

## Frédéric RAYNAL

43 rue du Commerce  
75015 PARIS

Mail : frederic.raynal@miscmag.com  
fred@security-labs.org

Né le 17 Mars 1972

Nationalité française

Dégagé des obligations militaires

## EXPÉRIENCES PROFESSIONNELLES

- Jun 2006 -** **Responsable R&D Sécurité Informatique** . SOGETI IS / CAP GEMINI.  
Constitution de l'activité de R&D autour de la sécurité des systèmes d'informations. Études sur la cryptanalyse appliquée, les malwares, l'analyse de protocoles et les attaques à base d'information.
- Oct. 2004 - Mars 2006** **Responsable R&D Sécurité Informatique** . EADS CENTRE DE RECHERCHE.  
Animation et orientation de la R&D autour de la sécurité des systèmes d'informations : analyse de programme (source/binaire), sécurisation des noyaux, reverse engineering, malwares...  
▷ *Titularisation en tant qu'Expert Informatique pour tout le groupe EADS*
- Jun 2003 - Sept. 2004** **Ingénieur R&D Sécurité Informatique** . EADS DCS.  
Projets et études amonts
- Jan. 2001 -** **Rédacteur en chef** . MISC (MULTI-SYSTEMS & INTERNET SECURITY COOKBOOK).  
Magazine bimestriel consacré à la sécurité informatique.
- Nov 2002 - Mai 2003** **Ingénieur R&D** . SPEKA NETWORKS.  
Études pour la réalisation d'un point d'accès sécurisé pour réseau wireless. Système de veille web.
- 1997 - Nov. 2001** **Doctorant en dissimulation d'information** . INRIA - PROJETS FRACTALES & CODES.  
Fractales pour le *watermarking*, élaboration d'un *protocole d'évaluation* pour les algorithmes de *watermarking*, études sur les liens entre la *cryptographie* et la *dissimulation d'information*, programmation génétique appliquée au problème inverse pour les IFS  
▷ *Administration système Unix*

## FORMATION : INGÉNIEUR ET DOCTEUR EN INFORMATIQUE

- 2007** **Formation professionnelle**. ÉCOLE DE GUERRE ÉCONOMIQUE.  
Vice-major
- 1998 - Nov. 2001** **Doctorat en Informatique**. PARIS XI (ORSAY) & INRIA, PROJETS CODES ET FRACTALES.  
(3 ans)  
Mention Très Honorable - Qualifié en Janvier 2003  
▷ **Sujet** : *Études d'outils pour la dissimulation d'information : approches fractales, protocoles d'évaluation et protocoles cryptographiques*
- 1997** **DEA IARFA** . UNIVERSITÉ PARIS VI-JUSSIEU.  
Mention Bien
- 1990 - 1996** **Ingénieur ESIEA** (ÉCOLE SUPÉRIEURE D'INFORMATIQUE, D'ÉLECTRONIQUE ET D'AUTOMATIQUE).  
Mention Très Honorable

## COMITÉS

- Sept. 2007** **Comité de rédaction** . JOURNAL OF VIROLOGY.  
Publication IEEE à caractère scientifique sur les codes malicieux
- Depuis 2006** **Comité d'Organisation** . HACK.LU.  
Conférence internationale organisée par le Honeynet luxembourgeois
- De 2003 à 2006** **Président du Comité d'Organisation** . SSTIC.  
Symposium sur la Sécurité des Technologies de l'Information et de la Communication  
En Juin à l'ESAT à Rennes, première édition en Juin 2003

## ENSEIGNEMENT

- Janvier 2008** **IRISA**. ÉCOLE DE CHERCHEURS.  
Professeur invité pour un cours sur les failles logicielles
- Depuis 2005** **Professeur** . MASTER SSI - ESIEA.  
Cours sur les Systèmes d'Exploitation et l'analyse post-mortem
- Depuis 2004** **Professeur** . AGENCE INTERNATIONALE POUR LA FRANCOPHONIE.  
Cours de cryptographie, Système d'Exploitation, analyse post-mortem & programmation à Ouagadougou (Burkina Faso, 2004), Libreville (Gabon, 2005), Dakar (Sénégal, 2006), Rabat (Maroc, 2007)
- Jun - Juillet 2004** **CEA/INRIA/EDF**. ÉCOLE D'ÉTÉ.  
Professeur en charge des cours de cryptographie, système et programmation, analyse post-mortem
- Depuis 2003** **ESIEA et Université de Limoges**. DERNIÈRE ANNÉE INGÉNIEUR.  
Cours intitulé *Programmation (in)sécurisée* (18h)
- Jan. - Avr. 2003** **Université Paris XII - Val de Marne**. DESS ISYDIS .  
Cours intitulé *Cryptographie et sécurité informatique* (30h)
- 1998 - 2000** **Paris IX - Dauphine**. DEUG MASS 1<sup>ÈRE</sup> ANNÉE.  
(2 × 1 an)  
TD/TP d'informatique (Algorithmique et Java), sous la direction de F. Rossi  
▷ **Projets** : *compression JPEG et simulation d'un système multi-agents*



# Publications scientifiques

## Journaux

### **Communications chiffrées : et si le ver n'était pas (que) dans la pomme ?**

F. RAYNAL, E. FILIOL

Revue de Défense Nationale, numéro spécial sur la cybercriminalité

Mai 2008

### **Rootkit modeling and experiments under Linux**

F. RAYNAL, É. LACOMBE, V. NICOMETTE

Journal in Computer Virology 4(2) : 137-157

2008

### **New Threats and Attacks on the World Wide Web**

T. HOLZ, S. MARECHAL, F. RAYNAL

IEEE Security & Privacy Journal

Mars 2006

### **Attacking attackers (2 parts)**

T. HOLZ, F. RAYNAL

SecurityFocus,

<http://www.securityfocus.com/infocus/1856>

<http://www.securityfocus.com/infocus/1857>

Janvier 2006

### **Defeating Honeypots : System Issues (2 parts)**

T. HOLZ, F. RAYNAL

SecurityFocus,

<http://www.securityfocus.com/infocus/1826>

<http://www.securityfocus.com/infocus/1828>

Avril 2005

### **Honeypot forensics : analyzing system and files**

F. RAYNAL, Y. BERTHIER, P. BIONDI, D. KAMINSKY

IEEE Security & Privacy Journal

Août 2004

### **Honeypot forensics : analyzing the network**

F. RAYNAL, Y. BERTHIER, P. BIONDI, D. KAMINSKY

IEEE Security & Privacy Journal

Juin 2004

### **Les Canaux cachés**

F. RAYNAL

Techniques de l'Ingénieur

Édition spéciale Sécurité Informatique - Déc. 2003

### **Stéganographie : visite de l'univers numérique pour dissimuler des informations**

F. RAYNAL, F. PETITCOLAS, C. FONTAINE

Pour la Science

Édition spéciale Cryptographie - Juillet 2002

### **Évaluation automatique des méthodes de tatouage**

F. RAYNAL, F. PETITCOLAS, C. FONTAINE

Journal du Traitement du signal

Édition spéciale Tatouage 2001

### **Polar IFS + Individual Genetic Programming = Efficient IFS Inverse Problem Solving**

P. COLLET, E. LUTTON, F. RAYNAL, M. SCHONAUER

Genetic Programming and Evolvable Machines Journal

Volume 1, Issue 4, pp. 339-361, October 2000

### **Polar IFS and Individual Genetic Programming to solve IFS Inverse Problem**

P. COLLET, E. LUTTON, F. RAYNAL, M. SCHONAUER

Research Report INIRA 3849

December 1999

## Conférences

### **Petit traité de manipulation à l'usage des honnêtes gens**

F. RAYNAL, F. GASPARD  
Guerre de l'information et lutte informatique, IHEDN  
Paris, France, Déc. 2008

### **Malicious Origami in PDF**

F. RAYNAL, G. DELUGRÉ  
6th PacSec  
Tokyo, Japon, Oct. 2008

### **Cryptographie : attaques tous azimuts**

F. RAYNAL, E. FILIOL, J.B. BEDRUNE  
6th SSTIC Annual Conference  
Rennes, France, Juin 2008

### **Small treatise about e-manipulation for honest people**

F. RAYNAL, F. GASPARD  
17th EICAR Annual Conference  
Laval, France, Mai 2008

### **Malicious cryptography...reloaded : über-malware**

E. FILIOL, F. RAYNAL  
9th CanSecWest Annual Conference  
Vancouver, Canada, Mars 2008

### **Attacks : from technical to informational field**

F. RAYNAL  
Bellua Cyber Security (BCS)  
Jakarta, Indonesia, Oct. 2007

### **De l'invisibilité des rootkits : application sous Linux**

É. LACOMBE, F. RAYNAL, V. NICOMETTE  
Symposium sur la Sécurité des Technologies de l'Information et des Communications (SSTIC)  
Rennes, France, Juin 2007

### **Malicious crypto : (ab)using cryptology**

F. RAYNAL  
EuSecWest  
Londres, Angleterre, Fév. 2006

### **Kernel rootkits for fun and profit**

É. LACOMBE & F. RAYNAL  
Libre Software Meeting (LSM)  
Dijon, France, Juillet 2005

### **Detecting suspicious execution environments**

T. HOLZ, F. RAYNAL  
Information Assurance Workshop 05 (IAW05)  
West Point, USA, Juin 2005

### **From vulnerabilities to exploits : technical and legal issues**

F. RAYNAL, M. BAREL  
Eurosec 2005  
Paris, France, Mars 2005

### **Développement, sécurité et Logiciels Libres**

F. RAYNAL, C. BLANCHER  
Rencontres Africaines du Logiciel Libre (RALL)  
Ouagadougou, Burkina Faso, Nov. 2004

### **Methods for honeypot forensics**

F. RAYNAL, Y. BERTHIER, P. BIONDI, D. KAMINSKY  
Information Assurance Workshop 04 (IAW04)  
West Point, USA, Juin 2004

### **Honeypot forensics : a case study**

F. RAYNAL, P. BIONDI  
Eurosec 2004  
Paris, France, Mars 2004

**Covert Channels**

F. RAYNAL

Libre Software Meeting (LSM)

Metz, France, Juillet 2003

**(In)secure Programming**

F. RAYNAL

Libre Software Meeting (LSM)

Bordeaux, France, Juillet 2002

**About the links between cryptography and data hiding**

C. FONTAINE AND F. RAYNAL

Society for Imaging Science and Technology (IS&T) and International Society for Optical Engineering (SPIE)

San Jose, USA, Janvier 2002

**StirMark Benchmark : audio watermarking attacks**

M. STEINEBACH, F. A. P. PETICOLAS, F. RAYNAL, J. DITTMAN AND C. FONTAINE, C. SEIBEL, N. FATÈS

Information Technology : Coding and Computing (IEEE ITCC'2001)

Las Vegas, USA, Avril 2001

**A public automated web-based evaluation service for watermarking schemes : StirMark Benchmark**

F. A. P. PETICOLAS, M. STEINEBACH, F. RAYNAL, J. DITTMAN, C. FONTAINE, N. FATÈS

Society for Imaging Science and Technology (IS&T) and International Society for Optical Engineering (SPIE)

San Jose, USA, Janvier 2001

**Individual GP : an alternative viewpoint for the resolution of complex problems**

P. COLLET, E. LUTTON, F. RAYNAL, M. SCHONAUER

Genetic and Evolutionary Computation Conference (GECCO99)

Orlando, USA, Juillet 1999

**Manipulation of IFS attractors using Genetic Programming**

F. RAYNAL, P. COLLET, E. LUTTON, M. SCHONAUER

Congress on Evolutionary Computation (CEC99)

Washington DC, USA, Juillet 1999

# Autour de Linux et de la sécurité

## MISC

Num.	Titre
36	Attaques informationnelles sur Internet (en collaboration avec F. Gaspard)
HS1	L'information, nouveau nerf de la guerre ? (en collaboration avec F. Gaspard)
28	Nouveaux mécanismes de protection, nouvelles méthodes de contournement(en collaboration avec P. Bétouin, S. Duverger)
26	Attaquer les attaquants (en collaboration avec T. Holz)
20	Polymorphisme cryptographique : quand les <i>opcodes</i> se mettent la chirurgie esthétique
16	Eating Apple for fun & profit
13	Injection de code sous Unix (en collaboration avec P. Biondi, S. Dralet et Y. Fourastier)
12	Programmation cryptographique (en collaboration avec P. Junod)
) 10	Échange de clés avec Diffie-Hellman
7	Menaces informationnelles (en collaboration avec R. Bidou, P. Biondi, E. Detoisien)
6	Les insécurités du WEP (en collaboration avec E. Filiol)
5	Virux : les virus sous Unix (en collaboration avec S. Dralet)
	Tunnels avec le protocole SSH
4	Les dénis de services réseau (en collaboration avec V. Vuillard)
3	Manipulations avec le protocole ARP (en collaboration avec C. Blancher et E. Detoisien)
2	Exploitation automatique des bogues de format distants
1	Méthodes d'authentification du protocole HTTP
	Protections contre l'exploitation des vulnérabilités - 1 : introduction (en collaboration avec S. Dralet)
	Stéganographie : introduction (en collaboration avec F. A. Petitcolas et C. Fontaine)

## Hors Séries Linux Magazine France

Num.	Titre
17	Voyage au centre du kernel - Épisode II (Rédacteur en chef) – Linux Security Modules (en collaboration avec P. Biondi)
16	Voyage au centre du kernel - Épisode I (Rédacteur en chef)
13	Firewall, votre meilleur ennemi - Acte II (Rédacteur en chef) – Firewalk
12	Firewall, votre meilleur ennemi - Acte I (Rédacteur en chef)
8	La sécurité informatique (Rédacteur en chef) – Tests d'intrusion (en collaboration avec É. Detoisien) – Root-kits et intégrité

## Linux Magazine France - [www.linuxmag-france.org](http://www.linuxmag-france.org)

Num.	Titre
42	Programmation d'un sniffer : avec <code>/dev/bpf</code> (sous BSD), avec les sockets de type <code>PF_PACKET</code> (sous Linux), et avec <code>libpcap</code> (en collaboration avec C. Grenier)
39	Dossier spécial les patches Openwall et PaX pour la sécurité du noyau (en collaboration avec S. Dralet) Programmation sécurisée (en collaboration avec C. Blaess et C. Grenier) – Introduction, UID/EUID, exécution de commandes externes – Organisation de la mémoire, pile et fonctions, shellcode
23 à 28	– Débordements de buffer : les exploiter, les éviter – Bogue de format : les exploiter, ne plus utiliser de NOP dans son shellcode, exploitation de la section <code>.ctors</code> – Les "race conditions" et les fichiers temporaires – Les scripts CGI
22	Gérer ses connexions avec <code>xinetd</code>
21	Dossier spécial sur IPv6 (en collaboration avec M. Souissi)
20	La sécurité avec Bastille-Linux
19	Les secrets de NFS
16 à 18	Trilogie sur les Yellow Pages (NIS) sous Linux
15	<code>automount</code> et <code>autofs</code>