

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

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

Détection Disclosure DNS DNSSec **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°138

JANVIER 2010

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:

Le défi RSA-768 remporté

La conférence ASACS

Quelques décisions de l'OMPI commentées

Après CVE, MAEC...

Les blocs d'adresses IPV4 réservés

La conférence 26C3

ENISA EQR Vol5 N°4

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

SUR LA RESILIENCE DU DNS	2
CRYPTOGRAPHIE - CHALLENGE RSA-768	2

ANALYSES ET COMMENTAIRES

CONFERENCES

ACSAC – 2009	4
<i>TrustGraph: Trusted Graphics Subsystem for High Assurance Systems</i>	4
<i>The Design of a Trustworthy Voting System</i>	5
<i>Analyzing Information Flow in JavaScript-based Browser Extensions</i>	5
<i>Symmetric Cryptography in Javascript</i>	6
<i>Detecting Software Theft via System Call Based Birthmarks</i>	7
CCC - 26 CHAOS COMMUNICATION CONGRESS	8
<i>Exposing crypto bugs through reverse engineering</i>	8
<i>How you can build an eavesdropper for a quantum cryptosystem</i>	9
<i>Hacking the Universe : When strings are super and not made of characters</i>	10
<i>Privacy, openness, trust and transparency on Wikipedia</i>	10
<i>Our darknet and its bright spots</i>	11
GSM – SRSLY?	12

LOGICIELS

NIRSOFT - WINPREFETCHVIEW	14
---------------------------	----

MAGAZINES

ENISA - QUARTERLY REVIEW	15
<i>Résilience, Notification d'incident et Exercices</i>	15
<i>Sensibilisation</i>	16
<i>Interopérabilité et Protection</i>	17
ISMS	17

METHODOLOGIES ET STANDARDS

METHODES

MITRE – MAEC MALWARE ATTRIBUTE ENUMERATION AND CHARACTERIZATION	18
---	----

RECOMMANDATIONS

NIST - SP800-131 'RECOMMENDATION FOR THE TRANSITIONING OF CRYPTOGRAPHIC ALGORITHMS AND KEY SIZES'	19
---	----

STANDARDS

RFC5735 / SPECIAL USE IPV4 ADDRESSES	20
--------------------------------------	----

TABLEAUX DE SYNTHESE

CONFERENCES

CCC - 26 CHAOS COMMUNICATION CONGRESS	22
ACSAC – 2009	23
IAWACS – 2009	24

GUIDES

NIST – ETAT DES GUIDES DE LA SERIE SPECIALE 800	25
DISA – GUIDES ET CHECK LISTES DE SECURISATION	27
CIS - CATALOGUE DE PROCEDURES ET DE TESTS	28

MAGAZINES

ENISA - QUARTERLY REVIEW	29
--------------------------	----

INTERNET

LES DECISIONS DE L'OMPI	30
-------------------------	----

STANDARDS

IETF – LES RFC TRAITANT DIRECTEMENT DE LA SECURITE	30
IETF – LES RFC LIES A LA SECURITE	31
IETF – LES NOUVEAUX DRAFTS TRAITANT DE LA SECURITE	31
IETF – LES MISES A JOUR DE DRAFTS TRAITANT DE LA SECURITE	31

Le mot du rédacteur

Ce premier mois de l'année 2010 n'aura décidément pas été de tout repos, deux vulnérabilités découvertes dans le lecteur **Acrobat** (CVE-2009-4324) et dans **IE** (CVE-2010-0249) ayant été largement exploitées. Ces deux vulnérabilités ont en effet été utilisées dans le cadre d'une attaque de grande envergure, une opération dévoilée le 14 janvier et désormais désignée sous le nom de code '**Aurora**'.

<http://siblog.mcafee.com/cto/operation-%E2%80%99Caurora%E2%80%99D-hit-google-others/>

Après avoir annoncé le jour même qu'aucun correctif ne serait disponible hors du cycle de mise à jour normal, le second mardi de chaque mois, Microsoft devait rapidement faire volte-face en délivrant un correctif 'hors bande' dès le 21 janvier.

<http://www.microsoft.com/technet/security/advisory/979352.mspx>

La publication du code d'exploitation, et la reprise par la presse du monde entier de la recommandation d'utiliser *un navigateur alternatif dans l'attente d'un correctif* émise dès le 15 janvier par deux CERTS européens, dont le **CERTA**, a très probablement bien fait avancer les choses.

<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-001/>

La période de calme de la fin d'année dont nous parlions dans notre éditorial de décembre aura finalement été, hélas, de très courte durée. D'autres problèmes se profilent à l'horizon, en particulier d'ordre technique, qui laissent à penser que 2010 ne sera, de toutes façons, pas une année tranquille. Nous recommandons à ce propos la lecture du message qu'a publié **Stéphane Borzmeyer** sur la liste **FrNog** concernant l'impact de la signature **DNSSEC** des serveurs DNS racines.

<http://www.mail-archive.com/frnog@frnog.org/msg08914.html>

Nous terminerons en rappelant que le **CLUSIF** a mis en ligne son **Panorama de la Cybercriminalité** pour l'année 2009.

<http://www.clusif.asso.fr/fr/production/ouvrages/pdf/PanoCrim2k9-fr.pdf>

BONNE ANNEE 2010 A TOUS

BERTRAND VELLE

Deux informations de toute dernière minute:

- l'**ANSSI** vient de publier un guide à l'attention des voyageurs qui leur propose quelques règles applicables à la sécurisation des données stockées dans les téléphones, PDA, portables et autres équipements. A lire absolument.

http://www.securite-informatique.gouv.fr/IMG/pdf/Passeport-de-conseils-aux-voyageurs_janvier-2010.pdf

- l'**AFNIC** vient de diffuser un communiqué de presse « *invitant les responsables techniques réseaux à se préparer à la signature de la racine DNS en mai 2010* ».

<http://www.afnic.fr/actu/nouvelles/240/l-afnic-invite-les-responsables-techniques-reseaux-a-se-preparer-a-la-signature-de-la-racine-dns-en-mai-2010>

ACTUALITES SECURITE

SUR LA RESILIENCE DU DNS



La catastrophe ayant touché **Haïti** a mis à mal les moyens de communication du pays, quels qu'ils soient, ou presque. L'absolue nécessité de disposer de canaux de communication alternatifs, fiables, simples à mettre en œuvre et résilients s'était déjà posée lors du drame du 11 septembre 2001.

En ce qui concerne **Haïti**, et au regard des informations actuellement disponibles, il apparaît qu'une partie de l'infrastructure d'accès était encore fonctionnelle dans les heures ayant suivi le sinistre, les premières informations diffusées sur Internet le prouvent. Il faudra cependant se garder de prétendre que cela est le résultat des caractéristiques intrinsèques d'Internet, réseau conçu dit-on par le **DARPA** pour résister à toutes les agressions.

Internet est en effet robuste par conception et supporte désormais de multiples technologies d'accès dans sa constitution actuelle, dont des technologies sans fils ne requérant aucune liaison physique. Ces technologies - **WIFI**, **WiMax**, **3GPP** ou encore accès satellitaires - sont par nature indépendantes de toute contrainte environnementale, et sont donc susceptibles de continuer à fonctionner, sous réserve de disposer d'un approvisionnement énergétique et d'un maillage suffisant, quand les liaisons physiques traditionnelles - cuivre ou fibre - auront été rompues. C'est probablement par le biais de liaisons sans-fils que quelques haïtiens ont pu continuer d'accéder au réseau.

Encore faut-il que les services fondamentaux, tel le système de gestion et de résolution des noms ou DNS, continuent de fonctionner, et pour cela mieux vaut avoir pris au pied de la lettre le célèbre dicton 'il ne faut pas mettre tous ses œufs dans le même panier'. En dans ce domaine, les opérateurs en charge du domaine de tête - TLD - identifiant le pays, **.ht** dans le cas présent, ont fait preuve d'une très grande sagesse, en dupliquant et en délocalisant les serveurs de noms responsables de cette zone.

Comme le fait remarquer **Stéphane Borzmeyer** dans une remarquable analyse des événements post sinistre, le **.ht** n'a jamais cessé de fonctionner. La résolution des noms inscrits dans ce domaine aura continué de fonctionner, et ainsi d'autoriser l'accès aux sites où qu'ils se trouvent dans le monde, à l'exception de ceux situés en Haïti.

Le dit article, intitulé '[Reconfiguration des serveurs de noms du domaine haïtien](#)', a l'immense mérite de mettre en évidence, sur un cas hélas tragique, la nécessité d'organiser son système de gestion des noms afin de le rendre insensible aux aléas, que ceux-ci soient d'origine naturelle ou qu'ils résultent d'une volonté délibérée de nuire. Le cas cité dans l'article du domaine **.pf** (Polynésie Française) géré par deux serveurs tous deux situés à Papeete laisse à réfléchir, en particulier s'agissant d'un territoire politiquement sensible.

POUR PLUS D'INFORMATION

<http://www.bortzmeyer.org/dns-haiti.html>
<http://blog.icann.org/2010/01/haiti/>

CRYPTOGRAPHIE - CHALLENGE RSA-768



En mai 2001, la société **RSA Security** lançait une série de 8 défis cryptographiques dotés d'une prime de \$10 000 à \$200 000. Chacun de ces défis était identifié par la taille du nombre devant être factorisé exprimée en bits.

En décembre 2003 le premier défi de cette série, **RSA-576**, était remporté par une équipe allemande du BSI qui deux ans plus tard, en novembre 2005, remportait aussi le second défi, **RSA-640**, un nombre de quelques 193 chiffres décimaux (Rapport N°88 - Novembre 2005). Cette performance conduisait à revoir les recommandations en matière de longueurs de clef, du moins pour les clefs devant assurer une protection à long terme. En effet, si le matériel employé était accessible à toute organisation disposant d'un budget de l'ordre de 200K€, une telle opération n'a d'intérêt qu'à la condition que le gain espéré soit largement supérieur au coût global requis pour casser la clef, à savoir l'acquisition du matériel et son exploitation durant toute la durée des calculs, 18 semaines dans le cas cité.

Le 7 janvier dernier, soit quatre ans après la dernière annonce, une équipe internationale (EPFL, INRIA, Université de Bonn, NTT, et CWI) vient de remporter le quatrième défi, **RSA-768**, en factorisant un nombre comportant 232 chiffres décimaux:

```
1230186684530117755130494958384962720772853569595334792197322452151726400507263657518  
7452021997864693899564749427740638459251925573263034537315482685079170261221429134616
```

70429214311602221240479274737794080665351419597459856902143413

Un résultat remarquable qui marquera les esprits, comme ce fût le cas avec l'annonce précédente, puisque dans les deux cas, la taille de la clef correspond à des valeurs considérées il y a seulement dix ans comme optimales, et aptes à être utilisées pour des clefs à long terme. Désormais, il convient de considérer devoir utiliser de tailles de clef de 1024bits pour le 'tout venant' et de 2048 voir 4096 bits pour le long terme (Rapport N°134 – Septembre 2009).

Série de Défis		Taille digit/bits	Date	Coût estimé	Approche
Ancienne	Nouvelle				
RSA-100		100 / NA	1991	NA	
RSA-110		110 / NA	1992	NA	
RSA-120		120 / NA	06/1993	830 MIPS years	MPQS
RSA-129		129 / 426	04/1994	5000 MIPS years	MPQS
RSA-130		130 / 428	10/04/1996	1000 MIPS years	GNFS
RSA-140		140 / 465	02/02/1999	2000 MIPS years	GNFS
RSA-155		155 / 512	22/08/1999	8000 MIPS years	GNFS
RSA-160		160 / 530	01/04/2003	2.7 Pentium 1GHz CPU years	GNFS
	RSA-576	174 / 576	03/12/2003	13.2 Pentium 1GHz CPU years	GNFS
	RSA-640	193 / 640	08/11/2005	~12.0 Opteron 2GHz CPU years	GNFS
RSA-200		200 / 663	05/2005	121.0 Pentium 1GHz CPU years	GNFS
	RSA-704	212 / 704	Non Factorisé		
	RSA-768	232 / 768	07/12/2009	3300.0 Opteron 1GHz CPU years	GNFS
	RSA-896	270 / 896	Non Factorisé		
	RSA-1024	309 / 1024	Non Factorisé		
	RSA-1536	463 / 1536	Non Factorisé		
	RSA-2048	617 / 2048	Non Factorisé		

Une phénoménale évolution sur seulement deux décennies qui auront vu l'amélioration des procédés de factorisation – abandon de l'approche **MPQS** (Multiple Polynomial Quadratic Sieve) au profit de l'approche **GNFS** (General Number Field Sieve) – et les performances des systèmes de calcul s'envoler.

Il conviendra de prendre en compte les recommandations exposées en introduction du rapport de recherche rédigé par l'équipe ayant mené à terme cette factorisation (*Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen K. Lenstra, Emmanuel Thomé, Joppe W. Bos, Pierrick Gaudry, Alexander Kruppa, Peter L. Montgomery, Dag Arne Osvik, Herman te Riele, Andrey Timofeev, and Paul Zimmermann*).

Because the first factorization of a 512-bit RSA modulus was reported only a decade ago (cf. [7]) it is not unreasonable to expect that 1024-bit RSA moduli can be factored well within the next decade by an academic effort such as ours or the one in [7]. Thus, it would be prudent to phase out usage of 1024-bit RSA within the next three to four years.

Il n'y a pas encore le feu, et il reste suffisamment de temps pour préparer cette évolution. Encore faut-il l'inscrire dès aujourd'hui dans la liste de projets à engager sur l'année à venir.

POUR PLUS D'INFORMATION

<http://www.crypto-world.com/FactorAnnouncements.html>
<http://eprint.iacr.org/2010/006.pdf>

- Liste des records de factorisation

ANALYSES ET COMMENTAIRES

CONFERENCES

ACSAC – 2009



L'**ACSAC** (Annual Computer Security Applications Conference) fait partie de ces conférences, avec celles de l'**IEEE**, qui privilégient les communications portant sur la résolution pratique, ou théorique, d'un problème de sécurité.

Une approche positive de la sécurité qui, depuis quelques années, tend à faire défaut dans les trop nombreuses conférences traitant de ce thème. Ici point d'annonces fracassantes sur la mise en défaut d'un système mais des propositions d'amélioration astucieuses et réfléchies qui ne feront jamais la Une de la presse à sensation.

Les 42 communications qui ont été présentées dans la 25^{ième} édition de cette conférence sont toutes plus intéressantes les unes que les autres dans des domaines très variés. Ne pouvant toutes les commenter nous limiterons à celles nous ayant paru proposer une approche novatrice ou résolvant un problème d'actualité.

TRUSTGRAPH: TRUSTED GRAPHICS SUBSYSTEM FOR HIGH ASSURANCE SYSTEMS

Okhravi, Nicol

L'apparition à la fin des années 70 d'interfaces de présentation autorisant l'affichage simultané de multiples applications, et le transfert de données de l'une à l'autre par des mécanismes non conventionnels – le presse-papier par exemple – a rapidement soulevé un problème de sécurité en particulier dans les environnements contraints. En autorisant le transfert de données entre applications par le biais de canaux non contrôlés, et sous la seule responsabilité de l'opérateur, ces interfaces offraient la possibilité de court-circuiter les mécanismes de sécurité installés au sein du système d'exploitation.

Un problème d'autant plus complexe que le système de présentation graphique le plus performant de l'époque – le système **X11** développé par le **MIT** en 1984 – avait été conçu sous la forme d'un système client/serveur indépendant du système d'exploitation sous-jacent en embarquant un système de sécurité minimaliste. Ainsi, rien ne permettait d'interdire la capture de la souris par une application, ou encore la copie de données, via le presse papier, entre deux applications s'exécutant sous des comptes, ou avec des privilèges, différents. Un problème que rencontrera bien plus tard le système Windows avec plusieurs failles de sécurité liée à cette ressource partagée difficilement sécurisable.

Il faudra attendre 1987 pour voir apparaître des systèmes, en particulier chez SUN, dits '**CMW**' (Compartmented Mode Workstation), proposant une interface graphique multi-fenêtrée autorisant l'exécution d'applications dotés de privilèges distincts et respectant pourtant les fondamentaux de la sécurité, dont le principe '*' du modèle **Bell-Lapaluda** fort apprécié du **DoD**. Pour mémoire, ce principe stipule qu'une donnée peut être copiée vers un niveau d'habilitation supérieur, l'inverse étant interdit. Ces systèmes s'appuyant sur un mécanisme de labellisation des flux de données d'un bout à l'autre la chaîne, y compris sur le réseau, étaient certes sécurisés mais étaient aussi difficilement exploitables, l'ergonomie apportée par l'interface graphique étant mise en défaut par les multiples contraintes de sécurité.

Les modèles de sécurité mandataires n'ayant pas eu grand succès hors de certains environnements, la problématique du partitionnement d'un système à niveaux de sécurité multiples – **MLS** (Multi Level Secure) ou **MILS** (Multi Independent Level Secure) – a rarement été traitée.

La donne a changé depuis peu avec la vulgarisation des technologies de virtualisation, et des problèmes associés quand un même système physique partage ses ressources entre plusieurs environnements virtuels n'ayant pas les mêmes exigences de sécurité.

Dans cette communication, **Hamed Okhravi** et **David Nicol**, de l'Université Urbana-Champaign de l'Illinois, présentent '**TrustGraph**', un sous-système graphique

1. **Introduction**
2. **Background**
3. **Threat model**
4. **Design**
 - A. Principles
 - B. Labeled Resources
 - C. Secure Methods
 - D. Secure Operations
 - E. Window Manager
5. **Implementation**
 - A. Compatibility
 - B. End-to-End Implementation
6. **Evaluation and Formal methods**
 - A. Functionality Testing
 - B. Attack Evaluation

sécurisé adapté aux exigences des systèmes **MLS** et **MILS**. Pour éviter de réinventer la poudre, les auteurs ont intelligemment choisi de s'appuyer sur **DirectFB**, un environnement de fenêtrage existant.

- C. Formal Verification
- D. Covert Channel Analysis
- 7. Related work
- 8. Conclusion

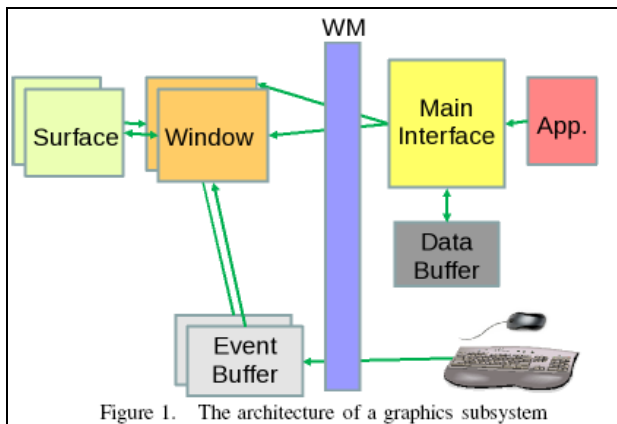


Figure 1. The architecture of a graphics subsystem

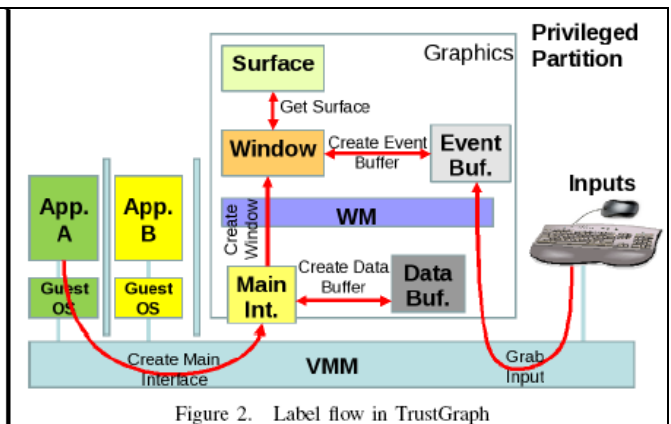


Figure 2. Label flow in TrustGraph

Les auteurs justifient le choix d'un système bien moins répandu que le système **X-Windows** par sa simplicité et ses performances au regard d'un système devenu trop complexe, instable et utilisant un modèle client/serveur inadapté aux besoins.

http://www.acsac.org/2009/openconf/modules/request.php?module=oc_program&action=view.php&id=46

THE DESIGN OF A TRUSTWORTHY VOTING SYSTEM

Paul, Tanenbaum

Nathanael Paul et **Andrew S. Tanenbaum**, deux chercheurs de l'université **Vrije** d'Amsterdam, traitent d'un sujet de fond, celui de la conception d'un système de vote digne de confiance. Dans le cas présent, le terme de 'protocole de vote' serait probablement plus adapté, leur communication ne se limitant pas à la simple description d'un schéma mathématique, ou cryptographique, mais bien à celle de l'ensemble des neuf étapes permettant de garantir la prise en compte du vote d'un citoyen sans que quiconque ne puisse remettre en cause l'intégrité et l'impartialité du système.

Le protocole proposé s'appuie sur une machine d'enregistrement constituée d'un matériel utilisant de préférence un processeur **AMD** et intégrant un module de sécurité conforme à la spécification **TPM V1.2**, une machine récente par exemple.

La solidité du protocole repose sur le respect de trois conditions fondamentales:

- 1- Le matériel de la machine à voter fonctionne correctement et n'a pas été compromis,
- 2- La clef privée du module TPM n'a pas été exposée,
- 3- Tous les logiciels susceptibles de s'exécuter durant le processus de vote sont listés dans le module.

Outre ces conditions, les auteurs posent comme principe que les sources de l'application de vote devront être publiées afin que toute personne le désirant puisse les vérifier.

Un choix qui, dans ce contexte, pourrait être le bon à condition toutefois de pouvoir garantir que le code s'exécutant a bien été généré à partir des sources publiées mais aussi par le biais d'outils – compilateur et éditeur de lien par exemple – intègres.

Une contrainte qui n'est hélas pas abordée, quand les auteurs considèrent pourtant que tout citoyen pourra vérifier la signature du code s'exécutant par le biais d'un échange sécurisé.

Nous ne pouvons nous prononcer sur la viabilité de cette proposition mais force est de constater que le protocole proposé par les auteurs prend en compte des problèmes rencontrés avec les systèmes actuels. Un travail de fond qui, n'en doutons pas, devrait a minima permettre d'améliorer les systèmes existants.

http://www.acsac.org/2009/openconf/modules/request.php?module=oc_program&action=view.php&id=62

- 1. Introduction
- 2. Assumptions
- 3. Outline of the Proposed Voting System
 - Step 1: Precinct Master Key Generation & Distribution
 - Step 2: Voter Registration
 - Step 3: Proof of Registration Mailed to the Voters
 - Step 4: Voting Machines are Prepared
 - Step 5: Key Assembly at Each Precinct
 - Step 6: Voters Show up and Check in
 - Step 7: Voters Cast Their Votes
 - Step 8: Tabulating the Votes
 - Step 9: Publishing the Result.
- 4. Discussion
- 5. Related Work
- 6. Conclusion

ANALYZING INFORMATION FLOW IN JAVASCRIPT-BASED BROWSER EXTENSIONS

Dhawan & Al.

Mohan Dhawan et Vinod Ganapathy, de l'université américaine de **Rutgers**, présente **SABRE** – Security Architecture for Browser Extensions – un environnement d'analyse du comportement des

modules d'extension du navigateur **Firefox**, modules écrits en JavaScript et dénommés JSE (JavaScript Extensions). Cet environnement a été développé dans l'optique de détecter les problèmes de sécurité liés à l'utilisation de tels modules, qu'il s'agisse d'une atteinte à l'intégrité du poste de travail ou à la confidentialité des données hébergées sur celui-ci.

En environnement **Firefox**, ces modules d'extension ont en effet la capacité d'accéder aux ressources fondamentales du système hôte, le code JavaScript de tels modules s'exécutant avec les privilèges du navigateur, et non avec des privilèges réduits comme cela serait le cas pour le code d'une application WEB.

Une approche en totale contradiction avec les principes fondamentaux de séparation des traitements et de l'exécution au moindre privilège s'il ne s'agissait de modules permettant d'étendre les fonctionnalités du navigateur, et non d'applications simplement présentées par celui-ci.

Cette communication est intéressante tant pour l'exposé des principes utilisés par **SABRE** pour tracer les flux d'information, et déterminer les risques d'atteinte à la confidentialité et à l'intégrité, que pour l'analyse de la conception de quelques **JSE Firefox** connus, dont **AdBlock Plus**, **GreaseMonkey**, **NoScript** ou encore **Web-of-Trust**. Un tableau de synthèse détaille notamment les interactions de quelques uns des modules d'extension les plus connus avec leur environnement.

- 1. **Introduction**
- 2. **Background and Motivating Examples**
- 3. **Tracking Information Flow with Sabre**
 - 3.1. Security Labels
 - 3.2. Sources and Sinks
 - 3.3. Propagating Labels
 - 3.4. Declassifying and Endorsing Flows
- 4. **Evaluation**
 - 4.1. Effectiveness
 - 4.2. Performance
- 5. **Related Work**
 - Browser extension security
 - JavaScript information flow
 - JavaScript sandboxing
- 6. **Conclusion**

JSE	Advertised Functionality of JSE	1	2	3	4	5
1. Adblock Plus	Prevent page elements, such as ads, from being downloaded		✓	✓		
2. All-in-One-Sidebar	Sidebar control to switch between sidebar panels and view dialog windows			✓		
3. CoolPreviews	Preview links and images without leaving current page or tab.		✓	✓		
4. Download Statusbar	Manage downloads from a tidy statusbar			✓		
5. Fast Video Download	Easy download of video files from popular sites				✓	
6. Forecastfox	Gets weather forecasts from AccuWeather.com		✓	✓	✓	
7. Foxmarks Synchronizer	Keeps bookmarks and passwords backed up and synchronized		✓	✓		
8. Ghostery	Alerts user's about web bugs, ad networks and widgets on webpages		✓	✓		
9. GooglePreview	Inserts thumbnails and ranks of web sites into Google search results		✓	✓		
10. Greasemonkey (0.8.1)	Allows users customize webpages with user scripts		✓	✓		
11. NoScript	Restricts executable content to trusted domains		✓	✓		
12. PDF Download	Tool for handling, viewing and creating Web-based PDF files		✓	✓	✓	
13. Pwdhash	Customizes user passwords to domains to prevent phishing	✓				
14. SpeedDial	Easy access to frequently visited websites			✓	✓	
15. StumbleUpon	Discovers web sites based on user's interests		✓	✓	✓	
16. Stylish	Easy management of user styles to enhance browsing experience		✓	✓	✓	✓
17. Tab Mix Plus	Enhances Firefox's tab browsing capabilities			✓	✓	
18. User Agent Switcher	Switches the user agent of the browser			✓		
19. Video DownloadHelper	Tool for web content extraction		✓	✓		
20. Web-of-Trust	Warns users before they interact with a harmful site		✓	✓	✓	

(1) HTML forms; (2) HTTP channels; (3) File system; (4) Loading URLs; (5) JavaScript events.

http://www.acsac.org/2009/openconf/modules/request.php?module=oc_program&action=view.php&id=10

SYMMETRIC CRYPTOGRAPHY IN JAVASCRIPT

Stark & Al.

Comme son titre le laisse entendre, la communication '**Symmetric Cryptography in Javascript**' proposée par trois chercheurs de l'université américaine de Stanford traite de l'implémentation d'algorithmes cryptographiques en langage JavaScript.

Un thème qui pourrait apparaître sans grand intérêt – pourquoi donc implémenter un algorithme consommateur de ressources dans un langage interprété et donc a priori peu performant – s'il n'était l'usage de plus en plus fréquent de la cryptographie au plus près des applications s'exécutant dans l'environnement d'un navigateur, un client d'accès à un service hébergé dans les nuages par exemple.

Si l'on peut envisager qu'un module d'extension puisse faire appel à une implémentation logicielle, ou matérielle, optimisée externe ayant accès aux ressources du système, il n'en va pas de même dans le cas d'une application WEB laquelle devra s'appuyer sur les seules ressources mises à sa disposition par le serveur distant, une librairie de fonctions par exemple.

Quelques librairies cryptographiques **JavaScript** sont d'ores et déjà disponibles qui offrent une algorithmique **AES** avec performances acceptables, honorables pourrions nous dire dans un tel contexte. Rappelons en effet que le langage JavaScript est un langage interprété.

Souhaitant pouvoir disposer d'une librairie offrant à la fois d'excellentes performances, et une taille réduite notamment pour limiter le temps de chargement et l'occupation mémoire, les auteurs sont partis de l'hypothèse que les techniques d'optimisation usuelles en environnement natif peuvent ne pas

offrir les gains de performance attendus en environnement interprété.

Un postulat qui les conduira à étudier les spécificités des implémentations de l'interpréteur **JavaScript** dans les principaux environnements de navigation – **Chrome, IE 8, Safari 4, Firefox 3.0 et 3.5.**

Implementation	Size (B)	Speed (kB/s)				
		Chrome	IE 8b	Safari 4	Firefox 3.0	Firefox 3.5b5
Our code	5687	585.2	60.4	264.8	97.4	451.6
Clipperz	9395	58.6	2.1	12.3	4.8	5.4
EKU	14667	99.0	2.7	136.9	5.1	42.8
BrowserSync	15916	125.9	5.2	231.5	21.8	62.3
Javascript	6455	16.2	1.3	33.6	13.3	13.9
Movable Type	6460	111.4	5.2	110.7	13.1	45.8
Improvement	12%	365%	1062%	14%	347%	625%

CRUNCHED SIZES AND SPEEDS FOR VARIOUS JAVASCRIPT AES IMPLEMENTATIONS.

Cette étude leur permettra de produire une librairie non seulement plus petite (12%) que la plus petite des librairies disponibles mais aussi onze fois plus performante que la plus performante de ces mêmes librairies.

	Time (ns)				
	Chrome	IE 8b	Safari 4	Firefox 3.0	Firefox 3.5b5
Fastest bitwise operation	1.76	35.4	10.1	4.96	1.55
Table lookup	1.81	32.9	10.7	4.48	23.80
132 bitwise operations	232	4673	1333	655	205
16 table lookups	29	526	172	72	381

TIMINGS FOR BITWISE OPERATIONS AND TABLE LOOKUPS ACROSS BROWSERS.

Une belle réussite au regard de la variation des performances des implémentations de fonctions simples (OU exclusif et recherche dans une table) sur les navigateurs étudiés.

Les auteurs ont étendu le périmètre de recherche à l'analyse de la qualité de la génération de séquences pseudo-aléatoire par la fonction '**Random**' proposé par la librairie standard '**Math**'. Ils ont constaté que celle-ci ne pouvait être utilisée dans le contexte d'un système de sécurité, et que la seule fonction apte à remplir ce rôle, '**Window. Crypto.Random**' livrée avec **Netscape 4** n'était plus disponible avec les principaux navigateurs du marché. Un générateur pseudo aléatoire offrant les qualités requises a donc été développé.

Les sources de la librairie '**jsCrypto**' – quelques 44Ko commentaires inclus – sont librement accessibles sur le site du groupe de cryptographie appliquée de l'université de **Stanford**.

<http://crypto.stanford.edu/sjcl/>

http://www.acsac.org/2009/openconf/modules/request.php?module=oc_program&action=view.php&id=116

1. **Introduction**
2. **Background**
3. **Fast And Small Aes In Javascript**
 - A. Maximizing precomputation
 - B. Loop unrolling
 - C. Bitslicing
 - D. Unifying encryption and decryption functions
4. **Randomness In Javascript**
 - A. Explicit random number generators
 - B. Operations which implicitly use entropy
 - C. RFC 4086
 - D. User interaction
 - E. Cookies
 - F. PRNG
5. **Experiments**
 - A. Comparison to other implementations
 - B. Effects of precomputation
 - C. Effects of loop unrolling
 - D. Comparison to other algorithms
6. **Conclusion**

DETECTING SOFTWARE THEFT VIA SYSTEM CALL BASED BIRTHMARKS

Wang & Al.

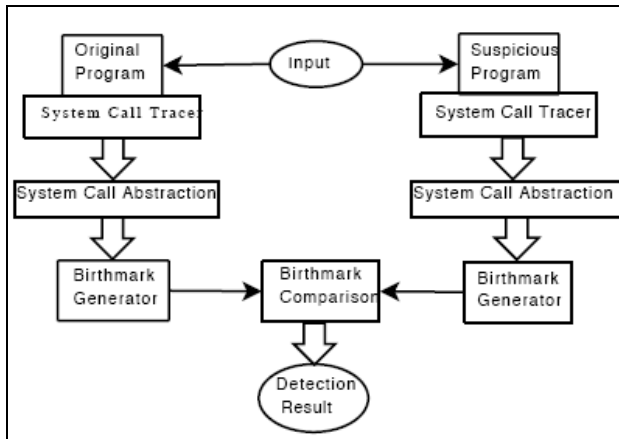
Cette communication proposée par quatre chercheurs de l'université de **Pennsylvanie** aborde la problématique de la détection du plagiat dans le domaine de l'ingénierie logicielle. Un problème qui se pose avec d'autant plus d'importance que l'avènement du modèle **Open Source** a amené quelques développeurs et sociétés à prendre de trop grandes libertés avec les modèles de licence associées à des codes sources accessibles à tous.

La viabilité économique de ce modèle, et plus largement du marché du développement logiciel, passe par la mise en place d'une surveillance laquelle ne peut s'exercer efficacement sans disposer d'outils permettant de déterminer, avec une faible marge d'erreur, si l'application examinée est la 'copie' d'une autre application, ou contient une portion d'un code développé par un tiers.

Les auteurs de la communication présentent deux méthodes de détection s'appuyant sur la recherche de similarités entre l'application originale, et celle soupçonnée d'être une copie. Par copie, on entendra la reproduction à l'identique du programme original avec l'éventuelle application de transformations

destinées à masquer les similitudes sans pour autant modifier le comportement du programme. Plusieurs transformations invariantes de ce type sont connues qui vont de la modification des options d'optimisation du compilateur pour générer un code différencié ou pour rendre celui-ci inintelligible – obfuscation – à la simple lecture.

Ces deux méthodes - **SCSSB** (System Call Short Sequence Birthmark) et **IDSCSB** (Input Dependand System Call Subsequence Birthmark) – sont basées sur la recherche d'invariants simples dans le code, à savoir les appels systèmes.



1. **Introduction**
2. **Problem Formalization**
 - A. Software Birthmarks
 - B. System Call Birthmarks
 - C. System Call Short Sequence Birthmark
 - D. Measurement Of Birthmark Similarity
3. **System Design And Implementation**
 - A. System Call Tracer
 - B. System Call Abstraction
 - C. Birthmark Generator
 - D. Input Dependand System Call Subsequence Birthmarks
4. **Evaluation**
5. **Discussion**
 - A. Counterattacks
 - B. Limitations
6. **Related Work**
7. **Conclusion**

D'après les auteurs, l'approche est viable: appliquées à plusieurs programmes ayant été manipulés par l'outil 'SandMark', les deux méthodes ont permis d'identifier les plagiats. La seconde méthode serait à même d'identifier une copie dans laquelle des appels systèmes 'bidons' auraient été insérés pour leurrer l'analyse. Les deux méthodes partagent cependant une limitation inhérente à leur mode d'analyse: elles ne sont pas adaptées aux programmes fortement indépendant du système – calcul pur par exemple – et ne faisant par conséquent pas, ou peu, d'appels systèmes.

http://www.acsac.org/2009/openconf/modules/request.php?module=oc_program&action=view.php&id=147

POUR PLUS D'INFORMATION

http://www.acsac.org/2009/openconf/modules/request.php?module=oc_program&action=program.php&p=program

CCC - 26 CHAOS COMMUNICATION CONGRESS



Le congrès annuel du célèbre **CCC** – Chaos Computer Club – allemand n'est plus à présenter. Il explore cette année des territoires dangereux où l'on risque à tout instant de rencontrer des 'dragons'. C'est en tout cas ce que suggère le slogan **'Here be Dragons'** superbement illustré.

Il nous est impossible de commenter les 72 communications effectuées à l'occasion de cette conférence, dont certaines sont publiées dans la langue de Goethe. Six d'entres-elles ont plus particulièrement attiré notre attention, et feront donc l'objet d'une rapide présentation.

EXPOSING CRYPTO BUGS THROUGH REVERSE ENGINEERING

Philippe Oechslin

Philippe Oechslin est particulièrement connu pour sa contribution à l'optimisation de l'attaque en force d'un algorithme de chiffrement. Enseignant chercheur à l'EPL, il est en effet l'inventeur d'une technique permettant d'optimiser le parcours d'une table de code, c'est-à-dire une table mettant en regard une chaîne de caractères et le résultat de son chiffrement pour une clé donnée. Dénommée tables 'Arc en Ciel', les tables de recherche ainsi optimisées ont connu un grand succès et ont été appliquées au schéma de chiffrement de mots de passe Windows, puis aux mécanismes de condensation **MD5** et **SHA1** puis, enfin, à l'algorithme de protection des communications **GSM** dit '**A5/2**'.

L'auteur n'intervient cependant pas ici à ce propos, mais pour présenter les résultats d'une analyse de sécurité, qu'il a mené avec sa société **OS Objectif Sécurité**, sur trois produits commerciaux. Trois exemples concrets d'une mise en défaut de la sécurité liée à des erreurs élémentaires dans la conception, ou l'implémentation, des mécanismes. A méditer.

La première cible est une clé USB certifiée conforme aux exigences **FIPS 142-3 Level 2** par le **NIST** américain, un niveau d'exigences somme toute relativement faible. Le niveau 2 stipule simplement que le niveau de sécurité physique du dispositif devra être renforcé au regard de celui du niveau 1 qui n'impose aucune protection d'aucune sorte. Le **NIST** précise que des procédés permettant de visualiser l'atteinte à l'intégrité de la protection physique, et donc d'avertir de la compromission possible des clés embarquées, devront être mis en œuvre: sceaux d'intégrité, revêtement spécifique... Les exigences concernant la protection d'accès aux secrets – tel l'effacement de ceux-ci en cas d'effraction –

apparaissent au niveau 3. Une réalité totalement oubliée des médias qui dernièrement n'ont pas hésité à mettre en cause la certification **NIST** après que des problèmes de sécurité dans l'implémentation du contrôle d'accès aient été découverts sur trois clefs USB, elles aussi certifiées FIPS142-3 Level 2.

Dans le cas présent, après avoir ouvert une clef **MXI Stealth**, lu la mémoire 'flash' contenant les informations de l'utilisateur et analysé le logiciel Windows permettant d'accéder à cette clef, **Philippe Oechslin** a mis en évidence une erreur de conception donnant l'accès aux condensés des trois derniers mots de passe avant même que la phase d'authentification de l'utilisateur n'ait été engagée.

La seconde cible de l'analyse de sécurité est **E-Capsule PrivateSafe**, un produit commercial permettant de créer des volumes chiffrés selon une logique susceptible de répondre aux besoins d'une entreprise. Quatre mots de passe sont en effet actifs sur chaque container: un mot de passe administrateur donnant accès au container, un premier mot de passe usager donnant accès à une partie des données, un second mot de passe usager donnant accès au reste des données et enfin, un mot de passe provoquant la destruction des données lors de son utilisation. Une construction intéressante mais rapidement mise en défaut par l'analyse détaillée du contenu des deux fichiers formant un container de sécurité. Quatre blocs sont ainsi identifiés qui correspondent au stockage des paramètres associées aux quatre modes d'accès, blocs qu'il suffit d'invertir deux à deux pour aussi échanger leur rôle. Il est ainsi possible d'accéder à toutes les données en ne connaissant que le mot de passe ouvrant l'accès partiel, ou encore de provoquer la destruction des données par la présentation du code d'accès administrateur.

Le dernier produit étudié, **DataBecker Private Safe**, est ici encore un logiciel permettant la création de containers chiffrés mais n'offrant aucune des fonctionnalités avancées du précédent. Pensant bien faire, les concepteurs de ce logiciel ont mis en place un contrôle d'intégrité de la clef de déchiffrement. La simple connaissance de cet algorithme de contrôle peut faciliter une attaque en force en permettant d'éliminer les clefs non-conformes. Encore faut-il que le temps d'exécution de l'algorithme ne soit pas largement supérieur à celui d'une opération de déchiffrement. Ce sera rarement le cas, et dans le cas présent, l'algorithme utilisé donne même une information complémentaire sur la forme de la clef.

Avouons à la décharge des auteurs de ce mécanisme qu'il est parfois tentant d'engager, avant toute autre tâche, une opération de vérification préalable de la structure, et de la validité, de la clef qui sera utilisée pour déchiffrer les données du container au fil de l'eau. Le contrôle du domaine de validité d'une donnée externe, et son filtrage, est d'ailleurs l'une des règles de base d'une programmation sûre. Une règle qui souffre d'une exception dans le cas d'un élément cryptographique, élément sur lequel il sera indispensable de fournir le moins d'information possible. Le seul fait de rejeter, ici des caractères non autorisés, ou là une structure invalide, est une information en soi.

Dans le cas d'un volume de données devant être traité par le système d'exploitation, il peut être nécessaire de valider la clef afin d'éviter tout dysfonctionnement lié au chargement d'une structure de donnée invalide. Les concepteurs ont choisi une approche consistant à vérifier autant que peut se faire la structure de la clef, d'autres pourront choisir de contrôler la cohérence du déchiffrement d'un bloc témoin – offrant ainsi un critère d'arrêt fiable en cas d'attaque en force – ou encore celle du premier bloc du volume.

http://events.ccc.de/congress/2009/Fahrplan/attachments/1462_26c3_oeschlin_crypto_bugs.pdf

HOW YOU CAN BUILD AN EAVESDROPPER FOR A QUANTUM CRYPTOSYSTEM

Qin Liu, S.Sauge

Le domaine de la sécurité des systèmes d'information, et pour être honnête plus largement celui de la recherche, a cela de passionnant qu'une publication ou une découverte peut passer inaperçue puis faire la Une de la presse quelques temps après à l'occasion d'une nouvelle présentation.

Il va ainsi de la communication intitulée '**How we eavesdropped 100percent of a quantum crypto key**' publiée en août dernier à l'occasion de la conférence '**Hacking At Random 2009**'. Cette communication qui n'avait eu aucun retentissement nous avait donné l'occasion de rédiger un article permettant à chacun de comprendre les implications de l'étude menée par les cinq chercheurs de l'université Norvégienne des sciences et technologies – **NTNU** – et du centre pour les technologies quantiques de Singapour – **CQT** (Rapport N°134 – Septembre 2009).

Nous précisons à ce sujet que « *l'attaque présentée ne remettait pas en cause les fondements de la cryptographie quantique. Elle pose simplement le problème fondamental de la capacité des capteurs physiques à assurer une traduction fidèle, reproductible, mais aussi inaltérable, des informations reçues* ».

Cinq mois plus tard, alors que rien n'a changé, ni dans l'expérimentation, ni dans les conclusions, la présentation de cette même communication par la même équipe provoque cette fois un véritable raz de marée médiatique. Il faut reconnaître que le domaine abordé est complexe, et que le choix d'une conférence de faible notoriété pour une première annonce a dû rebuter plus d'un journaliste couvrant l'événement. Autre lieu, autre intitulé, autre audience et autre sensibilisation, voilà peut-être les facteurs ayant contribué à changer la donne...

Nous conseillons à nos lecteurs intéressés par cette présentation de se rapporter à notre article de septembre.

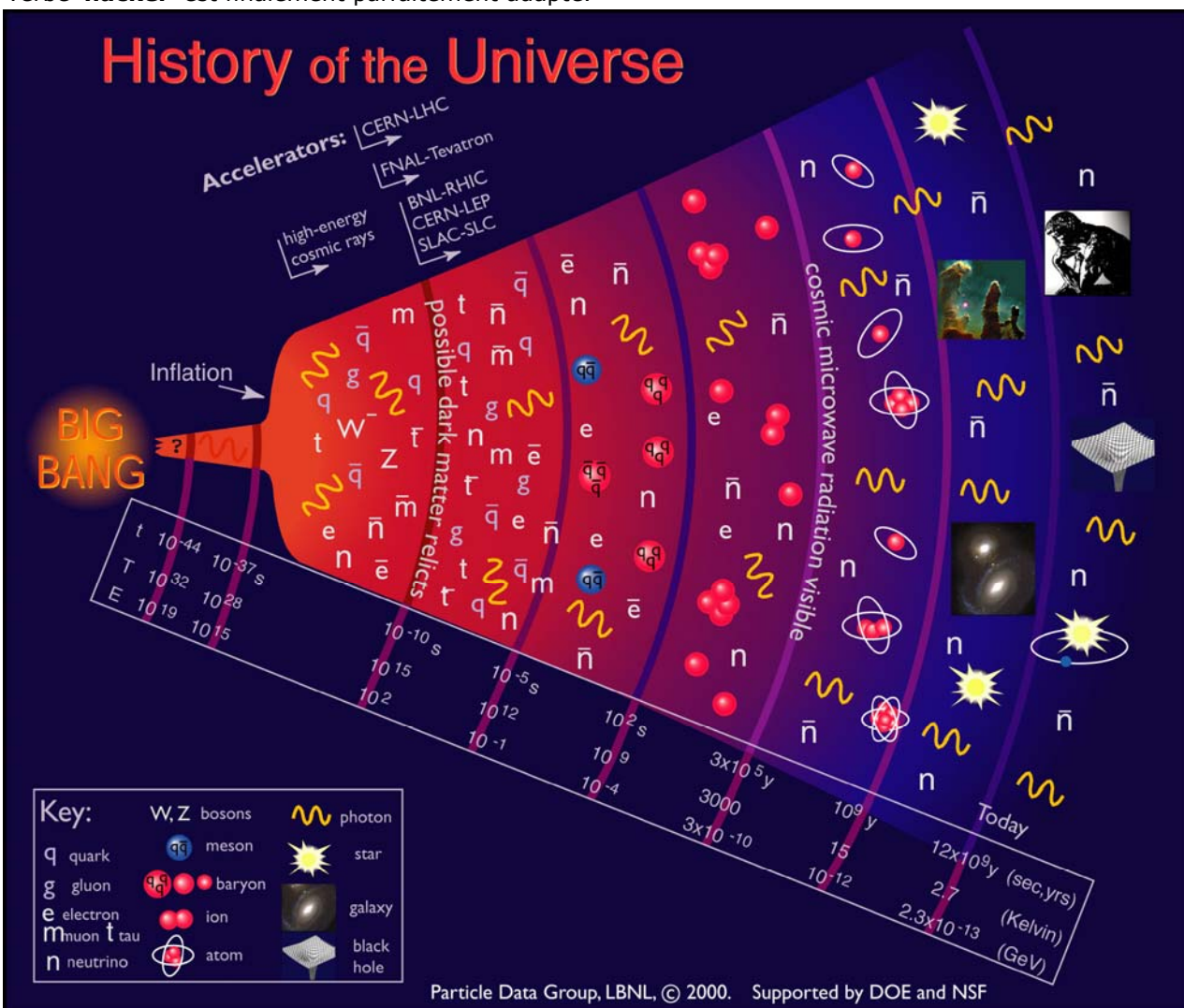
http://events.ccc.de/congress/2009/Fahrplan/attachments/1469_26C3_Sebastien_Sauge_Qin_Liu.pptx

HACKING THE UNIVERSE : WHEN STRINGS ARE SUPER AND NOT MADE OF CHARACTERS

Robert Helling

Nous devons avouer avoir été attiré par le curieux titre de cette communication, et emballé par son contenu bien que celui-ci n'ait rien à voir avec notre domaine d'intérêt. L'auteur a bien pris soin de le préciser: les chaînes dont il sera question ne sont pas faites de caractères. Un jeu de mots difficilement traduisible en français, le terme anglais 'string' signifiant à la fois la 'chaîne' de caractères manipulée par un système d'information et la 'corde' de la théorie éponyme fort à la mode dans certains milieux de la physique théorique.

Et c'est bien de ces cordes, supposées être les éléments fondateurs de notre univers, dont il est question dans cette communication. Que l'on se rassure, la théorie associée n'y fait qu'une brève apparition dans les dernières pages de la présentation (page 47, et au-delà), celle-ci étant principalement consacrée à la description de l'univers, de ses constituants, observables ou théoriques, et des outils mis à disposition des chercheurs pour ouvrir, manipuler voir modifier cette matière. Le verbe 'hacker' est finalement parfaitement adapté.



Une présentation que les curieux pourront parcourir, ne serait-ce que pour méditer sur notre destiné, aidé en cela par de magnifiques illustrations, et de superbes photos de cette 'impensable machine à remonter le temps' (par l'observation de la matière ayant existé dans premières minutes de notre univers) qu'est le **LHC Européen**.

http://events.ccc.de/congress/2009/Fahrplan/attachments/1505_universe.pdf

PRIVACY, OPENNESS, TRUST AND TRANSPARENCY ON WIKIPEDIA

HaeB

Wikipedia est une formidable source de savoir communautaire qui n'a pour seul défaut que d'être

alimentée par cette même communauté. Un modèle d'organisation fantastique sur le papier mais hélas difficile à mettre en œuvre dans une société où les intérêts de chacun priment encore sur ceux de la communauté. La mise en place de **comités d'arbitrage**, que d'aucuns pourraient considérer être des organes de censure, avec raisons dans certains cas, ne suffit pas à garantir la fiabilité et la véracité des informations publiées.

De l'avis de certains experts, le modèle d'édition libre, et sans referee, de **Wikipedia** pourrait bien provoquer son effondrement, chacun étant libre de publier, ou de modifier, un article sans avoir à justifier d'un minimum de connaissances dans le domaine traité. Cette liberté a conduit à de véritables guerres d'édition, amusantes dans la majorité des cas mais hélas dangereuses quand l'objectif est de manipuler volontairement la connaissance, qu'il s'agisse d'une volonté révisionniste ou d'une véritable campagne de désinformation.

La lutte contre de tels abus est d'autant plus difficile que le modèle ouvert de '**Wikipedia**' autorise quiconque à éditer anonymement la majorité des articles sans aucune obligation de divulgation de son identité réelle. Un travers que **Citizendium**, le concurrent de **Wikipedia**, tente de combattre avec, hélas, de grandes difficultés en étant arrivé bien plus tard, et ceci malgré la réelle qualité de son modèle d'édition qui intègre un mécanisme de vérification de l'identité.

The Citizendium, a "citizens' compendium of everything", is an open wiki project dedicated to creating a free, comprehensive, and reliable repository of structured knowledge. Our community is built on the principles of trust and respect; contributors, or "citizens", work under their own real names, and all are expected to behave professionally and responsibly. Additionally, experts are invited to play a gentle role in overseeing the structuring of knowledge.

'**HaeB**', contributeur anonyme comme il se doit avec **Wikipedia**, est investi d'un rôle opérationnel dans la structure de surveillance. Son profil de '**CheckUser**' du domaine allemand lui permet d'accéder aux seules traces que laissera un contributeur: son adresse IP. Il a pour principale mission la chasse aux '**faux-nez**', la traduction **Wikipedia** du terme anglais '**sockpuppets**', terme qui désigne les individus opérant sous plusieurs identités – comprendre ici adresses IP – pour contourner la censure ou donner plus de poids à une prise de position. Son intervention sera déclenchée à la demande, généralement à la suite du constat d'une manipulation fallacieuse sur une page.

Disposant de la chronologie, et de la teneur des manipulations effectuées sur cette page, ainsi que des adresses IP utilisées par les éditeurs, il devra déterminer si ces altérations sont le fait d'une seule et même personne physique, voire d'un groupe organisé afin de réagir en verrouillant les accès sur cette page, et si nécessaire en rétablissant le contenu original.

Dans sa présentation, '**HaeB**' détaille les méthodes employées – essentiellement d'ordre statistique – pour mener à bien l'identification d'une éventuelle manipulation: analyse de proximité géographique, mais aussi temporelle, des adresses IP utilisées, mesure de la corrélation temporelle entre différentes éditions ou encore étude du style d'écriture.

Une communication intéressante qui met en lumière la complexité de la gestion, et du maintien en condition opérationnelle, d'un système basé sur le bon vouloir d'une communauté. Une approche similaire à celle de l'Open Source. Le fond documentaire Wikipedia a le mérite d'avoir permis de constituer en quelques années seulement la Bibliothèque d'Alexandrie du 21^{ème} siècle, un savoir incommensurable mis à disposition de tous, gratuitement, et dont il faut bien en conséquence accepter les imperfections du système qui le gère. Souhaitons seulement que cette bibliothèque ci ne connaisse pas le funeste sort de son antique prédécesseur.

[http://events.ccc.de/congress/2009/Fahrplan/attachments/1504_Privacy, openness, trust and transparency on Wikipedia \(sockpuppets\).pdf](http://events.ccc.de/congress/2009/Fahrplan/attachments/1504_Privacy,_openness,_trust_and_transparency_on_Wikipedia_(sockpuppets).pdf)

OUR DARKNET AND ITS BRIGHT SPOTS

aestetix & al.

Il est des présentations capables de saper le moral des plus optimistes spécialistes d'un domaine. C'est ici le cas avec une communication traitant de la création de réseaux virtuels privés par des groupes, ou organisations, libertaires pour ne pas dire 'anarcho-autonomes'.

Ces groupes, majoritairement allemands, revendiquent la liberté de communiquer et un droit à la confidentialité absolue des échanges, une exigence incompatible avec la volonté des grands états de contrôler l'Internet.

Ce besoin de liberté s'est exprimé dans un premier temps par la création de réseaux maillés robustes et anonymes basés sur le principe d'un échange entre pairs, réseaux dits '**P2P**'. En parallèle, et pour répondre au besoin grandissant d'anonymat, se sont développés des services d'accès dédiés sous la forme de passerelles garantissant le masquage des adresses d'accès puis d'infrastructures de routage dont la plus célèbre est **TOR** (The Onion Router).

Ces approches satisfaisantes pour l'utilisateur occasionnel ne répondent cependant pas au besoin de certaines communautés qui désirent disposer d'une infrastructure offrant:

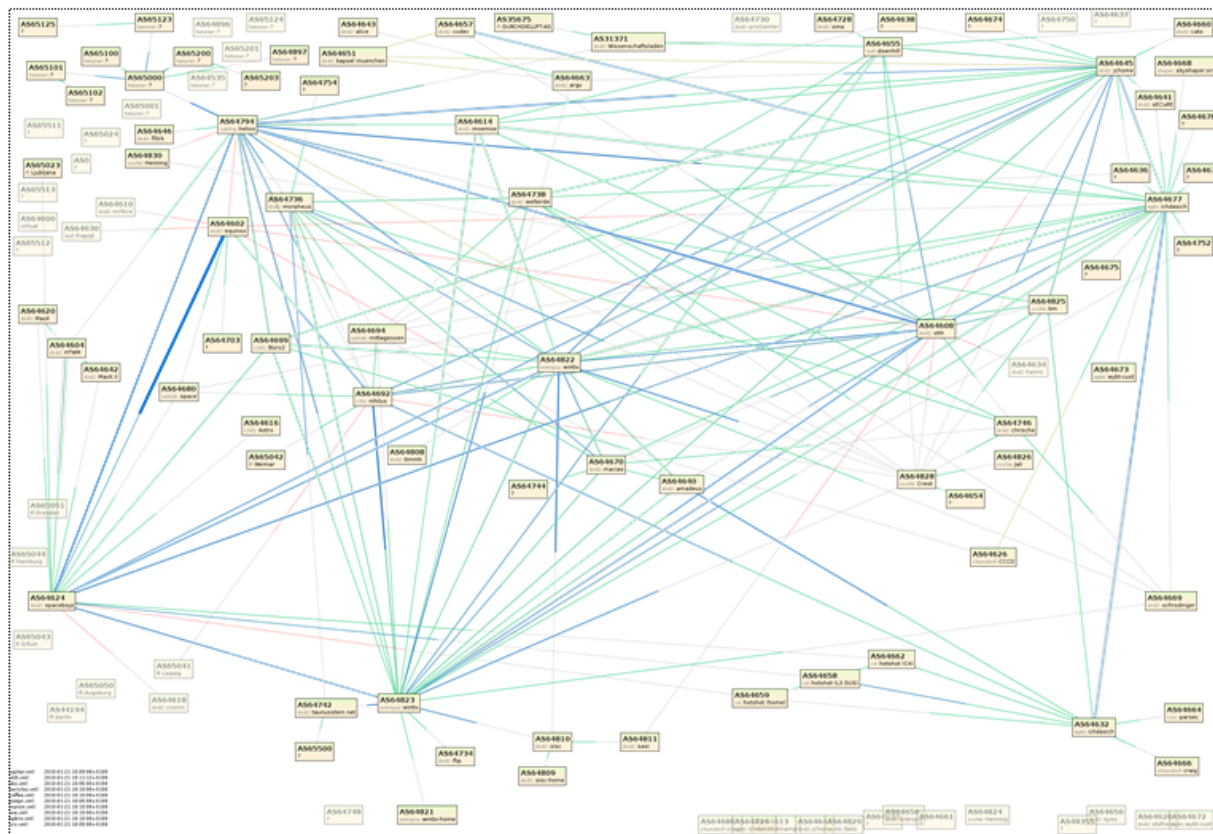
- la possibilité d'interconnecter les membres d'une même communauté,

- la possibilité de joindre n'importe quel membre tout en bloquant les accès des 'ennemis',
- une robustesse à toute épreuve,
- les meilleures performances possibles,
- la confidentialité des échanges vis-à-vis de l'extérieur,
- une administration simple et efficace.

Une gageure sauf à considérer implémenter une 'surcouche' offrant tous les services fondamentaux d'un réseau dont les nœuds seront constitués par les machines des usagers, et les liaisons point à point par des sessions IP chiffrées. De tels réseaux, correctement conçus, seront probablement très difficiles à détecter, à contrôler et encore plus à surveiller sauf à considérer pouvoir les infiltrer.

Quelques projets ont vu le jour dont les caractéristiques sont présentées dans la communication :

- le projet **dn42** (Decentralized Network) dont l'originalité est d'utiliser le protocole de routage **BGP** sur des liens d'interconnexion **OpenVPN** ou **IPSec**. Un service DNS est également disponible.



Le site d'accueil de ce projet, dont est extraite la topologie du réseau reproduite ci-dessus, liste quelques 51 domaines autonome de routage, ou **AS**, certains offrant une connectivité IPV6.

- le projet **ChaosVPN** qui, dans sa seconde version, propose un paquetage 'OpenWRT' contenant tout ce qui est nécessaire pour se connecter. Rappelons que le projet **OpenWRT** propose un firmware libre et ouvert remplaçant parfaitement celui nativement installé sur les routeurs ADSL de plusieurs constructeurs dont **Linksys**, **DLink**, **Asus**, **3Com** ou fournis par certains ISP dont **Fon** ou **Neuf**,
- le projet **FreiFunk** ayant pour objectif la construction de réseaux communautaires en s'appuyant sur des points d'accès Wifi **WRT54G** de chez **Linksys** dotés d'un firmware dédié.
- le projet **Agora** piloté par des américains mais sur lequel peu d'informations sont disponibles, le projet semblant être très récent.

Rien ne permet cependant de penser qu'il n'existe pas d'autres réseaux de ce type utilisés à des fins bien moins utopiques que celles revendiquées par ces groupes de passionnés contestataires. Le **Darknet** est probablement bien plus vaste qu'on le pense, et il sera de plus en plus difficile de cartographier ces espaces de communication et d'échange invisibles à qui ne connaît pas les bons points d'entrée ou à qui ne sait pas où chercher ces derniers...

http://events.ccc.de/congress/2009/Fahrplan/attachments/1497_darknet.pdf

GSM – SRSLY?

C.Paget, K.Nohl

La communication proposée par **Chris Paget** et **Karsten Nohl** est probablement celle qui aura le plus fait parler d'elle, et pour cause: elle présente l'état d'avancement de travaux menés sur l'algorithme de chiffrement **A5/1** utilisé pour protéger la confidentialité des conversations entre un téléphone mobile

et une station de base.

Et de fait, cette communication, fort intéressante du reste, a donné lieu à des titres délirants. Ainsi pouvait-on lire dans la presse «*la clé de chiffrement du GSM cassée*», «*L'algorithme de chiffrement GSM exposé en plein jour*», «*l'algorithme protégeant les appels GSM a été cracké*» ou encore «*algorithme A5/1 cracké: les appels GSM décryptés*», ce dernier titre ayant au moins le mérite de citer le nom de l'algorithme et d'employer le terme technique qui convient, car il s'agit bien ici de décryptage.

Beaucoup de bruit pour un résultat certes impressionnant mais attendu au regard de l'avancée des techniques de cryptanalyse d'une part, et d'interception d'autre part. Il eut été difficilement envisageable qu'un algorithme, à l'origine secret, puisse continuer d'assurer une qualité de service parfaite plus de 20 ans après sa conception.

Soyons aussi précis, si les résultats exposés prouvent qu'en effet il est désormais possible pour un amateur éclairé de déterminer la clef utilisée pour chiffrer une conversation en un temps 'raisonnable', l'environnement d'attaque disponible ne permet pas encore d'envisager pouvoir déchiffrer cette même conversation en temps réel, du moins à ce jour. Ce ne sera peut être plus le cas lorsque seront finalisés certains projets – dont le projet **OpenBTS** – ayant pour objectif la réalisation de stations de base réalisables par tout un chacun.

En 2007, le groupe de hackers **THC** – au sens premier du terme – avait engagé un impressionnant travail d'analyse portant aussi bien sur l'étude de l'algorithme de chiffrement **A5/1** ('A5Cracking Project') que sur l'infrastructure radio du réseau **GSM** et la possibilité d'intercepter les trames ('GsmScanner Project'). Les résultats de ces études ne sont hélas plus accessibles en ligne, les pages associées ayant été enlevées du Wiki du groupe. Seule [une copie du site](#) datant de la mi-2007 subsiste dans les archives Internet qui permet de se rendre encore compte de la qualité du travail accompli. En 2008, **THC** s'était engagé sur un nouvel axe de recherche dont l'objectif était de construire une table arc-en-ciel permettant d'accélérer la recherche des clefs **A5/1**, table qui n'a jamais été publiquement diffusée.

Chris Paget et Karsten Nohl ont depuis repris le flambeau en s'appuyant sur la communauté pour accélérer la construction d'une nouvelle table dont la structure a été optimisée pour une plus grande performance dans la recherche des clefs. La mise en évidence de l'existence de nouvelles structures prédictibles dans le flux des données chiffrées doit permettre de renforcer l'efficacité des attaques s'appuyant sur cette table. Une caractéristique – liée à un biais dans la conception du système de chiffrement ou dans sa mise en œuvre – qui facilite bien le travail du crypto-analyste en lui fournissant des informations bien utiles notamment pour déterminer la validité d'une clef, et un moyen d'arrêter la recherche.

		Assignment	Timing known through		
			Very early	Early	Late
Mobile terminated calls	1. Empty Ack after 'Assignment complete'	●	●	●	"Stealing bits"
	2. Empty Ack after 'Alerting'	●	●	●	
	3. 'Connect Acknowledge'	●	●	●	
	4. Idle filling on SDCCH (multiple frames)			●	
	5. System Information 5+6 (~1/sec)	●	●	●	
Network terminated calls	1. Empty Ack after 'Cipher mode complete'	●	●	●	Counting frames
	2. 'Call proceeding'	●	●	●	
	3. 'Alerting'	●	●	●	
	4. Idle filling (multiple frames)			●	"Stealing bits"
	5. 'Connect'	●	●	●	
	6. System Information 5+6 (~1/sec)	●	●	●	

Pour parer à ce problème, les opérateurs peuvent parfaitement décider d'utiliser un algorithme autre que l'algorithme **A5/1**, une facilité prévue dans la norme, et à notre connaissance utilisée un temps par certains opérateurs européens.

Encore faut-il disposer d'un algorithme de remplacement fiable et robuste pour la quinzaine d'année à venir, ce qui n'est hélas pas le cas de l'algorithme **A5/3** – nom de code **KASUMI** – spécifié par la

norme **3GPP**. Ce dernier vient en effet, hélas, d'être mis en défaut par trois grands experts du domaine dont **Adi Shamir** dans un papier intitulé '[A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony](#)'.

Une telle mésaventure confirme la nécessité de maintenir une activité de recherche et d'étude permanente dans le domaine de la cryptographie destinée à disposer d'un portfolio d'algorithmes dûment étudiés aptes à prendre la relève. Un challenge relevé par le projet Européen '**eStream**' lequel a abouti fin 2008 au référencement, et au suivi, de sept algorithmes de chiffrement prometteurs (Rapport N°135 - Octobre 2009).

http://events.ccc.de/congress/2009/Fahrplan/attachments/1479_26C3.Karsten.Nohl.GSM.pdf

POUR PLUS D'INFORMATION

<http://events.ccc.de/congress/2009/Fahrplan/>

LOGICIELS

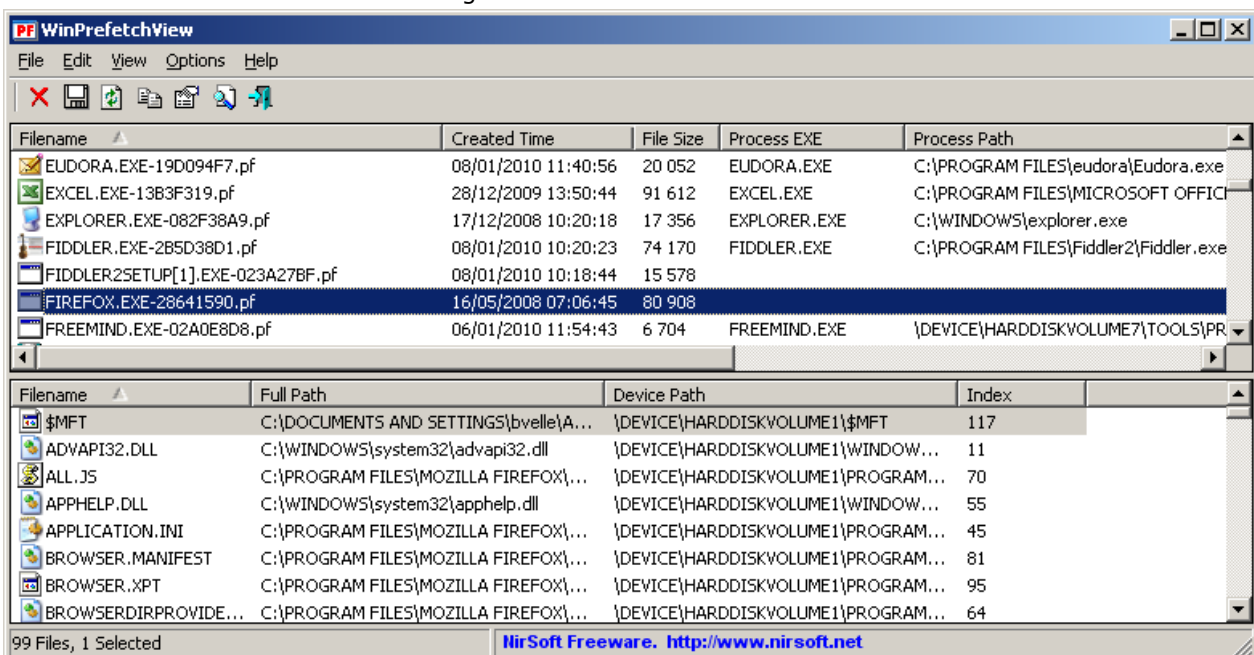
NIRSOFT - WINPREFETCHVIEW

NirSoft Nir Sofer nous propose un nouvel outil d'aide à l'administration et à l'exploitation d'un système Windows.

Cet outil, '**WinPrefetchView**', vient compléter l'impressionnant catalogue d'outils de visualisation, ou '**Viewers**', proposés par ce développeur génial et prolifique. Il permet d'explorer un mécanisme peu connu du système Windows, à savoir le cache des applications. Celui-ci permet d'accélérer l'accès aux applications les plus utilisées en chargeant les ressources – principalement des bibliothèques dynamiques – chargées par ces applications. Les informations requises par ce mécanisme de cache sont stockées dans un dossier spécifique dit '**Prefetch**' (préchargement) dont la taille sera limitée à 128 entrées.

Le comportement de ce mécanisme est dicté par divers paramètres stockés dans la base de registre sous la clef '**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters**' dont la clef '**EnablePrefetcher**'. Celle-ci permet de – désactiver le mécanisme (valeur 0), d'activer celui-ci pour les applications uniquement (1), pour le démarrage uniquement (2) ou dans tous les cas (3), option positionnée par défaut.

S'il est couramment admis que la destruction du contenu n'améliorera pas les performances du système, une telle opération permettra d'éliminer toute trace d'utilisation d'applications obsolètes, ou localisées sur un support externe. Une opération qui peut s'avérer nécessaire pour masquer l'usage de certains outils de sécurité et de confidentialité, tel par exemple **TrueCrypt**. La désactivation temporaire de cette fonction pourra même être envisagée dans certains cas – portable en transit – en admettant un léger ralentissement du système. Il va alors de soi que d'autres précautions devront être prises dont le nettoyage de la base de registre, la désactivation du fichier d'hibernation, des historiques, et le nettoyage des zones libres des volumes de stockage.



L'utilitaire développé par **Nir Sofer** permet de visualiser toutes les informations maintenues dans le cache du mécanisme de pré-chargement. Il n'offre cependant aucune option permettant de détruire, sélectivement ou globalement, les entrées enregistrées. Une fonction qui, à notre connaissance, n'est proposée par aucun outil de nettoyage ou d'analyse.

Il faudra alors procéder manuellement, en s'appuyant sur les informations fournies par '**WinPrefetchView**' pour identifier les fichiers présents sous le répertoire '%SystemRoot%\Prefetch' qu'il conviendra de détruire.

Nir Sofer nous propose ici un outil de très faible encombrement (moins de 42Ko) qui, couplé avec la dernière version de **Process Explorer** de Microsoft **Sysinternals**, s'avérera fort utile pour l'utilisateur averti, l'exploitant ou l'analyste.

POUR PLUS D'INFORMATION

- http://www.nirsoft.net/utills/win_prefetch_view.html
- <http://en.wikipedia.org/wiki/Prefetcher>

MAGAZINES

ENISA - QUARTERLY REVIEW



Ce dernier numéro de l'année 2009 est aussi le premier numéro édité sous le mandat du nouveau directeur de l'**ENISA**, **Udo Helmbrecht**. Pour son premier éditorial, ce dernier nous dévoile les grands axes de travail de l'agence dont il souligne qu'elle doit être un 'stimulateur' - le terme 'pacemaker' est employé - pour l'ensemble des parties prenantes dans le domaine de la sécurité des systèmes d'information en Europe. Il fait remarquer à ce propos que certains pays membres ne disposent pas encore d'une équipe gouvernementale chargée de la gestion des incidents de sécurité et rappelle que l'**ENISA** peut accompagner ceux-ci dans la mise en place d'un **CERT**. L'**ENISA** va devoir prouver qu'elle n'est pas simplement une agence 'placebo' comme cela a été dit mais bien une organisation reconnue pour son savoir-faire propre dans le domaine de l'accompagnement et du conseil aux pays membres. Un changement qui semble avoir déjà été amorcé au regard du nombre des publications mises à disposition ces dernières semaines.

Dans ce nouveau numéro de la revue de l'**ENISA**, 4 thèmes sont donc abordés:

RESILIENCE, NOTIFICATION D'INCIDENT ET EXERCICES

Ce thème de la résilience d'un système, qu'il s'agisse d'un réseau, d'un système informatique, ou plus largement d'un système d'information est abordé par le biais d'un intéressant article de Paul Théron - Thalès - intitulé '**Measuring Resilience - The Next Challenge**'. Car en effet s'il est assez aisé de définir ce qu'est la résilience d'un système - son aptitude à maintenir ses capacités opérationnelles intactes dans une situation de crise - le problème de l'évaluation de cette résilience reste entier, du moins dans le domaine qui nous intéresse ici. L'auteur considère qu'il convient d'aborder ce sujet selon trois axes distincts:

- 1- l'évaluation de l'aptitude du système à se maintenir durant un état de crise, à résister à la destruction et à revenir à l'état opérationnel en fin de crise, conduisant à la définition d'une classique échelle de résistance,
- 2- l'évaluation de la capacité de l'organisation à gérer la crise en s'appuyant par exemple sur un indicateur mesurant le niveau de préparation de cette organisation dans différents domaines pertinents,
- 3- la quantification précise de la robustesse attendue du système cible pour que celui-ci réponde aux objectifs de l'organisation.

L'auteur fait remarquer la norme **ISO/PAS 22399:2007 'Societal security - Guideline for incident preparedness and operational continuity management'**, et la définition de la capacité opérationnelle à répondre aux incidents, ou '**incident preparedness**' qu'elle propose, devrait permettre d'avancer sur le problème de la définition du niveau de résilience attendu d'un système.

L'article suivant, proposé par des experts attachés à l'**ENISA**, présente le guide '**Good Practice Guide on National Incident Reporting Schemes**' qui vient d'être publié. Après un bref rappel du contexte politique ayant conduit à la réalisation de ce guide, les auteurs détaillent les éléments qui ont dû être pris en compte pour l'établissement des schémas de systèmes de notification nationaux, et en particulier:

- 1- le rôle attendu du système de notification: un système de notification peut répondre à trois besoins spécifiques et donc conduire à l'établissement de schémas spécifiques: prévention, réponse à un incident ou encore correction d'un problème.

- 2- les types d'incidents: deux typologies d'incident ont été prises en compte dans l'établissement du guide, les incidents réseaux et les incidents de sécurité sur les données,
- 3- l'organisation de rattachement: celle-ci peut être une autorité de régulation des télécommunications, une autorité chargée de la protection des infrastructures vitales, un CERT gouvernemental ou tout CERT ayant une couverture nationale.

<http://www.enisa.europa.eu/media/news-items/incident-reporting>

Ces mêmes experts ont rédigé l'article suivant intitulé '**Good Practice Guide on National Exercises**'. Celui-ci met l'accent sur la nécessité d'entraîner régulièrement les équipes d'une structure de réponse aux incidents par le biais d'exercices représentatifs des problèmes susceptibles d'être rencontrés sur le terrain. C'est par ce biais que les équipes pourront roder leur mode de fonctionnement, acquérir les bons réflexes sans autres risques que d'exposer en comité restreint ses faiblesses et erreurs, et tout honte bue, d'améliorer leurs procédures.

Les auteurs rappellent que de tels exercices sont régulièrement menés par les plus hautes instances Européennes et par certains états membres: récemment en Irlande avec un exercice regroupant plusieurs opérateurs de réseaux de télécommunication, en 2008 en Norvège avec l'exercice ICT08 conduit par le DBS (Directorate for Civil Protection and Emergency Planning), aux Pays-Bas dans le cadre des exercices 'Waterproef' simulant l'inondation du pays. L'exercice le plus médiatique restera cependant certainement '**CyberStorm**', un exercice conduit en 2006 puis en 2008 par le département de la sécurité intérieure américain. L'**ENISA** recommande que de tels exercices soient régulièrement mis en œuvre au niveau national par les états membres tout en reconnaissant que la tâche est complexe et ardue. Celle-ci devrait être facilitée par la publication d'un guide dédié élaboré par l'**ENISA** sur la base du retour d'expérience acquis à l'occasion des deux exercices pilotes menés en 2009. Ce guide pourra être complété par le kit d'entraînement publié dernièrement lequel comporte un manuel d'exercice ('**CERT Exercice toolset**'), un corrigé type ('**CERT Exercice Handbook**') et autres informations utiles (Rapport N°137 – Décembre 2009).

<http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises>

Le dernier article de ce volet présente les premiers résultats des travaux d'un groupe de travail virtuel – **VWG** ou Virtual Working Group - créé en Mai 2009 sur le thème des mesures prises, ou susceptibles d'être prises, par les opérateurs des réseaux de communication européens pour renforcer la résilience de leurs infrastructures. En 2008, une enquête menée par l'**ENISA** avait mis en évidence la réticence des opérateurs à aborder ce sujet en soulignant l'immaturité des nouveaux entrants sur ce marché ce qui a conduit à la création du groupe de travail 'Network Providers Measures'. Celui-ci regroupe des représentants de 11 opérateurs européens: **FT-Orange** pour la France, **Telefonica O2** et **BT** pour le Royaume-Unis, **Telecom Italia** pour l'Italie, **Telefonica** pour l'Espagne, **KPN** pour les Pays-Bas, **SwissCom** pour la Suisse, **Vodafone** et **ForthNet** pour la Grèce, **SC Romtelecom SA** pour la Roumanie et **Interoute** pour la république Tchèque.

<http://www.enisa.europa.eu/act/res/providersmeasures/>

SENSIBILISATION

Le directeur général de l'Institut National des Technologies de COmmunication espagnol – INTECO – introduit le thème de la sensibilisation par le biais d'un article intitulé '**OSI: A Security Helpdesk for Internet Users in Spain**'. Le taux de pénétration de l'Internet, et des technologies associées, en Espagne a conduit les instances nationales, dont le ministère de l'industrie, du tourisme et du commerce, à engager plusieurs initiatives dans le domaine de la sécurité et de la sensibilisation. La plus récente est la création d'un service public d'information et d'aide au citoyen, dit 'Oficina de Seguridad del Internauta' ou **OSI**. Cette structure est ouverte tous les jours de 9h à 19h, et de 9h à 14h les samedis. Elle offre deux niveaux de services: un centre d'accueil téléphonique s'adossant à une équipe de support de premier niveau permet de répondre aux questions posées par les Internaute. Un deuxième niveau de support est en charge du traitement des problèmes plus complexes dont notamment la gestion des incidents de sécurité. Ce sont au total quelques 21 personnes qui assurent le fonctionnement au quotidien de ce service qui traite 500 appels téléphoniques par jour: 16 techniciens au premier niveau de support et 4 experts au second niveau. Le portail WEB, accessible en castillan, catalan et basque, reçoit quelques 40000 visites quotidiennes.

Les appels à cette structure se décomposent comme suit: 27% pour un problème avec un programme ou avec le système d'exploitation, 26% pour une question en rapport avec la sécurité, 21% pour un problème de sécurité, 18% pour un problème relatif à la connexion Internet et 8% pour un problème relatif à un mail suspect.

<http://www.osi.es>

Le second article nous présente l'approche retenue au Japon par l'agence pour la promotion des technologies de l'information, Information-technology Promotion Agency ou **IPA**. La sensibilisation des citoyens passe ici prioritairement par la réalisation de brochures d'information et l'animation de formations à la sécurité à travers le pays. Trois catégories de formation permettent de s'adapter à la

population cible: l'individu avec une formation aux fondamentaux de la sécurité lui permettant d'acquérir les bases de la sécurité, de comprendre les menaces et de mettre en place les mesures de protection élémentaires; le manager avec une formation ciblée sur les mesures organisationnelles et le technicien avec une formation à deux niveaux. Le niveau standard permet d'acquérir la connaissance des menaces et des contre-mesures possibles, le niveau professionnel allant plus en profondeur pour s'intéresser à la mise en œuvre des mesures de sécurisation. Une check-list de 25 points de contrôle a par ailleurs été établie pour aider les petites et moyennes entreprises à mieux qualifier leur niveau de protection.

<http://www.ipa.go.jp/index-e.html>

Le dernier article est proposé par trois hauts responsables de l'agence Coréenne pour la sécurité et l'internet, la **KISA** (Korea Internet & Security Agency). Cette agence, qui a vu le jour en juillet 2009, résulte du regroupement de trois structures nationales: la **Korea Information Security Agency** (KISA), la **National Internet Development Agency** (NIDA) et la **Korea IT International Cooperation Agency** (KIICA), une réorganisation qui coïncide avec les vagues d'attaque en déni de service ayant touché la Corée du Sud, en ce même mois de juillet 2009. L'article présente l'état d'avancement des actions de sensibilisation et de renforcement de la sécurité des systèmes d'information inscrites au titre du plan de sécurisation de l'Internet établi en 2008.

http://www.kisa.or.kr/new/eng/english_ver.html

INTEROPERABILITE ET PROTECTION

L'article 'Cloud Computing - Benefits, Risks and Recommendations for Information Security' proposé par deux experts de l'ENISA présente le rapport 'Cloud Computing Security Risk Assessment' publié dernièrement par l'ENISA (Rapport N°136 – Novembre 2009).

<http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment>

Les auteurs annoncent la prochaine de tenue de 'SecureCloud2010', une conférence consacrée à ce sujet organisée par l'ENISA. Celle-ci se tiendra du 10 au 17 mars prochain à Barcelone. Un appel à contribution est ouvert.

<http://securecloud2010.eventbrite.com/>

Le second article de ce volet traite de la signature électronique et de l'harmonisation de son application à travers l'Europe. Les auteurs mettent l'accent sur la nécessité d'accélérer le travail engagé il y a maintenant plus de dix ans et suggèrent de suivre les six recommandations émises par le projet 'WeSIGN', un projet soutenu par la commission européenne et menés par les chambres de commerce de 9 pays membres.

<http://www.wesign.org/>

ISMS

Leopold Koppensteiner et **Markus Kloibhofer**, tous deux du **Ministère des finances autrichien** (Bundesministerium für Finanzen ou **BMF**), propose de partager leur retour d'expérience sur la mise en place d'un **ISMS** – Système de gestion de la Sécurité de l'Information – au sein de leur ministère. Le premier système installé en 2002 a fait l'objet d'une évolution en 2007 pour le rendre compatible avec les exigences définies par la norme ISO/IEC 27001:2005. Un travail de fond récompensé par la certification obtenue en 2008, la première en Europe pour un ministère.

<http://www.cis-cert.com/veranstaltungen/symposium09/presentation/Pleskac2009.pdf>

Le dernier article détaille la démarche d'analyse de risque menée par l'**ISPESL** - Italian Institute for Occupational Safety and Prevention – dans l'optique d'obtenir sur 2010 la certification ISO/IEC 27001 de son centre de traitement des données. Cette démarche s'est appuyée sur la méthodologie **MAGERIT** (Methodology for Information Systems Risk Analysis and Management) dont la première version a été développée en 1997 par le **CSAE**, le conseil supérieur de l'administration électronique espagnol. Le questionnaire développé par le **CNIPA** Italien (Centro Nazionale per l'Informatica nella Pubblica Amministrazione) – 36 questions mesurant 4 indicateurs de performance – a aussi été utilisé mais les auteurs soulignent que l'utilisation de nombreuses questions binaires ne permet pas d'évaluer réellement l'efficacité des mesures. La seconde version de la méthodologie **MAGERIT** est accessible en langue anglaise sur le site du CSAE:

Livre I: **la méthode** (140 pages)

Livre II: **le catalogue des éléments** (87 pages)

Livre III: **les techniques** (30 pages)

Les questions du **CNIPA** pourront être trouvées dans le rapport d'enquête intitulé '**Primo Rapporto Sullo Stato Della Sicurezza Ict Delle Pac**' publié en 2006 présentant l'état de la sécurité des systèmes d'information publics.

http://www.cnipa.gov.it/site/_files/Cnipa_rapporto_sicurezza_cop.pdf

POUR PLUS D'INFORMATION

<http://www.enisa.europa.eu/publications/eqr/issues/eqr-q3-2009-vol.-5-no.-4>

METHODOLOGIES ET STANDARDS

METHODES

MITRE – MAEC MALWARE ATTRIBUTE ENUMERATION AND CHARACTERIZATION



Le MITRE vient d'annoncer le lancement d'une initiative ayant pour objectif de faciliter la caractérisation d'un quelconque code malveillant en levant toutes les ambiguïtés liées à la difficulté de décrire, dans un langage non adapté, un composant autonome complexe.

Pour ce faire, le MITRE a conçu **MAEC** (Malware Attribute Enumeration & Characterization), un langage formel de description prenant en compte les caractéristiques statiques mais aussi dynamiques d'un code.

La première version des spécifications de ce langage devrait voir le jour durant le second semestre de l'année mais les principes généraux de **MAEC** sont d'ores et déjà décrits sur le portail géré par le MITRE et dédié à ce projet.

Le langage MAEC, ou être plus précis, le système de description MAEC s'appuie sur trois composants:

1- Un vocabulaire énuméré et fini, dit 'MAEC **enumeration**', qui contient tous les éléments permettant de décrire le code malveillant à travers

l'observation de son comportement et des actions engagées. Cette taxonomie sera déclinée sur trois niveaux d'abstraction correspondant à trois formes de description:

- . une description élémentaire des attributs fondamentaux du code qu'ils soient observables – manipulation directe du système hôte – ou inférés – instructions spécifiques extraites par désassemblage du code,
- . une description intermédiaire permettant d'organiser les descriptions élémentaires pour décrire des comportements caractéristiques déterminant les objectifs du code – création d'une copie de son propre code par exemple, ou encore exécution du code au démarrage du système,
- . une description générale destinée à organiser les comportements caractéristiques précédents en des mécanismes génériques, un mécanisme de persistance par exemple.

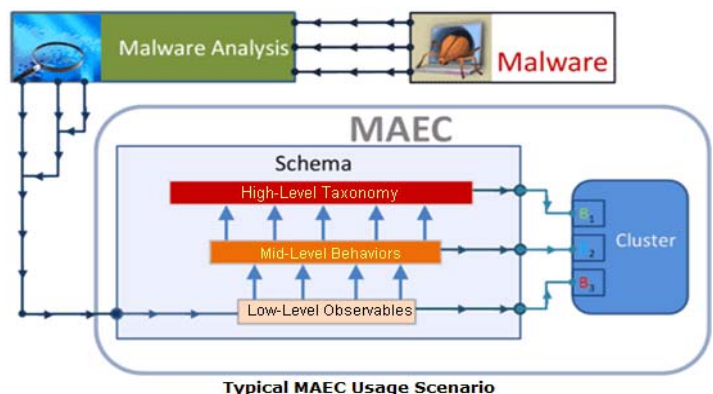
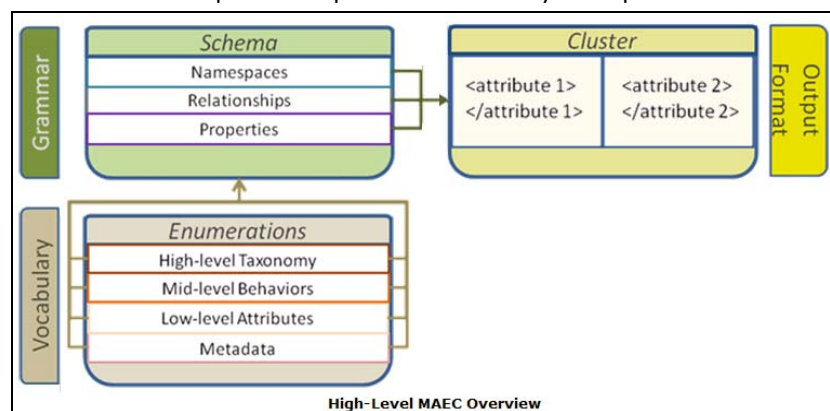
Le MITRE précise que ce niveau de description ne sera pas spécifié avant que les vocabulaires des niveaux précédents aient été totalement validés.

2- Une grammaire, dite 'MAEC **schema**', permettant d'assembler le vocabulaire précédent pour former une description complète et non ambiguë d'un composant.

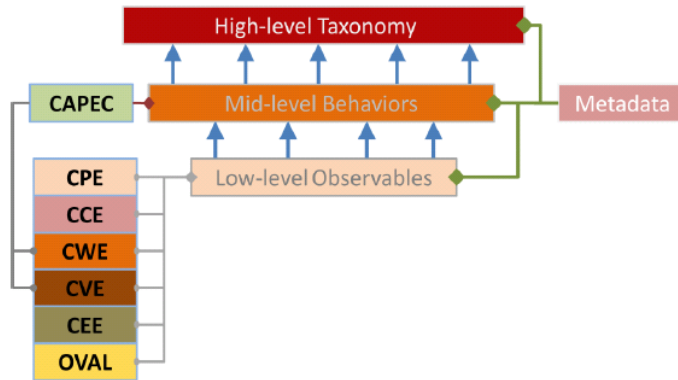
Trois éléments autorisent cet assemblage:

- . un schéma de nommage, dit '**namespace**', qui permet de regrouper les énumérations en des classes spécifiques,
- . un ensemble de règles, ou **relationships**, qui régissent les relations entre ces mêmes classes,
- . un ensemble de propriétés, ou **property**, qui permettront de caractériser les instances de ces classes.

3- Un format de présentation, ou **cluster**, qui déterminera la présentation d'une instance d'un code malveillant. Le format XML sera initialement utilisé.



Deux documents sont disponibles sur le site du MITRE. Le premier (20 pages), intitulé 'Malware Attribute Enumeration and Characterization Concept Document', propose une introduction à **MAEC** et livre quelques



POUR PLUS D'INFORMATION

- <http://maec.mitre.org/about/index.html>
- http://maec.mitre.org/about/docs/The_MAEC_Concept.pdf
- http://maec.mitre.org/about/docs/MAEC_SCAP_10_2009_briefing.pdf

exemples d'application pratiques. Il précise le positionnement relatif des différents outils mis à disposition par le **MITRE**.

Nous recommandons particulièrement la lecture de cette introduction.

Le second document, qui est intitulé 'Malware Attribute Enumeration and Characterization SCAP Presentation', contient la présentation de cette initiative engagée en octobre dernier dans le cadre de la 5^{ème} conférence **IT Security Content Automation**.

RECOMMANDATIONS

NIST - SP800-131 'RECOMMENDATION FOR THE TRANSITIONING OF CRYPTOGRAPHIC ALGORITHMS AND KEY SIZES'



Une version préliminaire du guide **SP800-131 'Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes'** vient d'être publiée.

Avec ce guide, le **NIST** récapitule les exigences applicables à la validation des algorithmes de sécurité, ou relatif à la sécurité, par lui normalisés: algorithme de chiffrement (**SP800-67**, **FIPS185**, **FIPS197**), schéma de signature (**FIPS186-V3**), génération de séquences pseudo-aléatoires (**SP800-90**), mise à la clef (**SP800-56A**), mécanisme d'échange et de transport de clef (**SP800-56B**)...

En ce qui concerne les algorithmes de chiffrement, le guide **SP800-131** précise que les implémentations des algorithmes **SKIPJACK**, et **Two-Keys 3DES** (chiffrement sous la clef 1, déchiffrement sous la clef 2 et sur-chiffrement sous la clef 1 soit $C=E_{k1}[D_{k2}[E_{k1}[M]]]$) ne feront plus l'objet d'aucune certification après 2010. Cette restriction n'impacte pas les implémentations des algorithmes **Three-Keys 3DES** (chiffrement sous la clef 1, déchiffrement sous la clef 2 et sur-chiffrement sous la clef 3 soit $C=E_{k3}[D_{k2}[E_{k1}[M]]]$) et **AES-128**, **AES-192**, **AES-256** lesquels continueront d'être supportés dans les années à venir sans qu'aucune durée de vie ne soit dépendant précisée.

La dernière mise à jour, le guide **FIPS-186 'Digital Signature Standard'** (WISec #25 - Juin 2009) a reconduit l'approbation des algorithmes de signature **DSA** et **RSA** en autorisant l'usage de l'algorithme **ECDSA** mais en imposant quelques contraintes sur le niveau de sécurité des signatures lequel devra passer de 80 bits à 112 bits.

Rappelons à ce propos qu'en algorithmique asymétrique, le niveau de sécurité offert pour une taille de clef donnée est dépendant de l'algorithme utilisé. Afin d'éviter toute confusion, ce niveau de sécurité sera défini par la taille que devra avoir la clef d'un algorithme symétrique pour obtenir le même niveau de sécurité. Ainsi, un niveau de sécurité de 80 bits signifiera qu'il sera nécessaire de disposer d'au plus 2^{80} signatures pour recouvrir la clef privée. Un tel niveau de sécurité pourra être atteint avec un algorithme de chiffrement symétrique utilisant une clef de 80 bits ou encore en utilisant l'algorithme **DSA** avec une taille de clef publique de 1024 bits.

Le **SP800-131** détaille ainsi les contraintes applicables à la validation des implémentations assurant la génération, mais aussi la vérification, des signatures durant la période de transition autorisée pour la mise en conformité avec la version 3 des spécifications FIPS-186, laquelle prend fin au 31 décembre 2010. A la fin de cette période, ne seront validées que les implémentations autorisant la génération de signatures d'un niveau de sécurité supérieur ou égal à 112bits, la vérification des signatures générées antérieurement devant être toujours assurée.

L'annexe A regroupe les tables des niveaux de sécurité offerts par les différents algorithmes, et la taille des clefs requise pour atteindre ce niveau de sécurité. Les conditions d'établissement de ces tables d'équivalence diffèrent légèrement de celles retenues par les experts, membres du réseau d'excellence européen **eCrypt**, dans leur recommandation annuelle sur la taille des clefs (Rapport N°134 - Septembre 2009).

Le sommaire de ce guide de 22 pages est le suivant:

- 1 **Introduction**

- 1.1 Background and Purpose
- 1.2 Useful Terms for Understanding this Recommendation
 - 1.2.1 Testing and Validation
 - 1.2.2 FIPS Mode
 - 1.2.3 Approved vs. Allowed
 - 1.2.4 New Validations and Already Validated Implementations
 - 1.2.5 Security Strengths
- 2 **Encryption**
- 3 **Digital Signatures**
 - 3.1 Transition from **FIPS 186-2** to **FIPS 186-3**
 - 3.2 Security Strengths for Digital Signature Keys
- 4 **Random Number Generation**
- 5 **Key Agreement Using Diffie-Hellman and MQV**
 - 5.1 Key Agreement Schemes Specified in **SP 800-56A**
 - 5.2 Key Agreement in Protocols that are Not Fully Compliant with **SP 800-56A**
- 6 **Key Agreement and Key Transport Using RSA**
- 7 **Key Wrapping**
- 8 **Deriving Additional Keys from a Cryptographic Key**
- 9 **Hash Functions**
- 10 **Message Authentication Codes (MACs)**
 - Appendix A:**
 - A.1 Comparable Algorithm Key Size Strengths
 - A.2 Hash Function Security Strengths for Cryptographic Applications
 - A.3 Recommended Algorithms and Minimum Key Sizes
 - A.4 FFC Parameter Size Sets
 - A.5 ECC Parameter Size Sets
 - Appendix B: References**

POUR PLUS D'INFORMATION

http://csrc.nist.gov/publications/drafts/800-131/draft-800-131_transition-paper.pdf

STANDARDS

RFC5735 / SPECIAL USE IPV4 ADDRESSES

Le **RFC 5735** annule et remplace le **RFC 3330 'Special use IP V4 addresses'** publié par l'**ICANN** en septembre 2002. Il a pour objet la documentation de la vingtaine de blocs d'adresses IPV4 ayant un rôle particulier dans le plan d'adressage de l'Internet. On retrouve dans cette liste les adresses non routables, permettant à un réseau ou à un système de s'auto-référencer (0.0.0.0/8 et 127.0.0.0/8) et les blocs d'adresses non routables réservés aux réseaux privés, blocs spécifiés par le célèbre RFC1918 (10.0.0.0/8, 172.17.0.0/16 et 192.168.0.0/16).

Cette liste est reproduite ci-dessous en précisant les modifications apportées au **RFC3330**: sur fond noir les blocs libérés, et sur fond jaune, les nouveaux blocs réservés.

0.0.0.0/8	"This" Network	RFC1700	
10.0.0.0/8	Private Use Networks	RFC1918	
14.0.0.0/8	Public Data Networks	RFC1700	Libéré
24.0.0.0/8	Cable Television Networks		Libéré
39.0.0.0/8	Reserved but subject to allocation	RFC1797	Libéré
127.0.0.0/8	Loopback	RFC1700	
128.0.0.0/16	Reserved but subject to allocation		Libéré
169.254.0.0/16	Link Local		
172.16.0.0/12	Private Use Networks	RFC1918	
191.255.0.0/16	Reserved but subject to allocation		Libéré
192.0.0.0/24	IETF Protocol Assignments	RFC5736	Réaffecté
192.0.2.0/24	TEST-NET-1	RFC5737	Réservé documentation
192.88.99.0/24	6to4 Relay Anycast	RFC3068	
192.168.0.0/16	Private-Use Networks	RFC1918	
198.18.0.0/15	Network Interconnect Device Benchmark Testing	RFC2544	
198.51.100.0/24	TEST-NET-2	RFC5737	Réservé documentation
203.0.113.0/24	TEST-NET-3	RFC5737	Réservé documentation
223.255.255.0/24	Reserved but subject to allocation		Libéré
224.0.0.0/4	Multicast	RFC3171	
240.0.0.0/4	Reserved for Future Use	RFC1700	
255.255.255.255/32	Limited Broadcast	RC919	

Trois blocs de classe C sont désormais réservés à l'usage de la documentation: les adresses associées,

non routées, pourront être référencées sans risques dans les exemples de configuration figurant dans les guides et manuels. Rappelons à ce propos, que le réseau '1.0.0.0/8' si souvent employé à cette fin – qui n'a jamais employé l'adresse '1.2.3.4' dans une documentation – vient d'être alloué à la zone Asie Pacifique gérée par l'APNIC. Le **RFC5737 'IPv4 Address Blocks Reserved for Documentation'** détaille les conditions d'utilisation de ces adresses.

L'usage d'un autre bloc de classe C jusqu'alors réservé sans attribution précise est désormais détaillé. Les adresses du bloc 192.0.0.0/24 pourront être attribuées par l'IANA pour certains protocoles, sur demande particulière et en conformité à la procédure décrite dans le **RFC5736 'IANA IPv4 Special Purpose Address Registry'**.

Enfin, cinq blocs, dont trois blocs de classe A, ont été reversés aux Registres Internet Régionaux, les **RIR** ou Regional Internet Registries, pour être alloués à de nouveaux usagers. Le problème de l'épuisement des adresses **IP V4** reste cependant entier: la dernière analyse du **NRO** (Number Resource Organization), l'organisation constitué des quatre **RIR** les plus importants (**APNIC, ARIN, LACNIC** et **RIPE CC**), laisse ainsi entendre que les blocs reversés seront épuisés dès septembre 2011.

are::you:IPv6:ready? Les blocs encore disponibles chez les **RIR** seront tous épuisés quelques mois plus tard. Fin 2012, les nouveaux équipements et services seront tous tenus d'utiliser l'adressage V6.

En attendant cette échéance proche, les exploitants et les ISP vont devoir faire rapidement face à un problème tout aussi important: la diffusion progressive de zones sécurisées **DNSSEC** par les serveurs racine. En juillet 2010, les treize serveurs DNS racines transmettront des enregistrements DNSSEC dont la taille dépassera largement la longueur usuellement traitée de 512 octets.

Comme le fait remarquer Stéphane Borzmeyer, de l'AFNIC, **les réseaux qui rejettent les paquets DNS de plus de 512 octets, ou même seulement ceux de plus de 1500 octets, ne pourront plus parler à la racine du DNS après juillet 2010 (puisque'ils ne recevront plus les réponses) et n'auront donc quasiment plus d'accès Internet en pratique.** Les quelques mois à venir vont donc devoir être mis à profit pour qualifier la capacité des serveurs DNS, et des équipements réseaux, et le cas échéant, migrer ceux-ci vers une version compatible avec les exigences **EDNS**.

L'AFNIC vient d'annoncer à ce propos qu'elle a placé de nouveaux serveurs **DNS** à plusieurs endroits en **France** (notamment à Lyon) et en **Europe** afin d'améliorer l'accessibilité du service **DNS** mais aussi d'offrir une meilleure résistance aux attaques par saturation. La technologie '**Anycast**' est utilisée à cette fin (Rapport N°126 – Mai 2008).

Le sommaire de cette spécification de 11 pages est le suivant:

1. **Introduction**
2. **Terminology**
3. **Global and Other Specialized Address Blocks**
4. **Summary Table**
5. **Assignments of IPv4 Blocks for New Specialized Uses**
6. **IANA Considerations**
7. **Security Considerations**
8. **Acknowledgments**
9. **References**
 - 9.1. Normative References
 - 9.2. Informative References
- Appendix A. Differences between This Document and **RFC 3330**

POUR PLUS D'INFORMATION

- <ftp://ftp.ietf.org/rfc/rfc5735.txt>
- <ftp://ftp.ietf.org/rfc/rfc5736.txt>
- <http://www.nro.net/media/less-than-10-percent-ipv4-addresses-remain-unallocated.html>
- <http://www.mail-archive.com/frnog@frnog.org/msg08914.html>
- <http://www.afnic.fr/actu/nouvelles/238/l-afnic-deploie-son-propre-nuage-anycast>

TABLEAUX DE SYNTHÈSE

CONFERENCES

CCC - 26 CHAOS COMMUNICATION CONGRESS



LA 26^{ème} édition de la célèbre conférence technique organisée par le **Chaos Computer Club - CCC** - allemand s'est tenue durant les derniers jours de l'année 2009, du 27 au 30 décembre, à Berlin. Le thème général de cette année était celui des territoires dangereux désignés par l'expression anglo-saxonne **'Here be dragons'**.

Ce seront quelques 72 communications, organisées autour de six thèmes, qui auront été présentées sur ces 4 jours.

Hacking	
"Yes We Can't!" - O kleptography and cryptovirology	Moti Yung
A part time scientists' perspective of getting to the moon	Reiners & al.
Advanced microcontroller programming: Getting deeper into AVR programming	wesen
Black Ops Of PKI	Dan Kaminsky
Blackbox JTAG Reverse Engineering	Felix Domke
Building a Debugger: Open JTAG with Voltage Glitching	Travis Goodspeed
cat /proc/sys/net/ipv4/fuckups	Fabian Yamaguchi
coreboot: Adding support for a system near you	Peter Stuge
DECT: What has changed in DECT security after one year	Erik Tews
Defending the Poor: Preventing Flash Exploits	FX of Phenoelit
Exposing Crypto Bugs through reverse engineering	Philippe Oechslin
Finding the key in the haystack A practical guide to Differential Power Analysis	hunz
Fuzzing the Phone in your Phone	Collin Mulliner
GSM: SRSLY?	C.Paget , K.Nohl
How you can build an eavesdropper for a quantum cryptosystem	Qin Liu , S.Sauge
Layer 8 based IP Address hijacking in the end of the days of IPv4	nibbler
Legic Prime: Obscurity in Depth	H.Plötz , K.Nohl
Optimised to fail: Card readers for online banking	Steven J. Murdoch
Playing with the GSM RF Interface Doing tricks with a mobile phone	Dieter Spaar
Reverse Engineering DisplayLink devices USB to DVI for Hackers	Florian Echtler
SCCP hacking, attacking SS7 & SIGTRAN applications one step further	Langlois , Brunet
secuBT Hacking the Hackers with User Space Virtualization	Mathias Payer
Technik des neuen ePA	Henryk Plötz
Using OpenBSC for fuzzing of GSM handsets	Harald Welte
Vier Fäuste für ein Halleluja	Erdgeist & al.
Making	
Conlanging 101: I make languages (and you can too)	Sai Emrys
Homewreckery: Electrifying the Thread out of Clothing	eli skipp
Milkymist: An open hardware video synthesis platform	S.Bourdeauducq
Peanut Butter and Plastic: Industrial Revolution	Bre
Photography and the Art of Doing it Wrong	Audrey
Understanding Telecommunication Interception: Intelligence Support Systems Müller	Maguhn
Wireless power transfer: Tesla invented wireless power	Davor Emard
Science	
After the Hype: The current state of One Laptop per Child and Sugar Labs	ChristophD
Europäische Biometriestrategien	kosmo_k
Fußgängernavigation mit Augmented Reality : Navit - Navigationssystem	Martin Schallaer
Hacking the universe: When strings are super and not made of characters	Robert Helling
Leyen Rhetorik	Martin Haase
Privacy & Stylometry Practical Attacks AgainKst Authorship Recognition Techniques	Mike Brennan
Privacy-Enhanced Event Scheduling	B.Kellermann
Society	
CKAN: apt-get for the Debian of Data	Dietrich & Pollock
Computer.Spiele.Politik.	Bastian Dietz
Cybernetic Cannibalism: Why is Brazil the country of the future?	Marinho & al.

Das Recht am eigenen Bild und das Ende der "Street Photography"	Axel Schmidt
Das Zugangserschwerungsgesetz	Matthias Bäcker
Der Hackerparagraph beim Bundesverfassungsgericht	Dominik Boecker
Die Ereignisse des 12.9. und ihre Folgen	Maguhn
Die neokonservativen Thinktanks in der BRD	Volker Birk
Die Schlacht um die Vorratsdatenspeicherung	Kurz & al.
Die Verwaltung rüstet auf - der digitale Steuerbürger	Kai Kobschätzki
ETSI-Vorratsdatenspeicherung 2009 und andere Sockenpuppen der GCHQ	Erich Möchel
Exciting Tales of Journalists Getting Spied on, Arrested and Deported	Bicyclemark
Here Be Electric Dragons - Preparing for the Emancipation of Machines	Lorenz
I, Internet We are more Borg than we thought	Christiane Ruetten
Im Herz der Bestie Medien hacken	Cantsin, dornberger
Internetsperren - #zensursula and beyond	MOGIS
Kunsthfreiheit statt Hackerparagraph	Pimendis , Ommeln
Liquid Democracy: Direkter Parlamentarismus gemeinsam verbindlich entscheiden	Daniel Reichert
Location tracking does scale up - How skyhook wireless tracks you continuously	L. Aaron Kaplan
Privacy, openness, trust and transparency on Wikipedia	HaeB
Tor and censorship: lessons learned	Roger Dingledine
Vom Kreationismus zum Kollektivismus	Kay Hamacher
Weaponizing Cultural Viruses	Aaron Muszalski
Why Germany succeeded where America failed in achieving Voting Computer Changes	Kathleen Wynn
Why Net Neutrality Matters?	J.Zimmermann
WikiLeaks Release 1.0	wikileaks
Wofür offenes Internet? Warum wir klare Regeln für Netzneutralität brauchen	Lueke

Community

A Hacker's Utopia: What's There and What's Missing	Sandro Gaycken
Chaos-Familien-Duell	Brock, M.Ackermann
DDoS/botnet mitigation & hosting online communities	rodent
Eine Zensur findet statt	Jens Kubieziel
Fjord-Jahresrückblick 2009 Von Abwrackprämie bis Zensursula	Leitner, Rieger
Nougatbytes - Ein Wortspiel, bunt und in stereo Die geekige Bilderrätselspielschau	Ben , Rainer
Our darknet and its bright spots	aestetix & al.
Security Nightmares	Frank Rieger , Ron

Culture

The Lost Cosmonauts - Critical Thinking	Brian Dunning
UNBILD Pictures and Non Pictures Reterritorialisierung und Globalisierung	Christoph Faulhaber
Playing with the Built City	Eleanor Saitta

POUR PLUS D'INFORMATION

<http://events.ccc.de/congress/2009/Fahrplan/>

ACSAC – 2009



La 25^{ème} édition de la conférence **ACSAC - Annual Computer Security Applications Conference** – a eu lieu du 7 au 11 décembre dernier à Honolulu. Cette conférence technique aborde l'ensemble des thèmes liés à la sécurité des systèmes informatiques, l'accent étant mis cette année sur les malwares et botnets.

Les papiers des 42 communications ont été mis en ligne.

Authentication and Audit

A New Approach for Anonymous Password Authentication	Yang & al.
On the Security of PAS (Predicate-based Authentication Service)	Li & al.

Cloud Security

SecureMR: A Service Integrity Assurance Framework for MapReduce	Wei Wei & al.
Justifying Integrity Using a Virtual Machine Verifier	Schiffman & al.

Discovering Policy

A Network Access Control Mechanism Based on Behavior Profiles	Martinez & al.
RoleVAT: Visual Assessment of Practical Need for Role Based Access Control	Zhang & al.
How to securely break into RBAC: the BTG RBAC model	Ferreira & al.

DoS Defense

RAD: Reflector Attack Defense Using Message Authentication Codes	Kline & al.
A Guided Tour Puzzle for Denial of Service Prevention	Abliz & al.
Online Signature Generation for Windows Systems	Just & al.

Hardware/Software Security

Evaluation of a DPA-Resistant Prototype Chip	Kirschbaum & al.
--	------------------

FPValidator: Validating Type Equivalence of Function Pointers On The Fly	Wang & al.
A Surgically returning to randomized lib(c)	Fresi Roglia & al.
Integrity	
Scalable Web Content Attestation	Moyer & al.
A Study of User-Friendly Hash Comparison Schemes	Hsiao & al.
Intrusion Detection, Recovery and Analysis	
Online Sketching of Network Flows for Real-Time Stepping-Stone Detection	Coskun & al.
Preserving Business Continuity and Availability in an Intrusion Recovery System	Xiong & al.
An Empirical Approach to Modeling Uncertainty in Intrusion Analysis	Xinming Ou & al.
IP Rights	
Unifying Broadcast Encryption and Traitor Tracing for Content Protection	Jin & al.
Detecting Software Theft via System Call Based Birthmarks	Wang & al.
An efficient publicly verifiable Secure Audit Logging Scheme for distributed systems	Yavuz & al.
Malware, Botnets and OS Security	
FIRE: FInding Rogue nEtworks	Stone-Gross & al.
Active Botnet Probing to Identify Obscure Command and Control Channels	Stoll & al.
TrustGraph: Trusted Graphics Subsystem for High Assurance Systems	Nicol & al.
Protecting Commodity OS Kernels from Vulnerable Device Drivers	Butt & al.
Detecting Malicious Flux Service Nets through Passive Analysis of Rec. DNS Traces	Perdisci & al.
Identification of Bot Commands By Run-time Execution Monitoring	Park & al.
Mobile Security	
Transparent Encryption for Ext. Storage Media with Key Mgmt Adapted to Mobile Use	Zugenmaier & al.
Semantically Rich Application-Centric Security in Android	Ongtang & al.
Leveraging Cellular Infrastructure to Improve Fraud Prevention	Park & al.
Multimedia and Web Security	
Analyzing and Detecting Malicious Flash Advertisements	Ford & al.
Symmetric Cryptography in Javascript	Stark & al.
Analyzing Information Flow in JavaScript-based Browser Extensions	Dhawan & al.
Privacy and Software Assurance	
The Design of a Trustworthy Voting System	Tanenbaum & al.
Privacy through Noise: A Design Space for Private Identification	Nohl & al.
A Survey of Vendor Software Assurance Practices	Epstein & al.
Trust Management	
Secure Web 2.0 Content Sharing Beyond Walled Gardens	Hawkey & al.
Enabling Secure Secret Sharing in Distributed Online Social Networks	Buchegger & al.
Deploying and Monitoring DNS Security (DNSSEC)	Osterweil & al.
Virtualization Security	
MAVMM: A Lightweight and Purpose-Built VMM for Malware Analysis	Schear & al.
Protecting Kernel Code & Data with a Virtualization Aware Collaborative OS	Oliveira & al.
HIMA: A Hypervisor Based Integrity Measurement Agent	Azab & al.

POUR PLUS D'INFORMATION

http://www.acsac.org/2009/openconf/modules/request.php?module=oc_program&action=program.php

IAWACS – 2009



En octobre dernier, du 23 au 25, se tenait à Laval la première édition de la conférence **iaWACS** (International Alternative Workshop on Aggressive Computing and Security) organisée par l'**ESIEA** (Ecole Supérieure d'Informatique, Electronique, Automatique). Les papiers de la majorité des communications viennent d'être mis en ligne.

Les actes sont annoncés disponibles en totalité en mars prochain.

Deux de ces communications ont attiré notre attention :

- La communication '**Processor-dependent malware**' détaille quelques astuces qui permettraient à un logiciel d'identifier le processeur hôte, une nécessité pour qui souhaiterait écrire un code adaptatif au contexte d'exécution sans jamais s'appuyer sur les fonctions offertes par celui-ci.
- La communication '**Playing in a Satellite Environment 1.2**' déjà présentée à l'occasion de nombreuses conférences dont le principal intérêt est d'attirer l'attention – est-ce un bien – sur les mécanismes de transfert de données utilisés par les satellites de diffusion et de communication. Un domaine jusqu'alors chasse-gardée de certains amateurs.

Cryptanalysis of Chaos-based Hash Function (CBHF)	M.Maqableh, V.Danchev
Facing the global cyber threat	Sebastien Tricaud
Functional polymorphism engines	Gregoire Jacob

How to choose RSA Keys (The Art of RSA : Past, Present and Future)?	R.Erra, C.Grenier
Playing in a Satellite Environment 1.2	Leonardo Nve Egea
Processor-dependent malware	E.Filiol, R.Erra, A.LDesnos
Side-channel Attacks Based on (multi) Linear Approximations	C.Tavernier & T.Roche
WiShMaster reloaded tutorial	Benjamin Caillat

POUR PLUS D'INFORMATION

http://www.esiea-recherche.eu/iawacs_2009_papers.html

GUIDES

NIST – ETAT DES GUIDES DE LA SERIE SPECIALE 800



Le **NIST** vient de publier la version préliminaire du guide **SP800-131** 'Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes' et la version définitive du guide **SP800-38E** 'Recommendation for Block Cipher Modes of Operation – XTS-AES'.

SP800-131	Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes	[R]	01/10
SP800-126r1	The Technical Specification for SCAP	[R]	12/09
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 Ipsec 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]	01/10
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

DISA – GUIDES ET CHECK LISTES DE SECURISATION



La **DISA** a procédé à la mise à jour des listes de contrôle des environnements Base de Données Générique, MS SQL, Oracle, Exchange 2003, Windows 2000, 2003, 2008 et enfin BlackBerry. On notera la publication d'une version provisoire d'une liste de contrôle destinée au système BlackBerry Enterprise Serveur 5 (**BES**).

[10 Mise(s) à jour, 4 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	1.2	05/01/10
ESM		1.1	05/06/06	1.1.3	10/04/07
ERP		1.1	10/04/07	1.1.1	10/04/07
Database	Générique	8.1	19/10/07	8.1.3	25/12/09
	Oracle 9, 10 et 11			8.1.6	25/12/09
	MS SQL Server 7, 2000, 2005			8.1.4	25/12/09
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
.NET				1.2.3	18/02/09
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 Guidance for BES			1.0	05/01/10
	BlackBerry			5.6	05/01/10
	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	6.2	25/12/09	6.1.2	28/08/09	M
	ACF2	6.2	25/12/09	6.1.2	28/08/09	M
	TSS	6.2	25/12/09	6.1.2	28/08/09	M
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	5.1.22	18/12/09	
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	6.1.15	25/12/09	6.1.15	25/12/09	N
	XP	6.1.15	25/12/09	6.1.14	23/10/09	N
	Vista	6.1.15	25/12/09	6.1.14	23/10/09	N
	2003			6.1.15	25/12/09	M
	2008			6.1.18	25/12/09	M
	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>

CIS - CATALOGUE DE PROCEDURES ET DE TESTS



Le **CIS (Center for Internet Security)** a publié la mise à jour des procédures de test des environnements SGBD **IBM DB2, SQLServer 2005** et système **ESX Server 3.5**.

Une première version des procédures de test de l'application **Mozilla Firefox** vient par ailleurs d'être mise à disposition.

APPLICATIONS				
Apache	Web Server Versions V1.3.37/2.0.59/2.2.4	P1 P2	V2.2	Outil existant
	Tomcat Server	P1	V1.0	
Bind	Version 9.0 – 9.5	P2	V2.0	
Firefox	Mozilla Firefox	P1	V1.0	
FreeRadius	Version 1.1.3	P1	V1.0	
IBM	DB2 8-9.5	P1	V1.1	
	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	V1.2	
	Office 2007	P1	V1.0.0	
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		P1	V1.0	
VMWare	ESX 3.0	P1	V1.0	Fichiers d'aide
	ESX 3.5	P1	V1.2	
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	
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>

MAGAZINES

ENISA - QUARTERLY REVIEW



Le dernier numéro de l'année 2009 de la revue de l'**ENISA** - EQR - a été publié fin décembre. Il aborde quatre thèmes:

- la résilience,
- la sensibilisation et l'état de la sécurité,
- l'interopérabilité et la protection,
- les systèmes de gestion de la sécurité des systèmes d'information.

Deux thèmes - résilience et sensibilisation - au cœur des préoccupations de l'**ENISA** ont déjà fait l'objet de plusieurs articles dans cette même revue.

Le sommaire de ce numéro est reproduit ci-dessous:

A Letter from the Executive Director

A Word from the Editor

A Word from the Experts

Resilience

- Measuring Resilience – the Next Challenge
- ENISA's Good Practice Guide on National Incident Reporting Schemes
- Good Practice Guide on National Exercises
- The ENISA Virtual Working Group on Providers' Measures for Resilience

Awareness Raising and Security Status

- OSI: A Security Helpdesk for Internet Users in Spain
- Awareness Raising in Japan
- Information Security Threats and Countermeasures in Korea

Interoperability and Protection

- Cloud Computing
- Electronic Signature Interoperability

ISMS

- Standardised Management and Control of Information Security – Austria
- Risk Analysis in an Italian Public Body: ISPESL

POUR PLUS D'INFORMATION

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.

Bien que n'entrant pas dans le cadre des litiges qui nous intéressent au plus haut point, le litige [D2009-1059 'lomalinda.com'](#) met en évidence les difficultés que rencontrera l'**OMPI** lorsque le désaccord porte sur un nom devenu d'usage public au fil des décennies, ici le nom d'une ville américaine déclinée de multiples manières depuis sa fondation en 1905. La [charte de nommage de l'AFNIC](#) doit normalement prévenir de tels problèmes par le biais de sa liste de termes interdits, ou réservés, dont les noms de communes.

Nos lecteurs pourront aussi s'intéresser au jugement du litige [D2009-0034](#) concernant les noms de domaine '[toywatch.fr](#)' et '[toy-watch.fr](#)', imitant la marque **ToyWatch**, domaines enregistrés par un tiers dans l'optique d'informer le consommateur sur la provenance des produits vendus sous cette marque. Le jugement est en faveur du détenteur des deux noms de domaine, le requérant n'ayant pu apporter les éléments permettant de justifier de son bon droit. Un jugement suffisamment rare pour être noté.

Le litige [D2009-1525](#) a ceci d'intéressant qu'il porte sur un domaine, '[online-mastercard.com](#)' acquis dans une mise aux enchères sur **eBay**. Le propriétaire argumente, sans succès, que ce nom est simplement constitué de l'association de trois mots courants que l'on peut trouver dans tout bon dictionnaire.

On notera, le litige [DFR2009-0036](#) concernant le nom de domaine '[sudnet.fr](#)' par une société en contrat de partenariat avec la société **NordNet**, laquelle a estimé que ce nom de domaine portait atteinte à ses droits de marque sur le terme 'nordnet'. La transmission du nom 'sudnet.fr' au profit de la société **NordNet** est ordonnée au titre d'une violation du comportement loyal en matière commerciale.

Enfin, et pour terminer ce rapide tour d'horizon des derniers arbitrages, citons le litige [D2009-1661](#) portant sur 1542 noms de domaines portant référence à sept marques réputées dans le domaine de l'hôtellerie. Le tiers ayant enregistré ces domaines disposerait d'un portefeuille de plus de 70000 noms selon les recherches effectuées par l'expert mandaté par le **WIPO**.

D2009-1405	skyrockent.com	Vortex (SkyRock)	23/12
D2009-1514	tati.com	L.M.X. Holding (marque TATI)	30/12
D2009-1431	diors.com	Christian Dior Couture	04/01
D2009-1482	jambon-parme.com	Consorzio del Prosciutto di Parma	05/01
D2009-1530	sanofiaventiszentiva.com	Sanofi-aventis	05/01
D2009-1521	go-vuitton.com	Louis Vuitton Malletier	30/12
D2009-1525	online-mastercard.com	MasterCard International Inc.	07/01
DFR2009-0036	sudnet.fr	NordNet	13/01

POUR PLUS D'INFORMATION

<http://www.wipo.int/rss/index.xml?col=dnddocs>

http://www.wipo.int/freepublications/fr/arbitration/779/wipo_pub_779.pdf

- Dernières décisions

- Procédure de règlement des litiges

STANDARDS

IETF – LES RFC TRAITANT DIRECTEMENT DE LA SECURITE

Thème	Num	Date	Etat	Titre
ANCP	5713	01/10	Inf	Security Threats and Security Requirements for the Access Node Control Protocol (ANCP)
CMS	5752	01/10	Pst	Multiple Signatures in Cryptographic Message Syntax (CMS)
	5753	01/10	Inf	Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)
IKE	5723	01/10	Pst	Internet Key Exchange Protocol Version 2 (IKEv2) Session Resumption
KEYNOTE	5708	01/10	Inf	X.509 Key and Signature Encoding for the KeyNote Trust Management System

PKI	5755	01/10	Pst	An Internet Attribute Certificate Profile for Authorization
	5758	01/10	Pst	Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA
	5759	01/10	Inf	Suite B Certificate and Certificate Revocation List (CRL) Profile
SHA2	5754	01/10	Pst	Using SHA2 Algorithms with Cryptographic Message Syntax
SMIME	5750	01/10	Pst	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling
	5751	01/10	Pst	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification

IETF – LES RFC LIÉS A LA SECURITE

Thème	Num	Date	Etat	Titre
IPV6	5569	01/10	Inf	IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)

IETF – LES NOUVEAUX DRAFTS TRAITANT DE LA SECURITE

Thème	Nom du Draft	Date	Titre
EAP	draft-wang-hokey-erp-aak-00	19/01	EAP Protocol Extensions for Authenticated Anticipatory Keying
KARP	draft-lebovitz-karp-roadmap-00	14/01	Roadmap for Crypto. Auth. of Routing Proto. Packets on the Wire
SASL	draft-wierenga-ietf-sasl-saml-00	15/01	A SASL Mechanism for SAML
	draft-lear-ietf-sasl-openid-00	19/01	A SASL Mechanism for OpenID
TLS	draft-agl-tls-nextprotoneg-00	20/01	TLS Next Protocol Negotiation Extension
	draft-kanno-tls-camellia-gcm-00	27/01	Camellia Galois Counter Mode (GCM) Cipher Suites for TLS
	draft-kanno-tls-camellia-psk-00	27/01	Pre-Shared Key Cipher Suites for Camellia for TLS

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

Thème	Nom du Draft	Date	Titre
DHCP	draft-sakane-dhc-dhcpv6-kdc-option-06	22/01	Kerberos Option for DHCPv6
DNS	draft-ietf-dnsext-dnssec-alg-allocation-02	25/01	Cryptographic Algorithm Identifier Allocation for DNSSEC
	draft-hoffman-dnssec-ecdsa-01	25/01	Elliptic Curve DSA for DNSSEC
DTNRG	draft-irtf-dtnrg-bundle-security-13	22/01	Bundle Security Protocol Specification
EAP	draft-marin-eap-frm-fastreauth-01	19/01	Fast EAP Re-authentication based on a new EAP method
GEOPRIV	draft-ietf-geopriv-policy-21	15/01	Document Format for Expressing Privacy Preferences for Location
GIST	draft-ietf-nsis-ntlp-sctp-08	20/01	GIST over SCTP and Datagram TLS
HKDF	draft-krawczyk-hkdf-01	25/01	HMAC-based Extract-and-Expand Key Derivation Function (HKDF)
HOKEY	draft-ietf-hokey-preauth-ps-12	22/01	EAP Early Authentication Problem Statement
IKE	draft-nir-ike-qcd-06	19/01	A Quick Crash Detection Method for IKE
IPSEC	draft-ietf-ipsecme-ikev2bis-07	20/01	Internet Key Exchange Protocol: IKEv2
KERBEROS	draft-josefsson-kerberos5-starttls-08	22/01	Using Kerberos V5 over TLS protocol
OPSEC	draft-ietf-opsec-routing-protocols-crypto-...-03	21/01	Issues with Crypto. Protection Methods for Routing Protocols
RTP	draft-ietf-avt-srtp-not-mandatory-05	22/01	Why RTP Does Not Mandate a Single Security Mechanism
	draft-zimmermann-avt-zrtp-17	20/01	ZRTP: Media Path Key Agreement for Secure RTP
SASL	draft-ietf-sasl-gs2-20	11/01	Using GSS-API Mechanisms in SASL: The GS2 Mechanism Family
SIP	draft-ietf-sipcore-sec-flows-02	22/01	Example call flows using SIP security mechanisms
SNDP	draft-ietf-csi-sndp-prob-04	22/01	Securing Neighbor Discovery Proxy: Problem Statement
SSH	draft-igoe-secsh-x509v3-01	22/01	X.509v3 Certificates for Secure Shell Authentication
TCP	draft-ietf-tcpm-icmp-attacks-09	19/01	ICMP attacks against TCP
TLS	draft-kanno-tls-camellia-ecc-sha-01	27/01	Addition of Camellia ECC Suites with SHA-1 and SHA-2
	draft-campagna-tls-ecmqv-ecqv-01	15/01	ECMQV_ECQV Cipher Suites for Transport Layer Security

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