

INTERNATIONAL

**LE TOUR DU MONDE
DE LA CRYPTO**



ÉDITORIAL

DE MARC JACOB

©Hadi Djunaedi



Crypto : de l'ombre à la lumière

De tous temps, la problématique de la confidentialité des données a été adressée avec des techniques diverses et variées. Les premiers pas de la stéganographie pendant l'antiquité se sont d'ailleurs parfois accompagnés de méthodes pour le moins barbares. En effet, à cette époque, les messages d'importance étaient gravés sur la tête des esclaves. Ces derniers étaient décapités après lecture du message par le destinataire. Bien sûr, les dirigeants de ces temps-là ont très vite compris que ces méthodes sanguinaires étaient peu fiables et « peu rentables humainement »... Par la suite, bon nombre de techniques de dissimulation de l'information se sont développées et ont fait de la cryptologie une science quasi-incontournable.

Au fil du temps, les gouvernants ont réalisé que les clés de la crypto ne devaient pas être mises entre toutes les mains. Ainsi, pendant des années, ils ont gouverné par « l'obscurantisme » en interdisant strictement son utilisation à des fins civiles. Après des siècles de mise au secret, il a fallu « le coup de force » de Phil Zimmermann pour obliger nos dirigeants à remettre enfin ces technologies à « la lumière du jour ». Bien heureusement pour les fournisseurs et les utilisateurs, puisque la cryptographie se trouve, aujourd'hui, au centre de la plupart des déploiements sécurisés.

En effet, face aux pertes de données qui se multiplient, à la montée du cloud computing, à l'explosion des échanges d'information par mail... les vendeurs proposent de déployer des solutions de sécurité, dont le pivot est la cryptographie. Cet engouement redonne un « coup de jeunesse » à cette technologie séculaire. Cependant, si elles sont encore plus efficaces qu'autrefois, elles n'ont pas encore résolu le problème crucial : l'Homme. Ce « maillon faible » est porteur de données et de codes confidentiels qu'il manipule avec plus ou moins de rigueur. De plus, on se méfie de lui, car sa fidélité est sans cesse remise en cause par l'éventuelle suspicion d'une fuite d'informations. On ne rappellera d'ailleurs jamais assez que le meilleur outil du monde demeurera faillible contre l'Homme. C'est pourquoi, s'il reste essentiel aujourd'hui de déployer des solutions de cryptage, des sessions de formation s'imposent.

Par Marc Jacob

LISTE DES ANNONCEURS

APC	3 ^{ÈME} DE COUVERTURE	INFOSECURITY UK	6
ATHENA GS – SHADOW PROTECT	52	INTEGO	2 ^{ÈME} DE COUVERTURE
BULL	14	MED IT	2
CERCLE DE LA SÉCURITÉ	46	PRIM X TECHNOLOGIES	4 ^{ÈME} DE COUVERTURE
CHERRY	12	RIAM	8
DOCUMENTATION	56	SIMP : UN ENCART LIBRE	
EPSI	31	SOLUTIONS LINUX	58
GSDAYS	60-61	SOLUTIONS RH	4
HSC	43	STONESOFT : UN ENCART LIBRE	

REVUE TRIMESTRIELLE

N°10 – janvier, février, mars 2010
www.globalsecuritymag.fr et
www.globalsecuritymag.com
 ISSN : 1959 - 7061
 Dépôt légal : à parution
 Editée par SIMP
 RCS Nanterre 339 849 648
 17 avenue Marcelin Berthelot
 92320 Châtillon
 Tél. : +33 1 40 92 05 55
 Fax. : +33 1 46 56 20 91
 e-mail : marc.jacob@globalsecuritymag.com

REDACTION

Directeur de la Publication :

Marc Brami

Rédacteur en chef :

Marc Jacob

Rédactrice :

Emmanuelle Lamandé

Ont collaboré à ce numéro :

Olivier Iteanu, Anabelle Richard et Ophélie De Kersauson

Assistante :

Sylvie Levy

Responsable technique :

Raquel Ouakil

Photos :

Robert Martiano, Marc Jacob

Comité scientifique :

Pierre Bagot, Francis Bruckmann
 Eric Doyen, Catherine Gabay,
 François Guillot, Mauro Israël,
 Olivier Iteanu, Dominique Jouniot
 Zbigniew Kostur, Patrick Langrand,
 Yves Maquet, Thierry Ramard,
 Hervé Schauer, Wayne Sutton,
 Michel Van Den Berghe,
 Bruno Kerouanton

PUBLICITE

SIM Publicité

Tél. : +33 1 40 92 05 55

Fax. : +33 1 46 56 20 91

e-mail : ipsimp@free.fr

PAO

Imadjinn sarl

Tél. : 02 51 53 01 46

e-mail : info@imadjinn.fr

Images de couverture :

©Hadi Djunaedi

IMPRESSION

Imprimerie Hauguel

8-14 villa Léger

92240 Malakoff

Tél. 01 41 17 44 00

Fax 01 41 17 44 09

e-mail : info@imprimerie-hauguel.fr

Imprimé avec des encres végétales sur papier éco-responsable certifié PEFC par un imprimeur adhérent à Imprim'vert selon le procédé CTP sans chimie.

ABONNEMENT

Prix au numéro :

18 € TTC (TVA 19,60%)

Abonnement annuel :

50 € TTC (TVA 19,60%)



SALON

med-IT

2010

**Salon International sur les
Technologies de l'Information**



10 ▶ 11 ▶ 12 mai 2010

Palais de la Culture, Alger



EDITORIAL

DE MARC JACOB

©Hadi Djunaedi



Cryptology: out of the darkness

There have always been a variety of ways of tackling the problem of data confidentiality. The first attempts at steganography during ancient times sometimes used rather barbaric methods, with important messages being engraved on the heads of slaves who were subsequently decapitated when the recipient had read the message. Naturally, the leaders of the time soon realised that these bloody methods were not very reliable and rather costly in human terms. Subsequently, a number of concealment techniques were developed and cryptology became an almost indispensable science.

Over time, governing bodies realised that not everyone should have access to cryptology keys. As a result, they resorted to obscurantism and strictly prohibited the use of cryptology for civil purposes. After centuries of secrecy, it required 'offensive action' on the part of Phil Zimmermann to force governing bodies to finally bring these technologies out of the darkness. Just as well for suppliers and users because, today, cryptology is at the heart of most security applications.

In the face of rising cases of data loss, increased use of cloud computing and the explosion in email information exchange, vendors are offering security solutions that rely on cryptology. This enthusiasm has given a new lease of life to this age-old technology. However, although the technology is more reliable than it used to be, the human element is still a critical issue. This 'weak link' in the chain manipulates data and confidential codes with varying degrees of rigour. There is also the question of whether employees can be trusted not to leak data. One cannot stress enough that the best technology in the world remains fallible when there is human intervention. For this reason, training is of the utmost importance when encryption solutions are being deployed.

By Marc Jacob



© Andres

SOLUTIONS Ressources Humaines

Avec le soutien de



16^{ème} Salon

des outils et services dédiés aux dirigeants d'entreprises, aux DRH, aux responsables de la Formation et des Systèmes d'Information.



HALL 5.1
PARIS - PORTE
DE VERSAILLES

9-10-11
MARS 2010

18 porte de la

elearning
xpo

Formation à distance
et en ligne

LUDIMAT
EXPO

Jeu dans la formation
et la communication

www.solutions-ressources-humaines.com

INFOPROMOTIONS - 97 rue du Cherche-Midi - 75006 PARIS, FRANCE

Tel. : +33 (0)1 44 39 85 00 - Fax : +33 (0)1 45 44 30 40

E-mail : r.cerval@infoexpo.fr



THÉMA

18 CRYPTO DE L'OMBRE À LA LUMIÈRE

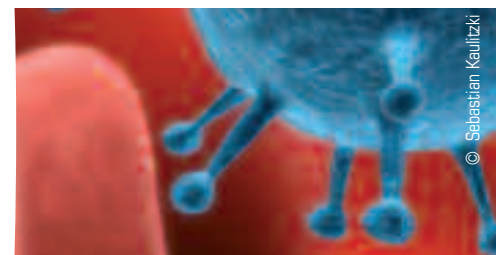
SOMMAIRE

- 01** Edito : Crypto : de l'ombre à la lumière
03 Editorial Cryptology: out of the darkness
09 Agenda Événements 2010
- 10 DU CÔTÉ DE L'INTERNATIONAL**
Le tour du monde de la cryptologie en dix pays
Par Annabelle Richard, Avocat à la Cour - Attorney at Law (New York Bar), et Ophélie De Kersauson, Juriste
- 18 THÉMA - CRYPTOLOGIE**
Jean-Louis Desvignes, Président de l'A.R.C.S.I. : la cryptologie « mathématique » a encore un bel avenir
Interview par Emmanuelle Lamandé et Marc Jacob
- 22** Carlos Aguilar-Melchor, Philippe Gaborit et Marc Rybowicz, Chercheurs à l'unité mixte de recherche Université de Limoges :
La cryptologie : de la théorie à la pratique
Interview par Emmanuelle Lamandé et Marc Jacob
- 28** Frédéric Boissel, AFPA :
Crypto : une question d'équilibre entre sécurité et facilité d'utilisation
Interview par Marc Jacob
- 30** La cryptographie : une arme à double tranchant
32 David Pointcheval, INRIA - ENS - CNRS :
vers un algorithme robuste à l'ordinateur quantique...
34 Cryptologie quantique : cette « méconnue » qui fait rêver
- 38 MALWARES BUSTERS**
Les « James Bond du clavier » ont de beaux jours devant eux
Par Marc Jacob et Emmanuelle Lamandé
- 44** Conficker : Champion du monde des virus en 2009
Par Marc Jacob et Emmanuelle Lamandé
- 48 NORME**
Conférence du Club 27001 : les organismes certificateurs doivent être plus dynamiques
Par Frédéric Connes, consultant HSC
- 54 CHRONIQUE JURIDIQUE**
Messageries électroniques instantanées en entreprise, un statut juridique méconnu
Par Olivier Iteanu, Avocat à la Cour Chargé d'enseignement à l'Université de Paris XI
- 62 SPECIAL GSDAYS 2009**
Promouvoir les bonnes pratiques par la sensibilisation des utilisateurs
Par Céline Vercruysse, Advens
- 64** SCRT : Webshag et MiniMySqlat0r, deux outils d'attaque Web
Par Paul Such, Alain Mowat et Sergio Alves Domingues, SCRT
- 66** Les périphériques multifonctions :
nouvel âge d'or des pirates ?
Par Jean baron et Thibault Koechlin, NBS System

10 LE TOUR DU MONDE DE LA CRYPTO



18 THÉMA



38 MALWARES BUSTERS



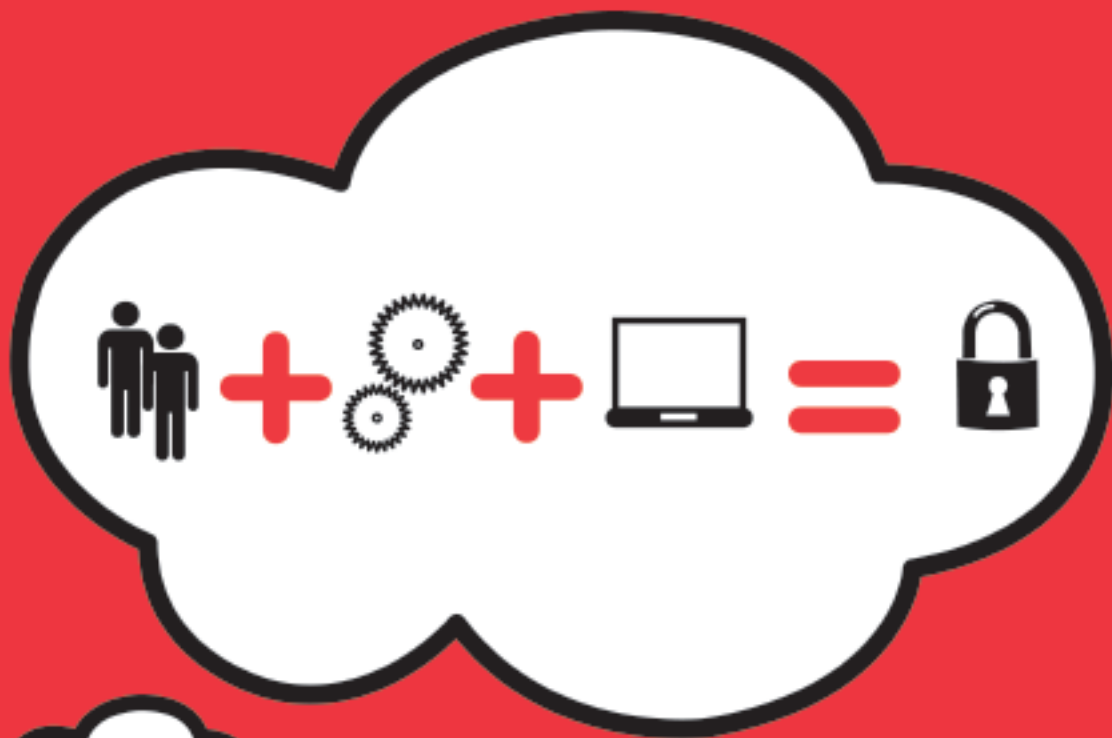
48 NORME



LES JOURNÉES FRANCOPHONES DE LA SÉCURITÉ

62 SPÉCIAL GSDAYS 2009

Retrouvez notre fil d'informations
sur la sécurité et le stockage sur
www.globalsecuritymag.fr
www.globalsecuritymag.com



INFORMATION SECURITY – ARE YOU BEING SMART ENOUGH?

Working smarter has never been so important and security so crucial when it comes to safeguarding and growing your business.

- Smart spending to justify and get value from budgets
- Smart optimization of your technology, processes and resources
- Smart people – education, training and awareness

Register free* to attend now at:
www.infosec.co.uk

**CELEBRATING 15 YEARS AT THE
HEART OF THE INDUSTRY
EUROPE'S NO.1
INFORMATION SECURITY EVENT**

27 – 29 April 2010

Earls Court

London | UK

Organised by:



* Register free before 23rd April at 5pm. Onsite registration £20.



FEATURE

18 CRYPTOLOGY OUT OF THE DARKNESS

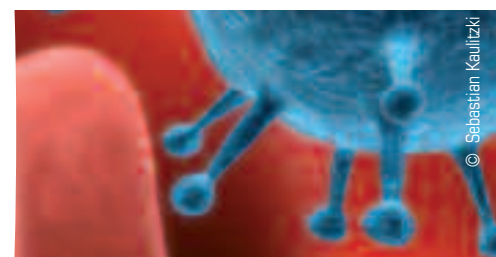
CONTENTS

- 01** **Edito** : Crypto : de l'ombre à la lumière
- 03** **Editorial** Cryptology: out of the darkness
- 09** **Agenda**
- 10** **INTERNATIONAL**
A round up of cryptology techniques in ten different countries
By Annabelle Richard, attorney-at-law (Paris & New York), and Ophélie De Kersauson, corporate lawyer
- 18** **FEATURE - CRYPTOLOGY**
Jean-Louis Desvignes, president of A.R.C.S.I.: 'mathematical' cryptology still has a bright future
Interview by Emmanuelle Lamandé and Marc Jacob
- 22** Carlos Aguilar-Melchor, Philippe Gaborit, and Marc Rybowicz, researchers at Limoges University
Cryptology: from theory to practice
Interview by Emmanuelle Lamandé and Marc Jacob
- 28** Frédéric Boissel, AFPA :
Cryptology: a question of balance between ease of use and security
Interview by Marc Jacob
- 30** Cryptology: a double-edged sword
- 32** David Pointcheval, INRIA - ENS - CNRS :
towards robust algorithms and quantum computing
- 34** Quantum cryptology: a little-understood technique that fires the imagination
- 38** **MALWARES BUSTERS**
The keyboard 'James Bonds' still have a bright future ahead of them
By Marc Jacob and Emmanuelle Lamandé
- 44** Conficker: world virus champion in 2009
By Marc Jacob and Emmanuelle Lamandé
- 48** **STANDARDS**
27001 Club conference: the certifying bodies have to be more dynamic
By Frédéric Connes, consultant with HSC
- 54** **LEGAL COLUMN**
Electronic messaging systems in the business environment: the legal status is not well known
By Olivier Itéanu, attorney-at-law, lecturer at the Paris XI university
- 62** **SPECIAL FEATURE- GS DAYS**
Promoting good practice by developing user awareness
By Céline Verduyssen, Advens
- 64** SCRT: Webshag and MiniMySQLat0r, two web attack applications
By Paul Such, Alain Mowat and Sergio Alves Domingues, SCRT
- 66** Multifunction peripherals: a new golden goose for hackers?
By Jean baron and Thibault Koechlin, NBS System

10 A ROUND UP OF CRYPTOLOGY TECHNIQUES



18 FEATURE



38 MALWARES BUSTERS



48 STANDARDS



62 SPÉCIAL GSDAYS 2009

Retrouvez notre fil d'informations sur la sécurité et le stockage sur
www.globalsecuritymag.fr
www.globalsecuritymag.com

