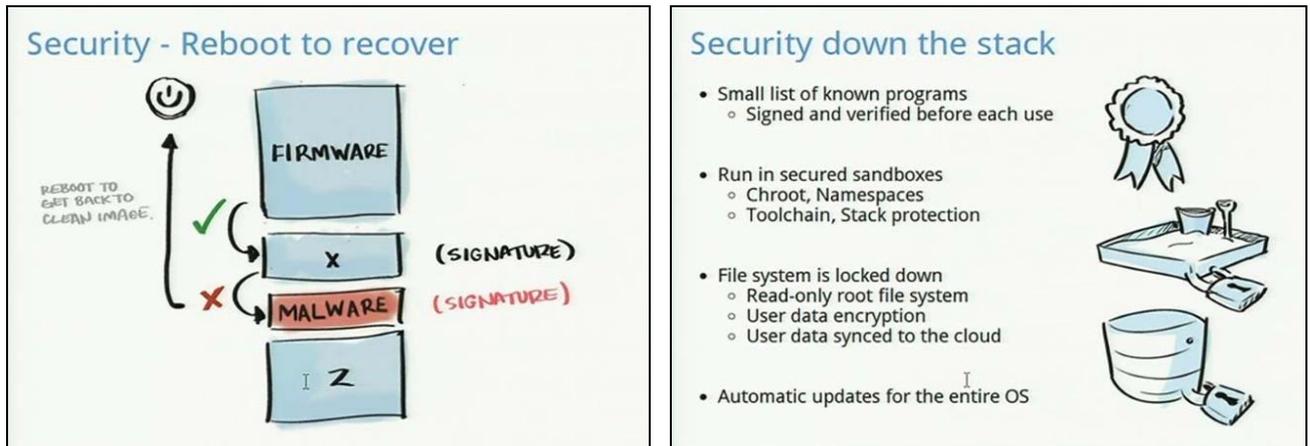
Une conférence de presse tenue le 19 novembre a permis de découvrir **Chrome OS**, le système d'exploitation Google destiné à animer le navigateur **Google Chrome**. S'appuyant sur un noyau Linux, ce système diffusé en source ouverte est prioritairement destiné à être embarqué sur des équipements légers, tel les **NetBooks**.

Allié au navigateur **Google Chrome**, ce système d'exploitation apparaît être une version moderne d'un concept vieux comme l'informatique, ou presque, le terminal de présentation. Une approche fort réussie en son temps par **IBM** et ses fabuleux terminaux **327x**, puis par **France Télécom** et son **Minitel** et enfin par divers constructeurs proposant des **Terminaux X**.

Qu'un problème survienne et il suffira de redémarrer cette **'WEB appliance'**, toutes les données et la configuration étant stockées ailleurs, dans le nuage et chez Google en l'occurrence. Cette approche ne sera pas sans rappeler celle, dite du **SCIT** ou **Self Cleansing and Intrusion Tolerance**, préconisée par une équipe de chercheurs de l'université Georges Massin et suggérant qu'une intrusion doit pouvoir être considérée comme un événement normal et indissociable du fonctionnement d'un système d'information. Auquel cas, la seule parade viable consistera à ramener régulièrement – et de manière totalement transparente pour l'utilisateur – le système dans un état connu et intègre (rapport N°118 – Mai 2008).

Les principes fondamentaux de sécurité ayant dirigé la conception de ce système sont parfaitement

résumés sur deux dessins, dessins extraits de la présentation effectuée devant la presse par le responsable du projet le 19 novembre dernier et reproduits ci-dessous.



Nos lecteurs intéressés pourront aussi regarder une animation présentant les objectifs du système et du navigateur. Les spécialistes du développement de logiciels apprécieront particulièrement la mise à disposition des dossiers de conception du système et du navigateur, dossiers remarquablement détaillés et justifiant chacun des choix effectués, en particulier en ce qui concerne l'analyse de sécurité et le renforcement des mécanismes de sécurité natifs du système LINUX. Une approche suffisamment rare, en particulier de nos jours, pour être soulignée.

POUR PLUS D'INFORMATION

- <http://www.chromium.org/chromium-os>
- <http://www.chromium.org/chromium-os>
- <http://www.chromium.org/Home>
- <http://www.youtube.com/watch?v=0QRO3gKj3qw>
- <http://www.youtube.com/watch?v=5JyFbF7QFIY>

- Annonce de presse
- Projet Open Source Chrome OS
- Projet Open Source Google Chrome
- Vidéo de la présentation du système
- Vidéo de l'annonce du passage en Open Source

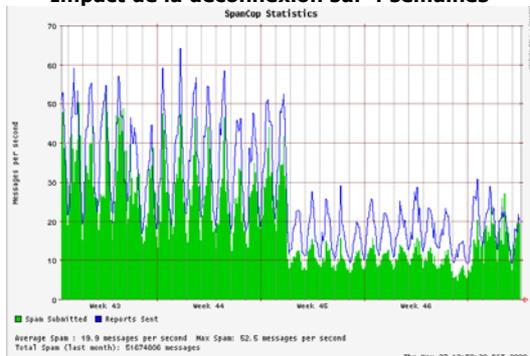
McCOLO, UN AN APRES



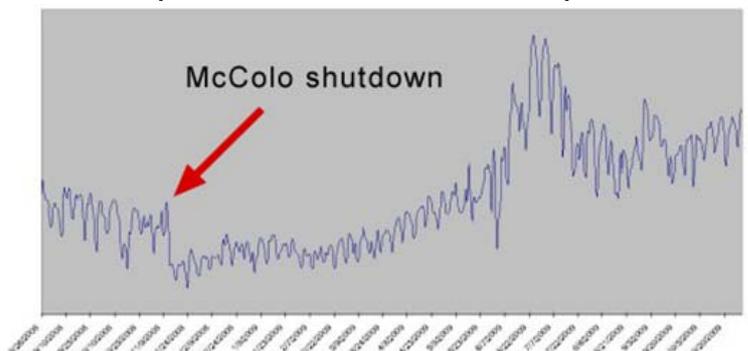
Fin 2008, **McColo**, un important hébergeur ayant pris de trop nombreuses libertés avec l'éthique et la législation se voyait interdit d'exercer son activité.

Sa déconnexion de l'Internet s'était alors immédiatement traduite par une baisse notable du niveau de SPAM, en particulier aux Etats-Unis. Avec maintenant un an de recul, les équipes de l'éditeur **McAfee** se sont posées la question de l'impact réel de cette déconnexion pour conclure, désabusées, qu'il ne s'agissait que d'un répit momentané, un petit événement sans finalement grande importance dans la vie de l'Internet. Et de fait, le volume de SPAM a non seulement très rapidement rejoint le volume d'avant la déconnexion - avril 2009 - pour atteindre en pic en juillet dernier, pic expliqué par l'activité de botnets extrêmement virulents tels **Rustock**, **Srizbi** ou **Mega-D**.

Impact de la déconnexion sur 4 semaines



Impact de la déconnexion sur une année pleine



La complexité de ces systèmes automatisés, et en un certain sens le professionnalisme des organisations opérant ces réseaux, pose un réel problème. Le fait qu'un domaine soit suspendu, ou qu'un provider soit déconnecté, n'aura qu'un impact très temporaire sauf à pouvoir arriver à organiser une opération parfaitement synchronisée sur plusieurs pays et visant plusieurs bureaux d'enregistrement ou opérateurs. La moindre erreur dans une telle opération autorisera la réorganisation du réseau et sa réactivation quelques heures après.

On pourra s'en convaincre en lisant le blog de **Dancho Danchev** qui, après avoir traqué divers réseaux dont **KoobFace**, se trouve être devenu la cible prioritaire de l'organisation opérant celui-ci. Un feuilleton avec ses rebondissements quotidiens opposant un individu à une organisation aux multiples ramifications et qui peut se permettre non seulement de remercier nominativement **Dancho Danchev** pour l'aide apportée dans l'amélioration de l'efficacité de son réseau mais aussi d'enregistrer les domaines utilisés en son nom, ou presque: Pancho Panchev, Vancho Vanchev. En démasquant publiquement ces réseaux, **Dancho Danchev** joue un jeu bien dangereux quand bien même la loi est de son côté.

POUR PLUS D'INFORMATION

<http://www.avertlabs.com/research/blog>

ANALYSES ET COMMENTAIRES

ETUDES

SC2009 – 34^{ÈME} TOP 500



La 34^{ème} liste des 500 calculateurs les plus puissants a été divulguée le 17 novembre durant la conférence **SC09** qui s'est tenue à Portland, Oregon. Mise à jour deux fois l'an, en juin et novembre, depuis 1993 cette liste est la référence des spécialistes des 'number crunchers'.

Les deux supercalculateurs affichant une puissance de calcul supérieure au **petaflops** depuis le 32^{ème} classement effectué en novembre 2008 continuent de se disputer les premières places avec toutefois une modification de taille. En effet, le calculateur **IBM RoadRunner** du département de l'énergie américain – le DoE - laisse après plusieurs années de suprématie la première place à son challenger, le calculateur **Cray XT5 HE**.

Ce dernier est l'héritier du calculateur **XT4** qui avait annoncé en novembre 2008 être le premier calculateur ouvert à la recherche publique à dépasser le seuil des 1000 TFlops. Une machine exceptionnelle utilisant des processeurs Opteron 6 cœurs à 2.6GHz qui aura vu sa puissance dépasser les 2000 TFlops par l'adjonction de 74010 cœurs (soit 12425 processeurs) aux 150152 cœurs déjà installés en juin 2009. Le second calculateur **Cray XT5** classé, celui de l'Université du Tennessee, passe de la 6^{ème} place à la 3^{ème}, ici encore par une augmentation conséquente du nombre de processeurs.

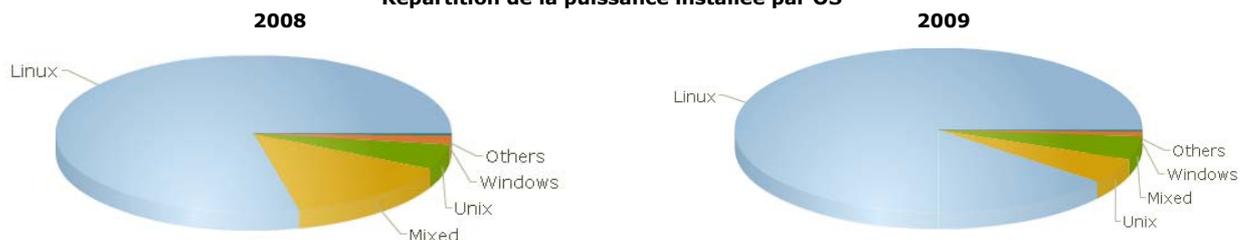
La grande nouveauté s'avère cependant être l'entrée en 5^{ème} position du calculateur chinois **Thiane TH1** du NSCC (National SuperComputer Center). Un calculateur entièrement 'fait main' par le **NUDT** (National University of Defense Technology) autour de processeurs **XEON E554x** tournant à 2.53GHz mais aussi de processeurs spécialisés **Radeon ATI** de la série HD4800. Une approche qui pourrait bien s'avérer être d'une redoutable efficacité dans les mois à venir.

Nos deux premiers calculateurs nationaux passent eux de la 20^{ème} à la 28^{ème} place pour le calculateur du Centre Informatique National de l'Enseignement Supérieur et de la 24^{ème} à la 32^{ème} place pour le calculateur de l'IDRIS à Orsay.

N°	06/09	Cons.	Système	Site	Pays	Core	06/09	TFlops	06/09
1↑	2	CRAY	XT5 HE	Oak Ridge	USA	224162	150152	1759	1 059
2↓	1	IBM	RoadRunner	DOE/NNSA/LANL	USA	122400	129600	1042	1105
3↑	6	CRAY	XT5 HE	NICS/U.Tennessee	USA	98928	66000	831	463
4↓	3	IBM	BlueGene/P	FZJ	DE	294912	294912	825	825
5	-	NUDT	Thiane TH1	NSCC	CN	71680	-	563	-
6↓	4	SGI	Altix 8200	NASA/NAS	USA	56320	51200	544	487
7↓	5	IBM	BlueGene/L	DOE/NNSA/LLNL	USA	212992	212992	478	478
8↓	7	IBM	BlueGene/P	ANL	USA	163840	163840	456	456
9↓	8	SUN	Ranger	Univ. Texas	USA	62976	62976	433	433
10↑	13	SUN	Red Sky	NNSA/Sandia	USA	41616	38208	423	204

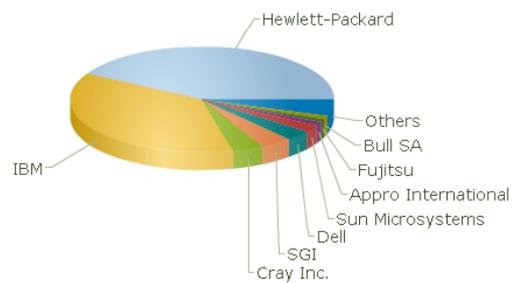
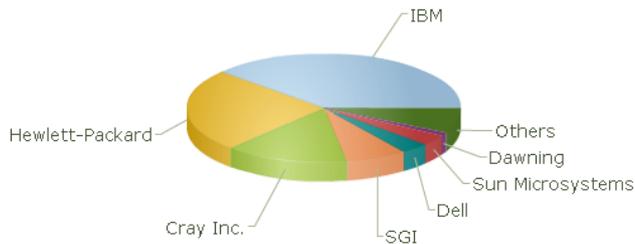
La majorité de ces machines prend la forme de clusters de lames interconnectées par un bus à très haut débit Infiniband, le système d'exploitation LINUX animant l'ensemble. L'utilisation de près de 23% (22% en novembre 2008 et 40% en novembre 2007) des machines listées n'est pas détaillée, la **recherche** 15.6% (14.4% en juin) et la **finance** 9.4% (9.2% en juin) se partageant toutefois les premières places.

Répartition de la puissance installée par OS



Répartition de la puissance installée par vendeurs





POUR PLUS D'INFORMATION

- <http://www.top500.org/lists/2009/11>
- <http://www.top500.org/lists/2009/06>
- <http://www.top500.org/lists/2008/11>
- <http://www.top500.org/lists/2008/06>
- <http://www.top500.org/lists/2007/11>
- <http://www.top500.org/lists/2007/06>
- <http://www.top500.org/lists/2006/11>

- Classement Novembre 2009
- Classement Juin 2009
- Classement Novembre 2008
- Classement Juin 2008
- Classement Novembre 2007
- Classement Juin 2007
- Classement Novembre 2006

UNE ETUDE COMPARATIVE DES PERFORMANCES DES ANTI-VIRUS



En septembre dernier, la société **Passmark Software**, basée en Australie, publiait les résultats d'une étude comparative des performances de plusieurs produits AntiVirus.

Commanditée par la société Symantec (produits Norton), cette étude ne traite nullement de la capacité de détection de produits mais uniquement de l'impact de ceux-ci sur les performances du système hôte. Il est de fait que, par conception, un produit de protection contre les virus, vers et autres codes malveillants ne peut qu'avoir un impact négatif sur les performances. Cet impact est toutefois bien moins perceptible par l'usager de nos jours sur des machines dotées de processeurs bien souvent sous-utilisés qu'il y a encore quelques années quand un processeur simple cœur cadencé au dessous du GHz peinait à animer les applications et un anti-virus.

L'étude '**Internet Security Products Performance Benchmarking - Vista/Dual Core Hardware**' n'en reste pas moins très intéressante au regard de la méthodologie d'analyse employée (détaillée dans l'annexe 1) et des résultats obtenus.

L'environnement de référence est constitué d'un système **Windows Vista** animé par un processeur double cœur et configuré à l'identique pour chacun des onze produits testés dans des versions publiées entre Juin et Septembre 2009, à savoir, classés par ordre décroissant de performance:

N°	Editeur	Produit	Score
1	Norton	Internet Security 2010	146
2	ESET	Smart Security 4	131
3	Kaspersky	Internet Security 2010	119
4	G-Data	Internet Security 2010	110
5	SourceNext	Security Zero 2010	101
6	AVG	Internet Security 8.5	90
7	Panda	Internet Security 2010	89
8	Trend Micro	Internet Security 2010	77
9	F-Secure	Internet Security 2010	65
10	McAfee	Internet Security 2010	69
11	Trend Micro	Virus Buster 2010	59

Nota: On pourra noter ici l'incroyable effort de marketing pour trouver un nom sortant de l'ordinaire. On ne s'étonnera alors plus de la facilité avec laquelle certains usagers tombent dans le piège des 'scarewares', ces faux logiciels anti-virus censés éradiquer une menace inexistante qui, eux, portent un nom réellement différenciateur: Adware Sheriff, Anti VirGear, Anti Spyware Expert, AVGold, Power Antivirus 2009, Totale Secure 2009, ... Une liste de ces faux produits pourra être trouvée [ici](#).

Les performances de ces produits ont été comparées sur 16 points précis représentatifs d'un usage classique, ou d'une fonctionnalité connue pour être consommatrice de ressources.

Boot Time	Impact sur le temps de démarrage.	1 ^{er} : Panda
Scan Speed	Temps d'analyse de 6159 fichiers.	1 ^{er} : Norton
Scan Speed on Solid State Drives	Idem sur disque flash	1 ^{er} : Norton
User Interface Launch Speed	Temps d'initialisation de l'IHM	1 ^{er} : ESET
Memory Usage while Idle	Occupation mémoire résiduelle	1 ^{er} : Norton
Browse Time Test	Impact sur les performances WEB	1 ^{er} : Norton
Internet Explorer Launch Speed	Impact sur le temps d'initialisation IE	1 ^{er} : F-Secure
Installation Time	Plus faible temps d'installation	1 ^{er} : ESET
Installation Size	Plus faible volume occupé sur disque	1 ^{er} : ESET
Registry Key Count	Plus faible nombre de clefs créées	1 ^{er} : Source next
Copying, Moving, Deleting different types of files	Plus faible impact sur les accès	1 ^{er} : Kaspersky
Installation of Third Party Applications	Temps d'installation d'applications	1 ^{er} : Kaspersky
Network Throughput Test	Performance en transfert réseau	1 ^{er} : AVG

File Format Conversion	Conversion format (ie MP3->WAV)	1 ^{er} : Norton
File Compression and Decompression	Temps d'accès fichiers compressés	1 ^{er} : Kaspersky
File Write, Open and Close	Temps d'accès fichier	1 ^{er} : G-Data

Le choix de chacun de ces tests est justifié dans l'introduction de l'étude. Nous n'avons par contre trouvé aucune trace de la règle utilisée pour agréger ces résultats et calculer le score ayant permis de classer les produits. Il en va de même avec la valeur médiane dénommée dans l'étude '**Industry Average**' proposée comme référence de comparaison pour chacun des résultats mais nullement documentée.

POUR PLUS D'INFORMATION

http://www.passmark.com/ftp/antivirus_10-performance-testing-ed2.pdf

ENISA – SUR LA DISTRIBUTION QUANTIQUE DE CLEFS



La distribution quantique de clefs, **QKD** ou **Quantum Key Distribution**, est un procédé qui fait appel à des concepts parfois difficiles à appréhender, et conduisant à lire tout et n'importe quoi dans la littérature.

Ce procédé permet de distribuer des clefs avec un niveau de sécurité inconditionnellement sûr en utilisant les propriétés fondamentales des particules quand celles-ci sont étudiées individuellement. Dans le cas présent, la sécurité de la transmission de la clef réside dans l'impossibilité d'observer, et donc de dupliquer, l'information reçue, information portée par une particule (un photon dans les implémentations actuelles) sans altérer celle-ci. Nos lecteurs pourront se rapporter à notre long article sur le sujet paru dans le rapport N°134 de Septembre 2009.

L'ENISA vient de publier un court dossier – 7 pages - consacré à ce sujet et intitulé '**ENISA Briefing: Quantum Key Distribution**' dont l'objectif est de faire le point sur l'utilisation de ce procédé et des technologies associées.

Après une brève introduction non technique aux propriétés ici mises à contribution, le dossier traite un point fondamental en rappelant ce que la distribution quantique de clefs n'est pas, ou n'assure pas. Ce n'est pas une technique de chiffrement. Ce n'est pas non plus un système purement quantique et autonome. Cette technologie, en l'état actuel, n'est pas adaptée aux grandes distances. Elle ne permet pas de s'affranchir d'une sécurité de bout en bout. Elle n'a rien à voir avec les calculateurs ou avec la cryptographie quantique. Et enfin elle ne peut pas être utilisée pour transmettre une information spécifique et prédéterminée. Une mise au point nécessaire au regard du nombre croissant de solutions de sécurité faisant référence à ce procédé, ou utilisant simplement la terminologie associée.

Le dossier décrit ensuite les deux approches techniques actuellement employées dans les produits du marché en précisant simplement que ces approches ne sont pas infaillibles et que diverses attaques ont été développées avec succès. Les axes de progrès et les thèmes de recherche sont esquissés en rappelant que cette technologie est sujette à controverses: sur son réel intérêt économique hors certains contextes spécifiques, sur l'intérêt de disposer d'un système dont le niveau de sécurité est supérieur de plusieurs ordres de grandeur à celui des autres composants ou encore sur le bien fondé de l'affirmation de l'inconditionnalité de la sécurité du procédé, lequel repose sur un modèle purement théorique, et donc par définition incomplet.

Le sommaire de ce dossier est le suivant:

- Key points**
- Introduction**
- What it is not**
- Implementations and weaknesses**
- Areas of controversy and open issues**
- Future trends and research**
- Sources and further reading**

POUR PLUS D'INFORMATION

<http://www.enisa.europa.eu/act/rm/files/deliverables/briefing-quantum-key-distribution>

http://www.enisa.europa.eu/act/rm/files/deliverables/briefing-quantum-key-distribution/at_download/fullReport

ENISA – SUR LES RISQUES LIES AU CLOUD COMPUTING



Le rapport sur le '**Cloud Computing**' que vient de publier l'**ENISA** deviendra, à n'en pas douter, une référence en la matière. L'agence de sécurité européenne nous propose en effet une analyse méthodique, et très complète, des problèmes de sécurité et des atteintes à la vie privée que pourrait poser l'adoption, à grande échelle, d'une nouvelle approche du traitement de l'information désignée par le terme imagé de '**Cloud Computing**'.

Visant à offrir le juste service au meilleur prix et conduisant à devoir délocaliser tout ou partie des

services, mais aussi des données, hors de l'entreprise et hors des frontières géographiques avec tous les risques que cela sous-tend, cette approche encore jeune et immature est encore à caractériser. Le **NIST** s'y est dernièrement essayé avec succès en s'appuyant sur les travaux de quatre chercheurs Européens publiés en 2008 dans la communication intitulée '**A Break in the Clouds: Towards a Cloud Definition**'. Dans son rapport, l'ENISA propose son propre modèle inspiré des travaux de ces chercheurs, de la définition du NIST et de l'article publié sur **Wikipedia**. Au risque de paraître politiquement incorrect, les modifications apportées par l'ENISA à la définition du NIST conduisent à une définition plus restrictive sans apporter de réelle valeur à l'ensemble comme le fait apparaître le tableau de comparaison que nous avons dressé:

NIST	ENISA
Caractéristiques essentielles	
On-demand self-service	Service on demand with a 'pay as you go' billing system
Broad network access	
Resource pooling	Shared resources (hardware, database, memory...)
Rapid elasticity	Near instant scalability and flexibility
	Highly abstracted resources
Measured Service	Near instantaneous provisioning
	Programmatic management
Modèles de service	
Cloud Software as a Service (SaaS)	Software as a service (SaaS)
Cloud Platform as a Service (PaaS)	Platform as a service (PaaS)
Cloud Infrastructure as a Service (IaaS)	Infrastructure as service (IaaS)
Modèles de déploiement	
Private cloud	Private
Community cloud	Partner
Public cloud	Public
Hybrid cloud	

L'analyse de risque engagée par l'ENISA considère quelques 35 risques fondamentaux classés dans quatre catégories.

Policy and organizational risks	
R.01 Lock-in	5
R.02 Loss of governance	7
R.03 Compliance challenges	7
R.04 Loss of business reputation due to co-tenant activities	4
R.05 Cloud service termination or failure	4
R.06 Cloud provider acquisition	4
R.07 Supply chain failure	3
Technical risks	
R.08 Resource exhaustion (under or over provisioning)	4
R.09 Isolation failure	6
R.10 Cloud provider malicious insider - abuse of high privilege roles	6
R.11 Management interface compromise (manipulation, availability of infrastructure)	6
R.12 Intercepting data in transit	5
R.13 Data leakage on up/download, intra-cloud	5
R.14 Insecure or ineffective deletion of data	6
R.15 Distributed denial of service (DDoS)	5
R.16 Economic denial of service (EDoS)	4
R.17 Loss of encryption keys	4
R.18 Undertaking malicious probes or scans	4
R.19 Compromise service engine	5
R.20 Conflicts between customer hardening procedures and cloud environment	3
Legal risks	
R.21 Subpoena and e-discovery	5
R.22 Risk from changes of jurisdiction	7
R.23 Data protection risks	5
R.24 Licensing risks	4
Risks not specific to the cloud	
R.25 Network breaks	5
R.26 Network management (ie, network congestion / mis-connection / non-optimal use)	6
R.27 Modifying network traffic	4
R.28 Privilege escalation	4
R.29 Social engineering attacks (ie, impersonation)	5
R.30 Loss or compromise of operational logs	3
R.31 Loss or compromise of security logs (manipulation of forensic investigation)	3

R.32 Backups lost, stolen	4
R.33 Unauthorized access to premises (including physical access to machines and other facilities)	3
R.34 Theft of computer equipment	3
R.35 Natural disasters	3

La probabilité d'occurrence, et l'impact métier, de chacun de ces risques sont quantifiés au regard de trois cas de figure représentatifs des interrogations de l'Europe vis-à-vis de cette approche (les conditions d'analyse associées à ces trois cas sont décrites en annexe II et III du rapport).

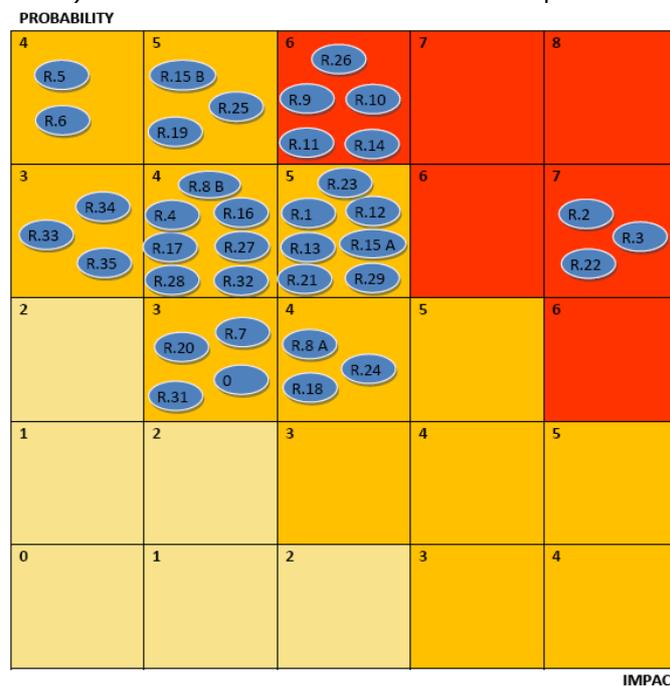
- 1- Migration d'une PME vers une infrastructure de service de 'Cloud Computing',
- 2- Impact du 'Cloud Computing' sur la résilience des services (un thème cher à l'**ENISA**),
- 3- Le 'Cloud Computing' dans le cadre du e-Gouvernement.

Chacun de ces 35 risques est ensuite caractérisé par la liste des vulnérabilités qu'il est susceptible de générer et des atteintes sur les biens qui en découlent (chapitre 3 du rapport).

Une liste de 53 vulnérabilités (identifiées V1 à V53) et 23 biens (identifiés A1 à A23) est pour cela établie (chapitres 4 et 5).

Les résultats de cette analyse permettent d'établir une classique matrice de risque Probabilité/Impact permettant de visualiser la distribution du risque et les risques prépondérants.

Une échelle à cinq niveau est ici utilisée pour la probabilité d'occurrence (Rare, Peu probable, Possible, Probable, Certaine) mais aussi pour l'impact (Très faible, Faible, Moyen, Elevé et Très élevé) conduisant à définir 9 niveaux de risque.



R.2 LOSS OF GOVERNANCE		
Probability	VERY HIGH	Comparative: Higher
Impact	VERY HIGH (depends on organization) (IaaS VERY HIGH, SaaS Low)	Comparative: Equal
Vulnerabilities	V34. Unclear roles and responsibilities V35. Poor enforcement of role definitions V21. Synchronizing responsibilities or contractual obligations external to cloud V23. SLA clauses with conflicting promises to different stakeholders V25. Audit or certification not available to customers V22. Cross-cloud applications creating hidden dependency V13. Lack of standard technologies and solutions V29. Storage of data in multiple jurisdictions and lack of transparency about THIS V14. No source escrow agreement V16. No control on vulnerability assessment process V26. Certification schemes not adapted to cloud infrastructures V30. Lack of information on jurisdictions V31. Lack of completeness and transparency in terms of use V44. Unclear asset ownership	
Affected assets	A1. Company reputation A2. Customer trust A3. Employee loyalty and experience A5. Personal sensitive data A6. Personal data A7. Personal data - critical A9. Service delivery – real time services A10. Service delivery	
Risk	HIGH	

L'ENISA nous offre ici une intéressante analyse de sécurité traitant d'un domaine en pleine expansion.

Les risques prédominants apparaissent être principalement, est-ce une surprise, liés à la délégation de l'autorité à un tiers offreur de service susceptible d'opérer sur un territoire placé hors de la juridiction Européenne (risques R22 mais aussi R2 et R3).

Viennent ensuite les risques techniques liés à la prédominance de l'utilisation de technologies de virtualisation permettant le partage d'un même système physique par plusieurs environnements n'ayant potentiellement, ni le même niveau de sécurité, ni même le même propriétaire (risques R09, R10 et R11 en impliquant l'opérateur du service).

Des risques non négligeables dans un monde unifié sur le plan des communications mais pas de celui des politiques. Les législations garantissant la sécurité des données et la protection de la vie privée sont loin d'être en accord.

La conclusion de l'étude apparaît alors être à ce titre bien neutre et trop politiquement correcte:

The key conclusion of this paper is that the cloud's economies of scale and flexibility are both a friend and a foe from a security point of view.

Le sommaire de cette étude de 123 pages est le suivant:

- Executive summary**
- Top recommendations
- Top security benefits
- Top security risks
- Contents**

Target audience
Cloud computing - working definition
Survey of existing work

1 Security benefits of cloud computing

- Security and the benefits of scale
- Security as a market differentiator
- Standardised interfaces for managed security services
- Rapid, smart scaling of resources
- Audit and evidence-gathering
- More timely and effective and efficient updates and defaults
- Audit and SLAs force better risk management
- Benefits of resource concentration

2 Risk assessment

- Use-case scenarios
- Risk assessment process

3 Risks

- Policy and organizational risks
- Technical risks
- Legal risks
- Risks not specific to the cloud

4 Vulnerabilities

- Vulnerabilities not specific to the cloud

5 Assets

6 Recommendations and key messages

Information assurance framework

- Introduction
- Division of liabilities
- Division of responsibilities
- Software as a Service
- Platform as a Service
- Infrastructure as a Service
- Methodology
- Note of caution
- Note to governments

Information assurance requirements

- Personnel security
- Supply-chain assurance
- Operational security
- Identity and access management
- Asset management
- Data and Services Portability
- Business Continuity Management
- Physical security
- Environmental controls

Legal requirements

Legal recommendations

Legal recommendations to the European Commission

Research recommendations

Glossary and abbreviations

Bibliography

ANNEX

- I – Cloud computing – Key legal issues
- II – SME use-case scenario
- III – Other use-case scenarios

POUR PLUS D'INFORMATION

- <http://www.enisa.europa.eu/media/press-releases/enisa-clears-the-fog-on-cloud-computing-security-1>
- http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

ENISA – CARTES D'IDENTITE ELECTRONIQUES ET INTERNET



L'ENISA a publié un rapport intitulé '**Privacy and Security Risks when Authenticating on the Internet with European eID Cards**' dont l'objectif est d'analyser les risques liés à l'utilisation des cartes d'identités électroniques délivrées par certains états membres comme moyen d'authentification auprès de services accessibles via l'Internet (Rapport N°132 – Juillet 2009). Deux cas de figures sont proposés à titre d'exemple: son utilisation dans le cadre d'un service de banque en ligne, un service fermé a priori digne de confiance, et son utilisation dans le contexte d'un service WEB ouvert, ici un réseau social, avec la possibilité de tirer parti de certaines fonctionnalités présentes dans

ces cartes pour effectuer les contrôles requis par la législation, sur l'âge de l'accédant par exemple.

Ce rapport propose une analyse de risque assez complète prenant en compte deux composantes agissant dans le sens d'un renforcement du niveau de sécurité:

- la **technologie d'authentification** avec 13 catégories (AT1: mot de passe à AT13: biométrie) et,
- les **fonctions de protection** des données personnelles avec 7 fonctions (PF1: contrôle d'accès à PF7: communications sécurisées de bout en bout).

et trois facteurs de modération:

- les **agresseurs** au nombre de 3 (TA1: attaquant à TA3: usager),
- les **vulnérabilités** avec 7 problèmes (V1: erreur de conception dans la carte à V7: vol de la carte) et
- les **menaces** au nombre de 15 (T1:carte à T15: délégation)

Trois conséquences sont identifiées allant du vol (RT1), à la fraude (RT3) en passant par l'atteinte à la vie privée (RT2).

Le niveau de risque associé à chacune des 15 menaces est établi classiquement comme étant le produit de la probabilité d'occurrence et de l'impact. Ces deux termes, et le niveau de risque résultant, sont exprimés sur une échelle comportant cinq niveaux pondérés de 1 à 5 pour les deux termes et de 1 à 25 pour le niveau. Les résultats de l'analyse sont ici présentés sous la forme d'un tableau ordonné par menace, et non d'une matrice Probabilité/Impact généralement bien plus lisible.

Ces résultats sont utilisés pour dresser deux tables, l'une établissant l'adéquation des 13 technologies d'authentification aux 7 menaces générant le risque le plus élevé, et l'autre, l'adéquation des 7 fonctions de protection au regard des 3 menaces impactant directement la vie privée.

Mechanism→ Threat↓	PF1 Access control	PF2 no UID	PF3 spec. UID	PF4 select	PF5 verify	PF6 pseudo	PF7/AT 10/AT1 1 SSL
T10 Data greed	X			X	X		
T11 Merge		+	X			+	
T12 Eve						X	X

Legend: X: can prevent threat +: can mitigate threat

Mechanism→ Threat↓	AT1 PIN	AT2 TAN	AT3 iTAN	AT4 mTAN	AT5 tbTAN	AT7 Imp T	AT8 Timer	AT9 Card	AT10 SSL	AT11 SSL m.a.	AT12 Call-back
T3 Passwd	X	X	X	X	X		X	X		X	X
T4 Keylog		X	X	X	X		X	X		X	X
T5 (T8) ²⁹ MITM			X	X	X	X	X	X	+	+	X
T6 (T8) Real-time					+	X		X	+	+	X
T7 (T8) Browser					+						
T9 Low-tech					+		X	X			+
T14 Coffee break		+	+	+	+		+	+			X

Legend: X: can prevent threat +: can mitigate threat
tbTAN: Transaction-based TAN
Imp T.: Impersonal token
m.a.: Mutual authentication

Le sommaire de cette étude de 41 pages est le suivant:

- 1 **Use-cases and applications**
 - 1.1 Use-case 1: Online banking
 - 1.2 Use-case 2: Social networking (and other web services)
- 2 **Technology overview**
 - 2.1 Authentication and out-of-band mechanisms
 - 2.2 Privacy features of electronic ID cards
 - 2.3 Additional remarks
- 3 **Risk assessment**
 - 3.1 Definitions
 - 3.2 Scenarios
 - 3.3 Assets
 - 3.4 Vulnerabilities
 - 3.5 Threat agents
 - 3.6 Threats
 - 3.7 Risks
- 4 **Security requirements**
 - 4.1 Online banking
 - 4.2 Social networking, online forums and virtual worlds
- 5 **Addressing the requirements**
- 6 **Recommendations and conclusions**
- 7 **References**

POUR PLUS D'INFORMATION

- <http://www.enisa.europa.eu/act/it/eid/eid-online-banking>
- http://www.enisa.europa.eu/act/it/eid/eid-online-banking/at_download/fullReport

LOGICIELS

OUTILLAGES ANTIVIRUS

Le site 'MalwareHelp' a publié un très intéressant état de l'art sur les outils d'éradication de virus autonomes, c'est-à-dire pouvant être activés sans avoir recours au système d'exploitation installé sur le poste de travail.

Pour la plupart proposées gracieusement par les principaux éditeurs de produits anti-virus, ces boîtes à outils spécialisées prennent bien souvent la forme d'un système d'exploitation majoritairement basé sur LINUX et configuré pour activer automatiquement une application d'analyse.

Il suffira alors de télécharger l'image de cet environnement mise à disposition sur le site de l'éditeur puis de la graver sur un **CD**, un **DVD**, ou encore dans certains cas de l'installer sur une clef **USB**, pour disposer d'un outillage qui sera fort pratique pour lever rapidement le doute quand à l'état d'un poste de travail.

L'intérêt d'un tel outillage: permettre d'intervenir sans avoir à s'appuyer sur le système natif qui, ayant pu être compromis, pourrait manipuler les résultats. En s'initialisant sur un environnement réputé intègre, avant même qu'aucun code tiers – hormis celui de la **BIOS** - n'ait pût être activé, les chances de détecter un code malveillant sont largement renforcées. La plupart des codes malveillants, virus, vers ou Troyens, s'étant installés sur le système pourront ainsi être détectés à condition toutefois que le produit dispose des algorithmiques et fichiers de définition ad hoc.

Le problème de la mise à jour de ces algorithmes et fichiers de signature est généralement élégamment résolu par l'activation d'une routine chargée de rapatrier par réseau les dernières versions depuis le site de l'éditeur, le système d'exploitation étant alors configuré pour obtenir automatiquement une adresse via le service **DHCP** local. L'utilisateur pourra bien souvent modifier cette configuration dans le cas d'infrastructures ne disposant pas d'une connectivité Internet ou des services requis pour la configuration automatique du poste de travail.

Ce mode de fonctionnement permet d'envisager pouvoir préparer plusieurs 'boîtes à outils' sans avoir à se préoccuper de leur mise à jour, une opération toujours délicate et particulièrement coûteuse en ressources quand il y a le feu. Il y aura cependant lieu de prévoir de documenter l'utilisation de chacun des environnements en précisant notamment les limitations techniques liées aux caractéristiques de la plateforme testée et les pré-requis en matière de connectivité.

L'état de l'art publié par **MalwareHelp** recense les 11 environnements listés dans le tableau ci-dessous, environnements pour lesquels nous avons ajouté quelques informations techniques utiles.

Outil	Accès	Taille	Ver.	MAJ	Mode	OS	MAJ
Avast! BART CD	Payant	-	-	-	Live CD	Windows	-
Avira AntiVir Rescue System	Gratuit	60Mo		NA	Live CD	Linux	Réseau
BitDefender Rescue CD	Gratuit	260Mo	2.00	03/08/09	Live CD	Knoppix	Réseau
Dr.Web LiveCD	Gratuit	76Mo	5.00	Journalière	Live CD	Linux	-
F-Secure Rescue CD	Gratuit	120Mo	3.11	22/09/09	Live CD	Knoppix	Réseau requis
G Data BootCD	Gratuit	-	-	-	Live CD	-	-
Kaspersky Rescue Disk	Gratuit	120Mo	8.8.1.36	23/06/09	Live CD	Gentoo	Réseau
Panda SafeCD	Gratuit	130Mo	3.4.3.5	27/07/09	Live CD	Linux	Manuelle
PC Tools' Alternate OS Scanner	Gratuit	60Mo	-	-	Live CD	Linux	USB
VBA32 Rescue	Gratuit	84Mo	3.12.2.0	-	Live CD	Gentoo	-
Quick Heal Live Scanner	Gratuit	66Mo	2009	-	Applic.	Windows	-

Trois des environnements identifiés dans l'article posent un problème:

- '**Avast ! BART CD**' qui s'appuie sur l'environnement autonome **Windows Bart PE** s'avère être payant,
- '**G Data BootCD**' qui utilise les moteurs **BitDefender** et **Avast** est introuvable sur le site de l'éditeur,
- '**QuickHeal Live Scanner**' est un exécutable portable qui devra être lancé depuis le système analysé.

Les environnements livrés sous la forme d'une image **ISO** ont été testés en chargeant chacune d'elles dans une instance de l'émulateur '**QEmu**' sur une machine Windows. Un système très performant est ici requis pour optimiser les temps de chargement. Nous nous sommes pour cela appuyés sur le remarquable utilitaire '**Mobalive**' qui permet d'initialiser une émulation en deux clics de souris (Rapport N°127 – Février 2009).

Habitué que nous sommes à travailler avec différents systèmes d'exploitation, notre préférence ira aux environnements proposés par **BitDefender**, et **Kaspersky** qui offrent un accès complet et direct au système LINUX sous-jacent, tous les services réseaux et système standards étant démarrés.

Nous avons aussi, a contrario, bien apprécié les outils proposés par **F-Secure** et **PCTools** qui, eux, permettent de se concentrer sur l'essentiel – l'analyse – par le biais d'une interface minimaliste, simple, en un mot: parfaitement réussie.

Bitdefender Rescue CD

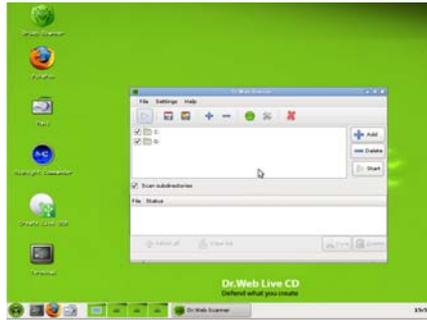
DrWeb Rescue CD



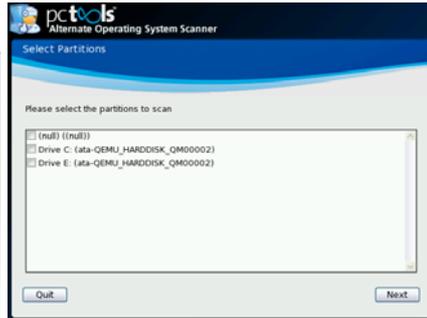
Kaspersky Rescue Disk



Avira AntiVir Rescue Scanner



PCTools' Alternate OS Scanner



VBA32 Rescue



POUR PLUS D'INFORMATION

<http://www.malwarehelp.org/anti-virus-rescue-cd-dvd-download-2009.html>

METHODOLOGIES ET STANDARDS

METHODES

ENISA - COMMENT AMELIORER LA SENSIBILISATION A LA SECURITE DE L'INFORMATION



L'ENISA a publié les versions allemande et française du très intéressant guide 'How to raise information security awareness' qui a été diffusé en langue anglaise en juillet 2008 (Rapport N°123 – Septembre 2008).

Ce guide résultait lui-même de la mise à jour d'une première version finalisée en août 2006 (Rapport N°91 – Février 2006). La mise à disposition d'une version française, quand bien même celle-ci serait tardive, devrait permettre l'accès au plus grand nombre d'un guide dont nous avons particulièrement apprécié l'accessibilité et l'aspect didactique. Avec ce guide qui conserve le fond et la forme du guide original, l'ENISA nous propose une approche 'clef en main' intégrant non seulement une méthodologie validée par l'expérience mais aussi tous les éléments requis pour une mise en œuvre quasi-immédiate.

Le sommaire de ce guide de 110 pages est le suivant:

L'importance des programmes de sensibilisation a la sécurité de l'information

Introduction

La sensibilisation, qu'est-ce que c'est?

Quand des programmes de sécurité de l'information sont-ils nécessaires?

Principaux processus d'exécution des programmes de sensibilisation à la sécurité de l'information

Stratégie globale d'exécution des programmes de sensibilisation à la sécurité de l'information

Hiérarchie de la mise en correspondance des processus

Principaux processus d'exécution des programmes de sensibilisation à la sécurité de l'information

Phase 1 – Planifier, évaluer et concevoir

A Constituer l'équipe de programme initiale

C Définir les buts et les objectifs

E Déterminer le personnel et le matériel

G Choisir une solution et une procédure

I Préparer le plan de travail

K Définir un concept de communication

M Définir un référentiel d'évaluation

B Adopter une approche de gestion du changement

D Définir les groupes cibles

F Évaluer les solutions potentielles

H Obtenir le soutien et le financement de la direction

J Établir le programme et les listes de contrôle des tâches

L Définir les indicateurs pour mesurer le succès du programme

N Documenter les enseignements

Phase 2 – Exécuter et gérer

A Confirmer l'équipe de programme

C Lancer et mettre en œuvre le programme

E Documenter les enseignements

B Réviser le plan de travail

D Exécuter le plan de communications

Phase 3 – Evaluer et ajuster

A Conduire les évaluations

C Intégrer le feedback de communication

E Mettre en œuvre les enseignements

G Relancer le programme

B Récolter des données

D Réviser les objectifs du programme

F Ajuster le programme de manière appropriée

Surmonter les obstacles à la réussite

Obstacles à la réussite

Facteurs de succès critiques

Conclusion

POUR PLUS D'INFORMATION

http://www.enisa.europa.eu/act/ar/deliverables/2008/new-users-guide-fr/at_download/fullReport

http://enisa.europa.eu/doc/pdf/deliverables/new_ar_users_guide.pdf

<http://www.iwar.org.uk/comsec/resources/ENISA/infosec-awareness.pdf>

- Version UK 2008

- Version UK 2006

OWASP – LA PROCHAINE TOP TEN LIST



L'édition américaine de la conférence de l'OWASP a été l'occasion de la diffusion d'une version préliminaire de la nouvelle 'Top Ten List', la liste des dix risques les plus critiques dans les applications WEB.

Publiée depuis 2007 et régulièrement mise à jour, cette liste fait 'peau neuve' à l'occasion de cette édition 2010. Elle devrait être officiellement publiée dans le courant du premier semestre 2010. Une période d'un mois, se terminant fin décembre, est en effet mise à profit pour collecter, et prendre en compte, les derniers commentaires et suggestions.

Les évolutions sont de trois ordres:

- Méthodologique par un classement prenant en compte l'estimation du risque et non plus la fréquence de la vulnérabilité associée,
- Pratique avec le rappel à tous les niveaux que **cette liste traite des risques** et non des vulnérabilités,
- Cosmétique avec une complète refonte de la mise en page.

Ceci conduit à une importante réorganisation de la liste tant sur le plan de l'ordonnancement des risques que sur celui des catégories représentées.

Ainsi, deux catégories disparaissent de la liste - **Malicious File Execution** et **Information Leakage and Improper Error Handling** - qui sont remplacées par une nouvelle catégorie - **Unvalidated Redirects and Forwards** - et une catégorie déjà représentée - **Security Misconfiguration** - mais sous une autre définition (Insecure Configuration Management).

OWASP Top 10 – 2007 (Previous)	OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	A1 – Injection
A1 – Cross Site Scripting (XSS)	A2 – Cross Site Scripting (XSS)
A7 – Broken Authentication and Session Management	A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	A5 – Cross Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	A6 – Security Misconfiguration (NEW)
A10 – Failure to Restrict URL Access	A7 – Failure to Restrict URL Access
<not in T10 2007>	A8 – Unvalidated Redirects and Forwards (NEW)
A8 – Insecure Cryptographic Storage	A9 – Insecure Cryptographic Storage
A9 – Insecure Communications	A10 – Insufficient Transport Layer Protection
A3 – Malicious File Execution	<dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	<dropped from T10 2010>

Le document d'accompagnement publié par l'OWASP nous libère – enfin – d'une tâche fastidieuse que nous devons jusqu'alors mener à chaque nouvelle édition, celui de l'établissement de l'évolution de la liste. Nous nous sommes simplement permis de souligner les changements de place sur le tableau extrait du document.

La mise en forme de ce document est particulièrement soignée. Chaque risque fait l'objet d'une fiche illustrée, et non plus d'une simple description textuelle comme cela était le cas avec la version précédente.

Se focalisant désormais sur la mesure du risque, celui est estimé en le déclinant sur chaque élément participant à la mesure de l'impact - technique et métier, d'une agression.

Threat Agent	Attack Vector	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact
?	Easy	Widespread	Easy	Severe	?
	Average	Common	Average	Moderate	
	Difficult	Uncommon	Difficult	Minor	

Une échelle colorimétrique à trois niveaux de gradation permet de mieux visualiser les éléments maîtrisés sur lesquels il faudra intervenir.

Les éléments pris en compte sont au nombre de six: l'agresseur, le vecteur de l'attaque, la prévalence de la vulnérabilité exploitée et la facilité avec laquelle celle-ci sera détectée, l'impact technique et enfin l'impact métier.

A n'en pas douter ce remarquable effort de pédagogie, et de communication, devrait porter ses fruits.

POUR PLUS D'INFORMATION

http://www.owasp.org/images/0/0f/OWASP_T10_-_2010_rc1.pdf

A1 Injection

Threat Agents

Attack Vectors

Security Weakness

Technical Impacts

Business Impacts

	Exploitability EASY	Prevalence COMMON	Detectability AVERAGE	Impact SEVERE
<p>Consider anyone who can send untrusted data to the system, including external users, internal users, and administrators.</p>	<p>Attacker sends simple text-based attacks that exploit the syntax of the targeted interpreter. Almost any source of data can be an injection vector, including internal sources.</p>	<p>Injection flaws occur when an application sends untrusted data to an interpreter. Injection flaws are very prevalent, often found in SQL queries, LDAP queries, XPath queries, OS commands, program arguments, etc. Injection flaws are easy to discover when examining code, but more difficult via testing. Scanners and fuzzers can help attackers find them.</p>	<p>Injection can result in data loss or corruption, lack of accountability, or denial of access. Injection can sometimes lead to complete host takeover.</p>	<p>Consider the business value of the affected data and the platform running the interpreter.</p>

Am I Vulnerable To Injection?

The best way to find out if an application is vulnerable to injection is to verify that all use of interpreters clearly separates untrusted data from the command or query. For SQL calls, this means using bind variables in all prepared statements and stored procedures, and avoiding dynamic queries.

Checking the code is a fast and accurate way to see if the application uses interpreters safely. Code analysis tools can help a security analyst find the use of interpreters and trace the data flow through the application. Manual penetration testers can confirm these issues by crafting exploits that confirm the vulnerability.

Automated dynamic scanning which exercises the application may provide insight into whether some exploitable injection problems exist. Scanners cannot always reach interpreters and can have difficulty detecting whether an attack was successful.

How Do I Prevent Injection?

Preventing injection requires keeping untrusted data separate from commands and queries.

- The preferred option is to use a safe API which avoids the use of the interpreter entirely or provides a parameterized interface. Beware of APIs, such as stored procedures, that appear parameterized, but may still allow injection under the hood.
- If a parameterized API is not available, you should carefully escape special characters using the specific escape syntax for that interpreter. OWASP's ESAPI has some of these [escaping routines](#).
- Positive or "whitelist" input validation with appropriate canonicalization also helps protect against injection, but is not a complete defense as many applications require special characters in their input. OWASP's ESAPI has an extensible library of [white list input validation routines](#).

Example Attack Scenario

The application uses untrusted data in the construction of the following vulnerable SQL call:

```
String query = "SELECT * FROM accounts WHERE custID=" + request.getParameter("id") + "";
```

The attacker modifies the "id" parameter in their browser to send: ' or '1='1. This changes the meaning of the query to return all the records from the accounts database, instead of only the intended customer's.

<http://example.com/app/accountView?id=' or '1='1>

In the worst case, the attacker uses this weakness to invoke special stored procedures in the database, allowing a complete takeover of the database host.

References

OWASP

- OWASP SQL Injection Prevention Cheat Sheet
- OWASP Injection Flaws Article
- ESAPI Encoder API
- ESAPI Input Validation API
- ASVS: Output Encoding/Escaping Requirements (V6)
- OWASP Testing Guide: Chapter on SQL Injection Testing
- OWASP Code Review Guide: Chapter on SQL Injection
- OWASP Code Review Guide: Command Injection

External

- CWE Entry 77 on Command Injection
- CWE Entry 89 on SQL Injection

Veille Technologique Sécurité N°136

© DEVOTEAM - Tous droits réservés

Page 17/34

Diffusion restreinte aux clients abonnés au service de veille technologique

RECOMMANDATIONS

NIST - SP800-126 'THE TECHNICAL SPECIFICATION FOR THE SECURITY CONTENT AUTOMATION PROTOCOL'



Le guide **SP800-126** 'The Technical Specification for the Security Content Automation Protocol (**SCAP**)' vient d'être publié.

Le projet **SCAP** a pour objectif de standardiser l'échange des informations entre produits de sécurité qu'il s'agisse d'éléments de configuration, ou d'informations, concernant une vulnérabilité. L'adoption des spécifications associées permettra d'automatiser un grand nombre de tâches fastidieuses, et pourtant nécessaires pour garantir la sécurité d'un système d'information: mesure de la vulnérabilité d'un système face à des menaces connues, ou encore validation de la conformité de la configuration de ce système.

Une démarche ambitieuse nécessitant l'adhésion de tous pour aboutir, des fournisseurs de produits aux utilisateurs finaux. En mai dernier étaient ainsi publiés deux documents fondamentaux: le guide **SP800-17** 'Guide to Adopting and Using the Security Content Automation Protocol' destiné à sensibiliser tous les acteurs concernés par la sécurité des systèmes d'information en général, et des organisations gouvernementales américaines en particulier, et le document **IR-7511** 'SCAP Validation Program Test Requirement' détaillant les exigences applicables aux produits et outils d'analyse de sécurité pour être déclarés conformes (Rapport N°130 – Mai 2009).

Avec ce nouveau guide, le **NIST** entre dans le détail de l'organisation de la première version de SCAP, en précisant le rôle de chacun de ses constituants lesquels sont regroupés en trois catégories: les **langages**, les **énumérations**, et les **systèmes de notation et de mesure de vulnérabilité**. **SCAP V1.0** est ainsi constitué des éléments suivants:

Enumérations	Langages	Notation et de mesure
Common Platform Enumeration CPE 2.2	Extensible Configuration Checklist Description Format XCCDF 1.1.4	Common Vulnerability Scoring System CVSS 2.0
Common Configuration Enumeration CCE 5.0	Open Vulnerability and Assessment Language OVAL 5.3 et 5.4	
Common Vulnerabilities and Exposures CVE		

Chaque énumération fournit une nomenclature standardisée, et un dictionnaire d'éléments définis à l'aide de cette nomenclature. L'énumération dite '**CVE**' propose ainsi un dictionnaire de toutes les vulnérabilités et failles de sécurité actuellement connues. Les langages offrent un moyen d'identifier sans ambiguïté ce qui doit être évalué, et de définir la manière de vérifier l'état du système cible. Enfin, les systèmes de notation et de mesure permettront d'évaluer l'impact de vulnérabilités spécifiques sur le système cible.

Le sommaire de ce guide de 63 pages est le suivant:

1. **Introduction**
2. **Overview of SCAP 1.0**
3. **Basics of SCAP Components**
 - 3.1 **Languages**
 - 3.1.1 Extensible Configuration Checklist Description Format (XCCDF)
 - 3.1.2 Open Vulnerability and Assessment Language (OVAL) 5.3 and 5.4
 - 3.2 **Enumerations**
 - 3.2.1 Common Platform Enumeration (CPE)
 - 3.2.2 Common Configuration Enumeration (CCE)
 - 3.2.3 Common Vulnerabilities and Exposures (CVE)
 - 3.3 **Common Vulnerability Scoring System (CVSS)**
4. **SCAP General Requirements and Conventions**
 - 4.1 **XCCDF Conventions and Requirements**
 - 4.1.1 Metadata
 - 4.1.2 XCCDF and CPE Dependencies
 - 4.1.3 <Rule> Element
 - 4.1.4 Embedded CCE References
 - 4.1.5 Embedded CVE References
 - 4.1.6 Allowed Check System Usage
 - 4.1.7 Use of the OVAL as a Check System
 - 4.1.8 <xccdf:Value> and OVAL Variable Dependencies
 - 4.1.9 XCCDF Test Results
 - 4.1.10 Assigning CVE Identifiers to Rule Results
 - 4.1.11 Assigning CCE Identifiers to Rule Results
 - 4.1.12 Mapping OVAL Results to XCCDF Results
 - 4.2 **OVAL Conventions and Requirements**

- 4.2.1 OVAL Schema Specification
- 4.2.2 OVAL Definitions and Affected Platforms
- 4.2.3 OVAL Definitions and Compliance Validation
- 4.2.4 OVAL Definitions and Vulnerability Assessment
- 4.2.5 OVAL Definitions and Patch Assessment
- 4.2.6 OVAL Inventories
- 4.2.7 OVAL Results
- 4.3 **CPE Conventions**
- 4.4 **CCE Conventions**
- 4.5 **CVE Conventions**
- 4.6 **CVSS Conventions**
- 5. **SCAP Use Case Requirements**
 - 5.1 **SCAP Configuration Verification with XCCDF and OVAL**
 - 5.2 **SCAP Vulnerability Assessment**
 - 5.2.1 SCAP Vulnerability Assessment Using XCCDF and OVAL
 - 5.2.2 SCAP Vulnerability Assessment Using Standalone OVAL
 - 5.3 **Inventory Collection**
- Appendix A— **Acronyms and Abbreviations**
- Appendix B— **References and other Resources**
- Appendix C— **SCAP Extensions to the XCCDF Specification**
- Appendix D— **SCAP Compliance Verification Data Stream Example**

Un guide qui permettra de mieux appréhender le rôle de chacun des constituants développés par le **MITRE**, et désormais bien connus de tous les acteurs du domaine, au sein du projet **SCAP**.

L'annexe D '**SCAP Compliance Verification Data Stream Example**' propose un exemple pratique d'application à la vérification de la configuration d'un système **Windows XP**: définition de la liste des points de contrôle dans la syntaxe **XCCDF** (D.1), description de la méthode de vérification de chacun de ces points dans la syntaxe **OVAL** (D.2 et D.3) et enfin, définition **CPE** de la constitution de la plateforme Windows XP cible des contrôles (D.4 et D.5).

POUR PLUS D'INFORMATION

<http://csrc.nist.gov/publications/nistpubs/800-126/sp800-126.pdf>

NIST – IR7657 / PRIVILEGE MANAGEMENT

NIST Le **NIST** a publié, pour relecture et commentaires, le rapport d'analyse **IR7657 'Privilege Management'** qui traite, comme son titre l'indique, de la gestion de l'accès aux ressources offertes par le système d'information. Dans la terminologie technique en usage dans notre domaine d'intervention, le terme '**privilege**' – ici traduit par 'privège' – est couramment employé pour désigner le droit d'engager une action spécifique sur le système, un mécanisme d'autorisation qu'il conviendrait de distinguer de celui plus classique déterminant le droit d'accès aux ressources hébergées par le système.

Dans le cadre du document du **NIST**, le terme 'privège' est utilisé dans un cadre bien plus large, celui de l'autorisation d'accès aux ressources du système d'information qu'il s'agisse des accès physiques aux bâtiments ou logiques aux données mais aussi aux procédures.

Privilege management creates, manages, and stores the attributes and policies needed to establish criteria that can be used to decide whether an authenticated entity's request for access to some resource should be granted.

Un positionnement parfaitement défini par les deux figures présentées ci-dessous et extraites du rapport.

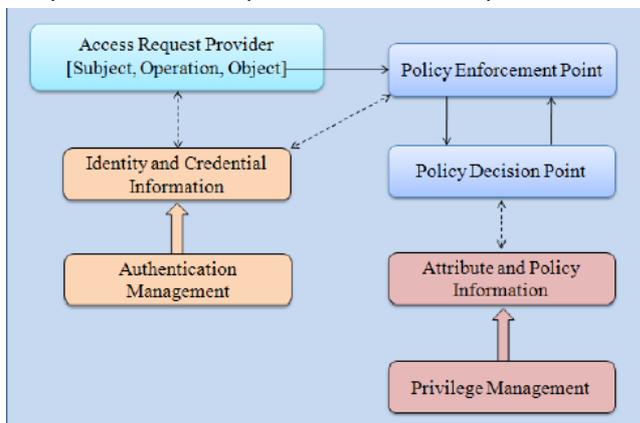


Figure 3. Authentication Management and Privilege Management

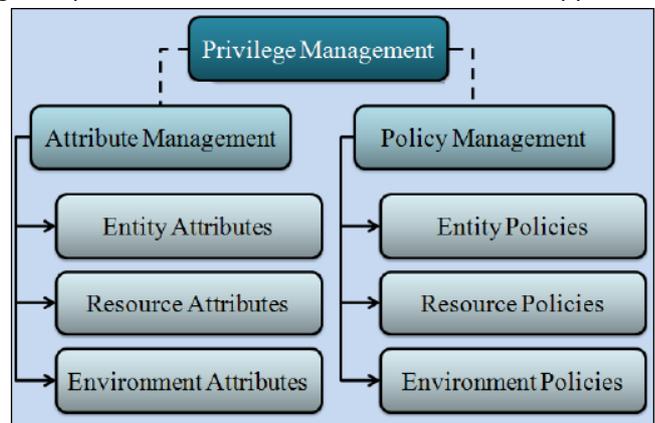
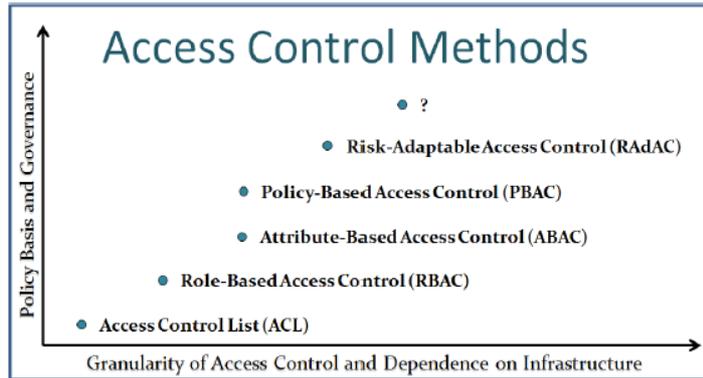


Figure 4. Information Managed by Privilege Management

Un modèle simple et pratique des relations et des interactions entre les différentes fonctions de gestion est par ailleurs proposé.

L'annexe B 'A Survey of Access Control Methods', accessible sous la forme d'un document attaché au document principal, est particulièrement intéressante.

Publiée conjointement par le **NIST** et **NSA**, elle détaille les caractéristiques des modèles de contrôle d'accès en usage dans les systèmes d'information actuels - **Access Control List (ACL)**, **Role-Based Access Control (RBAC)**, **Attribute-Based Access Control (ABAC)**, **Policy-Based Access Control (PBAC)** et **Risk-Adaptable Access Control (RAAdC)** – en comparant ceux-ci.



L'annexe D 'Advanced Capabilities for Privilege Management' liste les 17 propriétés fondamentales que devrait offrir un système de gestion des autorisations 'idéal'. Une liste qui pourrait s'avérer fort utile pour aider à la sélection d'un tel système.

Le sommaire de cet intéressant rapport de 32 pages est le suivant:

- Introduction**
- A Context for Thinking about Privilege Management**
- Definitions and Standards**
- Access Control Methods**
 - Basic Methods
 - Enhancements
 - State of the Practice
 - Considerations for Implementing Access Control
- Policies and Requirements**
- Research Agenda**
- Conclusion**
- Bibliography**
- Annexes**
 - Annex A: **Authorization and Attributes Glossary**
 - Annex B: **A Survey of Access Control Methods**
 - Annex C: **Authoritative Attribute Source and Attribute Service Guidelines**
 - Annex D: **Advanced Capabilities for Privilege Management**

POUR PLUS D'INFORMATION

http://csrc.nist.gov/publications/drafts/nistir-7657/draft-nistir-7657_privilege-management.pdf

STANDARDS

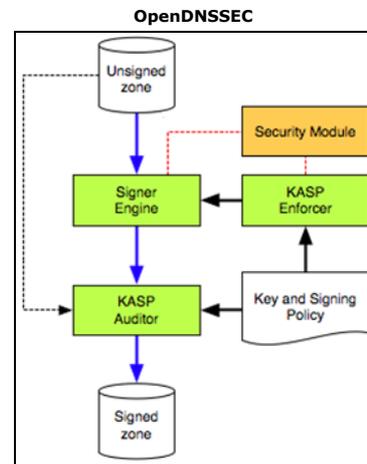
RFC5702 / USE OF SHA-2 ALGORITHMS WITH RSA IN DNSKEY AND RRSIG RESOURCE RECORDS FOR DNSSEC

Financé par la fondation hollandaise **NLNet**, le très actif laboratoire de recherche indépendant **NLnet Labs** dispose d'une expertise reconnue autour des deux technologies clés de l'Internet de demain: le protocole réseau **IP V6** et le service de gestion des noms sécurisé dit '**DNSSEC**'.

Ce laboratoire gère une dizaine de projets Open Source innovants parmi lesquels le projet **Unbound**, un service de résolution de nom récursif compatible DNSSEC résultant d'une collaboration avec **Nominet**, **Kirie** et **Verisign**, et le projet **NSD** (Name Server Daemon), un serveur de nom autoritaire performant et simple de conception.

Certains chercheurs de ce laboratoire, très impliqué dans le déploiement des extensions de sécurité du **DNS**, participent activement au remarquable projet **OpenDNSSEC**, un environnement permettant de gérer toutes les tâches requises avant la publication d'une zone sécurisée, de la génération des clés à la signature des enregistrements en passant par toutes les opérations de gestion associées. Un projet phare actuellement utilisé en grandeur réelle par '.SE', le gestionnaire du domaine suédois, l'un des premiers à avoir déployé DNSSEC.

Publié en mai 2001, le **RFC3110** spécifie les algorithmes cryptographiques qui devront être utilisés pour signer les enregistrements **DNS**, à savoir la suite de signature dite '**RSA/SHA-1**'.



Depuis 2001, plusieurs points de faiblesses ont été mis en évidence dans l'algorithme de signature **SHA-1** conduisant les experts à recommander l'abandon progressif de cet algorithme au profit de l'algorithme **SHA-2**. Concernant **DNSSEC**, cette transition ne pouvait avoir lieu avant que la spécification d'utilisation ne soit publiée. C'est désormais chose faite avec la publication par **Jelte Jansen**, un ancien du **NLnet Labs** qui officie désormais chez **ISC** l'éditeur du serveur de nom historique '**bind**', du **RFC5702**. Celui autorise l'utilisation de la suite de signature '**RSA/SHA-2**' et recommande d'activer celle-ci dès que les implémentations **DNSSEC** auront été rendus conformes à cette nouvelle spécification. La mise à jour de l'environnement **OpenDNSSEC** ne devrait pas tarder.

Users of DNSSEC are encouraged to deploy SHA-2 as soon as software implementations allow for it. SHA-2 is widely believed to be more resilient to attack than SHA-1, and confidence in SHA-1's strength is being eroded by recently announced attacks. Regardless of whether or not the attacks on SHA-1 will affect DNSSEC, it is believed (at the time of this writing) that SHA-2 is the better choice for use in DNSSEC records.

SHA-2 is considered sufficiently strong for the immediate future, but predictions about future development in cryptography and cryptanalysis are beyond the scope of this document.

Le sommaire de cette spécification de 10 pages est le suivant:

- 1 **Introduction**
- 2 **DNSKEY Resource Records**
 - 2.1. [RSA/SHA-256 DNSKEY Resource Records](#)
 - 2.2. [RSA/SHA-512 DNSKEY Resource Records](#)
- 3 **RRSIG Resource Records**
 - 3.1. [RSA/SHA-256 RRSIG Resource Records](#)
 - 3.2. [RSA/SHA-512 RRSIG Resource Records](#)
- 4 **Deployment Considerations**
 - 4.1. [Key Sizes](#)
 - 4.2. [Signature Sizes](#)
- 5 **Implementation Considerations**
 - 5.1. [Support for SHA-2 Signatures](#)
 - 5.2. [Support for NSEC3 Denial of Existence](#)
- 6 **Examples**
 - 6.1. [RSA/SHA-256 Key and Signature](#)
 - 6.2. [RSA/SHA-512 Key and Signature](#)
- 7 **IANA Considerations**
- 8 **Security Considerations**
 - 8.1. [SHA-1 versus SHA-2 Considerations for RRSIG Resource Records](#)
 - 8.2. [Signature Type Downgrade Attacks](#)
- 9 **Acknowledgments**
- 10 **References**

POUR PLUS D'INFORMATION

<ftp://ftp.ietf.org/rfc/rfc5702.txt>

TABLEAUX DE SYNTHÈSE

CONFERENCES

OARC 2009

DNS-OARC La conférence **OARC 2009**, organisée par le **DNS-OARC** (Domain Name System Operation, Analysis, and Research Center, s'est déroulée du 5 au 6 novembre à Beijing. Les supports de présentation sont accessibles en ligne.

Nous recommandons particulièrement la lecture de la communication intitulée '**Lessons Learned from May 19 China's DNS collapse**' effectuée par **Zigian Liu** de **China Telecom**. Revenant sur un dysfonctionnement majeur de l'infrastructure Internet rencontrée en Chine en mai dernier, cette présentation met en évidence non seulement la criticité du système de gestion de noms pour le bon fonctionnement de l'Internet mais aussi, et surtout, l'impact d'un dysfonctionnement pourtant a priori très localisé. Une attaque en déni de service ciblant un serveur de jeux d'un service très populaire, **baofeng.com**, a aussi mis hors service les serveurs **DNS** récursifs de ce domaine. Les serveurs **DNS** de l'opérateur China Telecom ont alors été très rapidement saturés par les milliers de demandes de résolution en attente d'une réponse des serveurs du domaine '**baofeng.com**'. Un problème qui passerait inaperçu en temps normal pour un service quelconque mais qui a conduit ici à l'engorgement de l'infrastructure de résolution s'agissant d'un service très demandé.

La présentation '**IPv6 and Recursive Resolvers**' propose un aménagement des serveurs de résolution de noms permettant de réduire l'impact d'un problème de résolution lié à la coexistence des versions 4 et 6 du protocole IP. Jason Fesler, de Yahoo!, suggère la mise en place d'un mécanisme permettant d'éviter qu'un client ne disposant pas d'une connectivité IP V6 se voit remettre une réponse contenant une telle adresse à la suite d'une requête erronée: transmission d'une requête 'AAAA' (demande d'adresse IPV6) en lieu et place d'une requête 'A' (demande d'une adresse IPV4). Une prochaine version de BIND devrait inclure l'option de configuration '**disable-aaaa-on-v4-transport**'.

BIND10 User Interface	Han Feng
DITL 2008-2009, some initial results from APNIC	George Michaelson
DNS-OARC Governance Update	Keith Mitchell
IDN TLD Variants Implementation Guideline	Jiankang Yao
IPv6 and Recursive Resolvers	Jason Fesler
Lessons Learned from May 19 China's DNS collapse	Zigian Liu
Major DNS abnormalities seen by .CN	Xin WANG
Measurement and Instrumentation at K-root	Wolfgang Nagele
New DNSSEC inline signer. DNSSEC without disrupting your workflow	Joao Damas
OpenDNSSEC	Stephen Morris
Packet Traces from a Simulated Signed Root	Duane Wessels
Results from DITL 2009 data analysis	Sebastian Castro
Security, for DNS and by DNS	Yonglin ZHOU
Signing with BIND 9.7	Peter Loshier
System Z: Cloud Computing and DNS	Simon Lau

POUR PLUS D'INFORMATION

<https://www.dns-oarc.net/oarc/workshop-200911/agenda>

OWASP AppSec 2009 – BRÉSIL



L'édition brésilienne de la conférence **AppSec** gérée par l'OWASP (Open Web Application Security Project) a eu lieu les 29 et 30 octobre derniers. Les supports de présentation sont disponibles.

Agile and Secure - Can we do both?	Jason Li, Jerry Hoff
Automated SQL Ownage Techniques	Sebastian Cufre
Exploiting Online Games	Gary McGraw
Making a Case for Data Security to Network-Centric Peers	Brian Contos
ModSecurity: Firewall OpenSource para Aplicações Web	Klaubert da Silveira
OWASP ROI: Optimize Security Spending using OWASP	Matt Tesauro

Preventive Approach for Web Application Security Testing	Luiz Otávio Duarte
Secure Programming with Static Analysis	Philippe Sevestre
Software Assurance Maturity Model (SAMM)	Pravir Chandra
The Building Security In Maturity Model	Gary McGraw
Tools and Practices for Secure Software Development	Cassio Goldschmidt
What is OWASP?	Dinis Cruz

POUR PLUS D'INFORMATION

http://www.owasp.org/index.php/AppSec_Brasil_2009_%28pt-br%29#tab=Arquivos_das_Apresenta.C3.A7.C3.B5es

HACK.LU - 2009



La conférence **Hack.Lu** consacrée à tout ce qui touche à la sécurité des systèmes d'information s'est tenue du 28 au 30 octobre. La majorité des supports des présentations est accessible en ligne.

Analyzing Word and Excel Encryption	Eric Filiol
DAVIX Visualization workshop	Jan.P.Monsch
Exploiting Delphi/Object Pascal	Ilja van Sprundel
Forensic and anti forensic enhancement with a HVM virtual monitor	Adrien Derock
Fun with Firefox extensions	Candid Wüest
Fuzzgrind: An automatic fuzzing tool	Gabriel Campana
HostileWRT: Fully-Automated Wireless Security Audit Platform on Embedded Hardware	P.Langlois, E.Parkinson
Implementation of K-ary Viruses in Python	Anthony Desnos
IpMorph: Unification of OS fingerprinting defeating	F.Vichot, G.Prigent
Malicious PDF origamis strike back	G.Delugre, F.Raynal
New advances in Office Malware analysis	Frank Boldewin
Ownage 2.0	Saumil Shah
PDF- Penetration Document Format	Didier Stevens
Peeking into Pandora's Bochs - instrumenting a full system emulator	Lutz Boehne
Perseus: A Coding Theory-based Firefox Plug-in to Counter Botnet Activity	E.Filiol, E.Deligne
Playing in a satellite environment 1.2	Christian Martorella
Sniff Keystrokes With Lasers/Voltmeters - Side Channel Attacks	D.Bianco, A.Barisani
Some Tricks For Defeating SSL In Practice	Moxie Marlinspike
When E.T. comes into Windows Mobile 6...	Cedric Halbronn

POUR PLUS D'INFORMATION

<http://2009.hack.lu/index.php/Agenda>

GUIDES

NIST – ETAT DES GUIDES DE LA SERIE SPECIALE 800



Le **NIST** a publié la version définitive du guide **SP800-126 'The Technical Specification for the Security Content Automation Protocol'**.

SP800-126	The Technical Specification for SCAP	[F]	11/09
SP800-124	Guidelines on Cell Phone and PDA Security	[F]	11/08
SP800-123	Guide to General Server Security	[F]	07/08
SP800-122	Guide to Protecting the Confidentiality of Personally Identifiable Information	[R]	01/09
SP800-121	Guide to Bluetooth Security	[F]	09/08
SP800-120	EAP Methods used in Wireless Network Access Authentication	[F]	09/09
SP800-118	Guide to Enterprise Password Management	[R]	04/09
SP800-117	Guide to Adopting and Using the Security Content Automation Protocol	[R]	05/09
SP800-116	Recommendation for the Use of PIV Credentials in Physical Access Control Systems	[F]	11/08
SP800-115	Technical Guide to Information Security Testing	[F]	09/08
SP800-114	User's Guide to Securing External Devices for Telework and Remote Access	[F]	11/07
SP800-113	Guide to SSL VPNs	[F]	07/08
SP800-111	Guide to Storage Encryption Technologies for End User Devices	[R]	11/07
SP800-110	Information System Security Reference Data Model	[R]	09/07
SP800-108	Recommendation for Key Derivation Using Pseudorandom Functions	[F]	11/08
SP800-107	Recommendation for Using Approved Hash Algorithms	[F]	02/09
SP800-106	Randomized Hashing Digital Signatures	[F]	02/09
SP800-104	A Scheme for PIV Visual Card Topography	[F]	06/07
SP800-103	An Ontology of Identity Credentials, Part I: Background and Formulation	[R]	09/06

SP800-102	Recommendation for Digital Signature Timeliness	[F]	09/09
SP800-101	Guidelines on Cell Phone Forensics	[F]	05/07
SP800-100	Information Security Handbook: A Guide for Managers	[F]	03/07
SP800-98	Guidance for Securing Radio Frequency Identification (RFID) Systems	[F]	04/07
SP800-97	Guide to IEEE 802.11i: Robust Security Networks	[F]	02/07
SP800-96	PIV Card / Reader Interoperability Guidelines	[R]	09/06
SP800-95	Guide to Secure Web Services	[F]	08/07
SP800-94	Guide to Intrusion Detection and Prevention (IDP) Systems	[F]	02/07
SP800-92	Guide to Computer Security Log Management	[F]	09/06
SP800-90	Random Number Generation Using Deterministic Random Bit Generators	[F]	03/07
SP800-89	Recommendation for Obtaining Assurances for Digital Signature Applications	[F]	11/06
SP800-88	Guidelines for Media Sanitization	[F]	09/06
SP800-87r1	Codes for the Identification of Federal and Federally-Assisted Organizations	[F]	04/08
SP800-86	Computer, Network Data Analysis: Forensic Techniques to Incident Response	[F]	08/06
SP800-85A1	PIV Card Application and Middleware Interface Test Guidelines	[F]	03/09
SP800-85B1	PIV Middleware and PIV Card Application Conformance Test Guidelines	[R]	09/09
SP800-85B	PIV Middleware and PIV Card Application Conformance Test Guidelines	[F]	07/06
SP800-84	Guide to Single-Organization IT Exercises	[F]	09/06
SP800-83	Guide to Malware Incident Prevention and Handling	[F]	11/05
SP800-82	Guide to Industrial Control Systems (ICS) Security	[R]	09/08
SP800-81r1	Secure Domain Name System (DNS) Deployment Guide	[R]	08/09
SP800-81	Secure Domain Name System (DNS) Deployment Guide	[F]	05/06
SP800-80	Guide for Developing Performance Metrics for Information Security	[R]	05/06
SP800-79r1	Guidelines for Certification & Accreditation of PIV Card Issuing Organizations	[F]	06/08
SP800-78-2	Cryptographic Algorithms and Key Sizes for Personal Identity Verification	[R]	10/09
SP800-78r1	Cryptographic Algorithms and Key Sizes for Personal Identity Verification	[F]	08/07
SP800-77	Guide to Ispsec VPNs	[F]	12/05
SP800-76r1	Biometric Data Specification for Personal Identity Verification	[F]	01/07
SP800-73r3	Interfaces to Personal Identity Verification	[R]	08/09
SP800-73r2	Interfaces to Personal Identity Verification	[F]	09/08
SP800-72	Guidelines on PDA Forensics	[F]	11/04
SP800-70r1	NCP for IT Products - Guidelines for Checklist Users and Developers	[F]	09/09
SP800-70	The NIST Security Configuration Checklists Program	[F]	05/05
SP800-69	Guidance for Securing Microsoft Windows XP Home Edition	[F]	08/06
SP800-68r1	Guidance for Securing Microsoft Windows XP Systems for IT Professionals	[F]	07/08
SP800-67	Recommendation for the Triple Data Encryption Algorithm Block Cipher	[F]	06/08
SP800-66r1	An Introductory Resource Guide for Implementing the HIPAA Security Rule	[F]	10/08
SP800-65r1	Integrating IT Security into the Capital Planning and Investment Control Process	[R]	07/09
SP800-65	Integrating IT Security into the Capital Planning and Investment Control Process	[F]	01/05
SP800-64r2	Security Considerations in the Information System Development Life Cycle	[F]	10/08
SP800-63r1	Electronic Authentication Guidelines	[R]	12/08
SP800-61r1	Computer Security Incident Handling Guide	[F]	03/08
SP800-60r1	Guide for Mapping Types of Information & IS to Security Categories	[F]	08/08
SP800-59	Guideline for Identifying an Information System as a National Security System	[F]	08/03
SP800-58	Security Considerations for Voice Over IP Systems	[F]	03/05
SP800-57p1	Recommendation for Key Management, 1: General Guideline	[F]	03/07
SP800-57p2	Recommendation for Key Management, 2: Best Practices	[F]	08/05
SP800-57p3	Recommendation for Key Management, 3: Application-Specific Key Management	[D]	10/08
SP800-56A	Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography	[F]	03/07
SP800-56B	Pair-Wise Key Establishment Using Integer Factorization Cryptography	[F]	09/09
SP800-55r1	Security Metrics Guide for Information Technology Systems	[F]	08/08
SP800-54	Border Gateway Protocol Security	[F]	07/07
SP800-53r3	Recommended Security Controls for Federal Information Systems	[F]	08/09
SP800-53r2	Recommended Security Controls for Federal Information Systems	[F]	12/07
SP800-53A	Guide for Assessing the Security Controls in Federal Information Systems	[F]	06/08
SP800-52	Guidelines on the Selection and Use of Transport Layer Security	[F]	06/05
SP800-51	Use of the Common Vulnerabilities and Exposures Vulnerability Naming Scheme	[F]	09/02
SP800-50	Building an Information Technology Security Awareness & Training Program	[F]	03/03
SP800-49	Federal S/MIME V3 Client Profile	[F]	11/02
SP800-48r1	Guide to Securing Legacy IEEE 802.11 Wireless Networks	[F]	08/08
SP800-47	Security Guide for Interconnecting Information Technology Systems	[F]	08/02
SP800-46r1	Guide to Enterprise Telework and Remote Access Security	[F]	06/09
SP800-46	Security for Telecommuting and Broadband Communications	[F]	08/02
SP800-45V2	Guide On Electronic Mail Security	[F]	02/07
SP800-44V2	Guidelines on Securing Public Web Servers	[F]	09/07
SP800-43	System Administration Guidance for Windows00	[F]	11/02
SP800-42	Guidelines on Network Security testing	[F]	10/03

SP800-41r1	Guidelines on Firewalls and Firewall Policy	[F]	09/09
SP800-41	Guidelines on Firewalls and Firewall Policy	[F]	01/02
SP800-40-2	Creating a Patch and Vulnerability Management Program	[F]	11/05
SP800-39	Managing Risk from Information Systems: An Organizational Perspective	[R]	04/08
SP800-38E	Recommendation for Block Cipher Modes of Operation – XTS-AES	[F]	08/09
SP800-38D	Recommendation for Block Cipher Modes of Operation – GCM	[F]	11/07
SP800-38C	Recommendation for Block Cipher Modes of Operation – CCM	[F]	05/04
SP800-38B	Recommendation for Block Cipher Modes of Operation – RMAC	[F]	05/05
SP800-38A	Recommendation for Block Cipher Modes of Operation – Method and Techniques	[F]	12/01
SP800-37r1	Guidelines for the Security C&A of Federal Information Technology Systems	[R]	11/09
SP800-37	Guidelines for the Security C&A of Federal Information Technology Systems	[F]	04/04
SP800-36	Guide to IT Security Services	[F]	10/03
SP800-35	Guide to Selecting IT Security Products	[F]	10/03
SP800-34r1	Contingency Planning Guide for Information Technology Systems	[R]	10/09
SP800-34	Contingency Planning Guide for Information Technology Systems	[F]	06/02
SP800-33	Underlying Technical Models for Information Technology Security	[F]	12/01
SP800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure	[F]	02/01
SP800-31	Intrusion Detection Systems	[F]	11/01
SP800-30	http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf	[F]	01/04
SP800-29	Comparison of Security Reqs for Cryptographic Modules in FIPS 140-1 & 140-2	[F]	10/01
SP800-28v2	Guidelines on Active Content and Mobile Code	[F]	03/08
SP800-27A	Engineering Principles for Information Technology Security – Rev A	[F]	06/04
SP800-26r1	Guide for Inform. Security Program Assessments & System Reporting Form	[R]	08/05
SP800-26	Security Self-Assessment Guide for Information Technology Systems	[F]	11/01
SP800-25	Federal Agency Use of PK Technology for Digital Signatures and Authentication	[F]	10/00
SP800-24	Finding Holes in Your PBX Before Someone Else Does	[F]	08/00
SP800-23	Guidelines to Federal Organizations on Security Assurance	[F]	08/00
SP800-22r1	Statistical Test Suite for Random and Pseudorandom Number Generators	[F]	08/08
SP800-21	Guideline for Implementing Cryptography in the Federal Government	[F]	12/05
SP800-16r1	Information Security Training Requirements: A Role & Performance Based Model	[R]	03/09
SP800-12	An Introduction to Computer Security: The NIST Handbook	[F]	10/95

[F] Finalisé

[R] Relecture

POUR PLUS D'INFORMATION

<http://csrc.nist.gov/publications/PubsSPs.html>

- Catalogue des publications

CIS - CATALOGUE DE PROCEDURES ET DE TESTS



Le **CIS (Center for Internet Security)** a publié la mise à jour des procédures de test de l'équipement **Apple iPhone**. Par ailleurs, deux nouveaux catalogues ont été publiés: l'un traitant du système de base de données **IBM DB2** en environnement Linux, Unix et Windows, l'autre du système **VMWare ESX** dans sa version 3.5.

APPLICATIONS				
Apache	Versions V1.3.37/2.0.59/2.2.4	P1 P2	V2.2	Outil existant
Bind	Version 9.0 - 9.5		P2 V2.0	
FreeRadius	Version 1.1.3	P1	V1.0	
IBM	DB2 8-9.5	P1	V1.0	N
Microsoft	Exchange Server 2003	P1	V1.0	
	Exchange Server 2007	P1	V1.0	
	IIS Web Serveur versions 6.0	P1	V1.0	
	SQL Serveur 2000		P2 V1.0	
	SQL Serveur 2005	P1 P2	V1.1.1	
MySQL	Versions 4.1, 5.0, et 5.1 Community Edition	P1 P2	V1.0.2	
Novell	eDirectory version 8.7	P1	V1.0	
OpenLDAP	Versions 2.3.39/2.4.6	P1	V1.0	
Oracle	Base de données 8i	P1 P2	V1.2	Outil existant
	Base de données 9i et 10g	P1 P2	V2.0.1	
	Base de données 11g		V1.0.1	
SYBASE	Base de données ASE 15.0	P1	V1.0.0	
Virtual Machines				
VMWare	ESX 3.0	P1	V1.0	Fichiers d'aide
	ESX 3.5	P1	V1.0	N
XEN	Server 3.2	P1	V1.0	
SYSTEMES				
AIX	Versions 4.3.2, 4.3.3 et 5.1	P1	V1.0.1	Script
FreeBSD	Versions 4.10	P1	V1.0.5	Outil existant

HP-UX	Versions 11.11, 11.23 et 11.31	P1	V1.5.0	Outil existant
Linux	Debian	P1	V1.0	
	RedHat 4, Fedora Core 1, 2, 3, 5 et 5	P1	V1.0.5	
	RedHat 5	P1	V1.1.2	
	Slackware	P1	V1.1.0	
	SuSE	P1	V2.0.0	
Mac OS/X	Version 10.4	P1	V2.0	
	Version 10.5	P1	V1.0	
Novell	OES NetWare	P1	V1.0	
Solaris	Versions 10, 11/06 et 8/08	P1	V4.0	
	Version 10	P1	V2.1.2	
	Versions 2.5.1 - 9	P1	V1.3.0	Outil existant
Windows	2003 Servers & 2003 Domain controller	P1	V2.0	
	XP Professional SP1/SP2	P2	V2.01	
	2000 Professional	P2	V2.2.1	
	2000 Serveur	P2	V2.2.1	
	2000	P1	V1.2.2	
	NT	P1	V1.0.5	
EQUIPEMENTS MOBILES				
Apple	iPhone OS 3.1.2	P1	V1.1.0	M
EQUIPEMENTS RESEAU				
CISCO	IOS routeurs	P1 P2	V2.2	Outil existant
	PIX, ASA et FWSM	P1 P2	V2.0	
CheckPoint	FW1/VPN1	P1 P2	V1.0	
MFD	Multi-Function Devices	P1	V1.0.0	
Wifi	Générique	P1	V1.0	
	Addenda Apple	-	-	
	Addenda Cisco	-	-	
	Addenda DLink	-	-	
	Addenda Linksys	-	-	

P1: Profil minimal et conservateur
P2: Profil étendu et protectionniste

N: Nouveau
M : Modifié

POUR PLUS D'INFORMATION

- <http://www.cisecurity.org/benchmarks.html>
- https://www.cisecurity.org/tools2/iphone/CIS_Apple_iPhone_3.1.2_Benchmark_v1.1.0.pdf
- https://community.cisecurity.org/download/?redir=/db2/CIS_IBM_DB2_Benchmark_v1.0.0.pdf

DISA – GUIDES ET CHECK LISTES DE SECURISATION



La **DISA** a procédé à la mise à jour du guide et de la liste de contrôle des environnements 'Secure Remote Computing'.

[1 Mise(s) à jour, 0 Nouveau(x) Document(s)]

		Guide (STIG)		Check Liste	
APPLICATIONS					
Applications	Sécurité et Développement	2.1	24/08/08	2.1.5	26/06/09
	Services	1.1	17/01/06	1.1.1	21/09/06
	Microsoft Exchange 2003	1.1	17/09/09	1.1	17/09/09
		1.1	05/06/06	1.1.3	10/04/07
ESM		1.1	10/04/07	1.1.1	10/04/07
Database	Générique	8.1	19/10/07	8.1.2	28/08/09
	Oracle			8.1.5	23/10/09
	MS SQL Server 2005			8.1.3	23/10/09
ENVIRONNEMENTS					
Access Control		2.2	18/12/08		
Directory Service		1.1	10/03/06	1.1.5	28/08/09
Collaboration		1.1	28/03/07	1.1	28/03/07
Desktop		3.1	09/03/07	3.1.11	26/06/09
Enclave	Périmètre	4.2	31/03/08	4.2	31/03/08
				1.2.3	18/02/09
.NET					
Personal Computer Clients	Voix, Vidéo et Collaboration	1.1	26/06/08	1.1.1	15/08/08
Secure Remote Computing		2.1	02/10/09	2.1	02/10/09
Instant Messaging		1.2	15/02/08	1.2.5	15/04/09
Biométrie		1.3	10/11/05	2.1.1	17/10/07
VoIP		2.2	21/04/06	2.2.4	12/08/08
Vidéo Téléconférence		1.1	08/01/08	1.1.2	06/11/08
PERIPHERIQUES					
	Sharing peripheral across the network	1.1	29/07/05		

- Multi-Function Device (MFD) and Printer Checklist				1.1.3	09/04/09
- Keyboard, Video, and Mouse (KVM) Switch Checklist				1.1.3	19/12/08
- Storage Area Network (SAN) Checklist				1.1.4	26/06/09
- Universal Serial Bus (USB) Checklist				1.1.3	19/12/08
RESEAUX					
Network	Liste de contrôle générique	7.1	25/10/07	7.1.10	28/08/09
	Cisco			6.1	02/12/05
	Juniper			6.4	02/12/05
IP WAN	Générique			2.3	12/08/04
Wireless	Liste de contrôle générique	6.1	06/08/09	6.1	23/10/09
	BlackBerry			5.5	23/10/09
	Apriva			5.2.2	15/04/09
	Motorola			5.2.3	15/04/09
	Windows			5.2.4	15/04/09
Wireless	LAN Security Framework	2.1	31/10/05		
	LAN Site Survey	1.1	31/10/05		
	LAN Secure Remote Access	1.1	31/10/05		
	Mobile Computing	1.1	31/10/05		
SERVICES					
DNS	Générique	4.1	17/10/07	4.1.7	28/08/09
Web Servers	Générique	6.1	11/12/06	6.1.7	15/04/09
	IIS			6.1.11	26/06/09
	Netscape/Sun			6.1.6	26/06/09
	Apache			6.1.11	26/06/09
	TomCAT			6.1.5	14/04/09
	WebLogic			6.1.4	14/04/09
SYSTEMES					
OS/390 & z/OS	Générique	6.1.1	06/08/09	5.2.7	17/01/08
	Logical Partition	2.2	04/03/05	2.1.4	04/06
	RACF	6.1.2	28/08/09	6.1.2	28/08/09
	ACF2	6.1.2	28/08/09	6.1.2	28/08/09
	TSS	6.1.2	28/08/09	6.1.2	28/08/09
MacOS/X		1.1	15/06/04	1.1.3	28/04/06
TANDEM		2.2	04/03/05	2.1.2	17/04/06
UNISYS		7.2	28/08/06	7.2	24/11/06
UNIX		5.1	04/04/06	5.2	23/10/09
VM IBM		2.2	04/03/05	2.2.1	04/06
SUN	Solaris 2.6 à 2.9			-	20/01/04
	RAY 4	1.1.1	17/04/09	1.1.1	17/04/09
OPEN VMS				2.2.3	17/04/06
Windows	NT	3.1	26/12/02	4.1.21	28/07/08
	2000			6.1.14	23/10/09
	XP	1.8	12/01/03	6.1.14	23/10/09
	Vista			6.1.14	23/10/09
	2003			6.1.14	23/10/09
	2008			6.1.7	23/10/09
	Addendum 2000/XP/Vista/2003	6.1	21/05/07		
VMWare ESX		1.1.0	28/04/08	1.4.0	15/10/09
Citrix XENApp		1.1.2	15/10/09	1.1.2	15/10/09
AUTRE					
Best Practice Security	Générique			2.1	29/01/07

POUR PLUS D'INFORMATION

<http://iase.disa.mil/stigs/checklist/index.html>
<http://measurablesecurity.mitre.org/about/index.html>

INTERNET

LES DECISIONS DE L'OMPI



L'Organisation Mondiale de la Propriété Intellectuelle – **OMPI** ou **WIPO** – est chargée de l'arbitrage et de la résolution des litiges relatifs aux noms de domaine. Parmi tous les litiges jugés, en voici quelques uns concernant l'usage abusif de marques célèbres en France. On notera qu'un premier litige portant sur des noms de domaine 'localisés', utilisant des jeux de caractères étendus, apparait avec celui lié à l'enregistrement du nom de domaine 'creditmutuel.tv'

DFR2009-0026	3suiises.fr	Les 3 suisses	02/11
D2009-1186	baccarat-crystal.net	Baccarat SA	06/11
DTV2009-0008	creditmutuel.tv (xn--crditmutuel-cbb.tv)	Conf. Nat. du Crédit Mutuel	18/11
D2009-1170	guccifragrance.com	Guccio Gucci	04/11
DFR2009-0028	notre-temps.fr	Bayard Presse	06/11
D2009-1268	raymondweil.asia	Raymond Weil SA	09/11
D2009-1185	transiliensncf.com	SNCF	29/10

POUR PLUS D'INFORMATION

- <http://www.wipo.int/rss/index.xml?col=dnddocs> - Dernières décisions
http://www.wipo.int/freepublications/fr/arbitration/779/wipo_pub_779.pdf - Procédure de règlement des litiges

STANDARDS

IETF – LES RFC TRAITANT DIRECTEMENT DE LA SECURITE

Thème	Num	Date	Etat	Titre
DSSC	5698	11/09	Pst	Data Structure for the Security Suitability of Cryptographic Algorithms (DSSC)
IETF	5704	11/09	Inf	Uncoordinated Protocol Development Considered Harmful
IKE	5685	11/09	Pst	Redirect Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2)
PKI	5697	11/09	Exp	Other Certificates Extension

IETF – LES RFC LIES A LA SECURITE

Thème	Num	Date	Etat	Titre
IETF	5706	11/09	Inf	Guidelines for Considering Operations and Management of New Protocols and Protocol Extensions
SYSLOG	5674	10/09	Pst	Alarms in Syslog
MPLS	5695	11/09	Inf	MPLS Forwarding Benchmarking Methodology for IP Flows

IETF – LES NOUVEAUX DRAFTS TRAITANT DE LA SECURITE

Thème	Nom du Draft	Date	Titre
AFS3	draft-brashear-afs3-pts-extended-names-00	18/11	Authentication Name Mapping ext. for AFS-3 Protection Service
CRTYPTO	draft-turner-asymmetrickeyformat-algs-00	10/11	Algorithms for Asymmetric Key Package Content Type
DNSSEC	draft-ietf-dnsop-dnssec-dps-framework-00	25/11	DNSSEC Signing Policy & Practice Statement Framework
IPSEC	draft-harkins-ipsecme-spsk-auth-00	11/11	Secure PSK Authentication for IKE
NHDP	draft-herberg-manet-nhdp-sec-00	11/11	Cryptographical Signatures in NHDP
	draft-herberg-manet-nhdp-sec-threats-00	11/11	Security Threats for NHDP
PKCS	draft-josefsson-pbkdf2-test-vectors-00	11/11	Test vectors for PKCS #5 PBKDF2
PKI	draft-cooper-pkix-rfc5280-clarifications-00	20/11	Clarifications to the Internet X.509 PKI Certificate and CRL Profile
RFC4869	draft-law-rfc4869bis-00	10/11	Suite B Cryptographic Suites for IPsec
RXRPC	draft-tkeiser-rxrpc-sec-clear-00	12/11	Rx Security Object Providing Cleartext Peer Identity Assertions
SSH	draft-igoe-secsh-x509v3-00	10/11	X.509v3 Certificates for Secure Shell Authentication

IETF – LES MISES A JOUR DE DRAFTS TRAITANT DE LA SECURITE

Thème	Nom du Draft	Date	Titre
BFD	draft-bhatia-bfd-crypto-auth-01	11/11	BFD Generic Cryptographic Authentication
CRYPTO	draft-chudov-cryptopro-cpxmldsig-06	25/11	GOST 28147-89, R 34.10-2001, R 34.11-94 for XML Security
	draft-bhatia-manral-igp-crypto-requirements-04	11/11	Cryptographic Alg. Implementation Req. for Routing Protocols
	draft-nsri-aria-03	17/11	A Description of the ARIA Encryption Algorithm
	draft-dolmatov-cryptocom-gost34102001-06	10/11	GOST R 34.10-2001 digital signature algorithm
	draft-dolmatov-cryptocom-gost2814789-04	10/11	GOST 28147-89 encryption, decryption and MAC algorithms
	draft-cheneau-csi-ecc-sig-agility-01	22/11	ECC public key and signature support in CGA and in SEND
	draft-cheneau-csi-send-sig-agility-01	22/11	Signature Algorithm Agility in SEND Protocol
	draft-turner-ecprivatekey-01	19/11	Elliptic Curve Private Key Structure
DHCP	draft-jjmb-dhc-eap-auth-analysis-01	19/11	DHCP Authentication Analysis
DNSSEC	draft-ietf-dnsexst-dnssec-gost-04	22/11	Use of GOST signature algorithms in DNSKEY and RRSIG RR
	draft-ietf-dnsexst-dnssec-registry-fixes-01	12/11	DNSSEC DNSKEY IANA Registry Algorithm Status Addition
	draft-crocker-dnssec-algo-signal-05	12/11	Signaling Cryptographic Algorithm Understanding in DNSSEC
DSKPP	draft-ietf-keyprov-dskpp-09	16/11	Dynamic Symmetric Key Provisioning Protocol (DSKPP)
DTNRG	draft-irtf-dtnrg-bundle-security-12	20/11	Bundle Security Protocol Specification
EAP	draft-clancy-emu-aaapay-03	12/11	EAP Method Support for Transporting AAA Payloads
IPSEC	draft-ietf-ipsecme-aes-ctr-ikev2-03	25/11	Using AES Counter Mode with IKEv2
IPSEC	draft-ietf-msec-ipsec-group-counter-modes-04	25/11	Using Counter Modes with ESP and AH to Protect Group Traffic

MIKEY	draft-seokung-msec-mikey-seed-05	22/11	IANA Registry Update for Support of the SEED Cipher Algorithm
OPSEC	draft-ietf-opsec-efforts-11	15/11	Security Best Practices Efforts and Documents
	draft-ietf-opsec-routing-protocols-crypto...-02	11/11	Issues in Cryptographic Protection Methods for Routing Protocols
PKIX	draft-ietf-pkix-prqp-04	16/11	PKI Resource Query Protocol (PRQP)
	draft-ietf-pkix-certimage-03	10/11	Internet X.509 Public Key Infrastructure - Certificate Image
RADIUS	draft-nelson-isms-extended-vacm-01	20/11	Extensions to View-based Access Control Model
SAAG	draft-housley-saag-crypto-key-table-01	26/11	Database of Long-Lived Symmetric Cryptographic Keys
SIP	draft-ietf-sipcore-sec-flows-01	23/11	Example call flows using SIP security mechanisms
TLS	draft-hajjeh-tls-identity-protection-09	13/11	Credential Protection Ciphersuites for Transport Layer Security
	draft-rescorla-tls-renegotiation-01	17/11	Transport Layer Security (TLS) Renegotiation Indication Extension
	draft-mrex-tls-secure-renegotiation-01	25/11	Transport Layer Security (TLS) Secure Renegotiation
ZRTP	draft-zimmermann-avt-zrtp-16	10/11	ZRTP: Media Path Key Agreement for Secure RTP
TLS	draft-ietf-tls-renegotiation-01	26/11	Transport Layer Security (TLS) Renegotiation Indication Extension

DEVOTEAM

86 rue Anatole France 92300 Levallois-Perret
Tél. : +33 (0)1 41 49 48 48 - Fax : +33 (0)1 47 57 24 76
www.devoteam.com