Florent Chabaud

né en 1970
marié, un enfant

28, rue Ernest Renan
75015 Paris
fax : 06 84 75 00 14
mél : florent.chabaud@polytechnique.org
www : http://www.carva.org/florent.chabaud

Expérience

- sept 2004- : Sous-directeur scientifique et technique à la Direction Centrale de la Sécurité des Systèmes d'Information.
  - Encadrement des trois laboratoires : Technologies de l'information, Cryptographie, Signaux compromettants.
  - Coordination de la cellule d'assistance technique en conception (AsTeC) et des travaux de rédaction du référentiel technique de la DCSSI (mécanismes cryptographiques, gestion des clés cryptographiques, authentification).
  - Président du groupe de travail interministériel de rédaction du rapport d'orientation des travaux de recherche et développement en matière de sécurité des systèmes d'information
  - Président du comité de pilotage de l'appel à projet SETIN 2006 de l'Agence Nationale de la Recherche.
  - Président du comité de programme du séminaire CESAR 2007.
- sept 2000-août 2004 : Chef du laboratoire des technologies de l'information à la Direction Centrale de la Sécurité des Systèmes d'Information.
  Coordination des études sur différents thèmes techniques dans le domaine de la SSI :
  - Interconnexion de réseaux IP ;
  - Sécurité locale des postes de travail ;
  - Machines virtuelles ;
  - Protocoles réseaux ;

  Enseignements au centre de formation à la sécurité des systèmes d'information (Unix et C, sécurité des postes physiques).
- juil 1997-août 2000 : Ingénieur de l'Armement au CELAR (CASSI/CA) : coordinateur technique sécurité du projet d'armement MUSE (Messagerie Universelle Sécurisée) comprenant notamment les aspects :
  - Expression des objectifs de sécurité d'un système apte à gérer des informations de haute sensibilité (FEROS par la méthode EBIOS).
  - Conception globale de la sécurité du système. Enoncé des exigences et des spécifications des systèmes de sécurité réalisés (carte PCMCIA, logiciel de sécurisation de la messagerie, infrastructure de clés publiques (AC, AE,...), sécurisation locale des postes).
  - Rédaction de la politique de sécurité des systèmes MUSE et IGC (Infrastructure de Gestion des Clés).
  - Réalisation, développement, déploiement et mise en place de l'infrastructure de gestion des clés publiques (politique de certification, profils de certificats X.509)
  - Gestion des contraintes d'interopérabilité avec les systèmes existants et futurs, notamment de l'OTAN.

    - Préparation du déploiement par la définition d'architectures sécurisées des réseaux de télécommunications.
    - Préparation de l'évaluation de sécurité des produits réalisés (Profils de protection, Critères Communs).
- sept 1996-juin 1997 : Ingénieur de l'Armement au CELAR, chargé d'études cryptographiques (CASSI/SCY/EC).
- 1993-1996 : Thèse de doctorat d'informatique de l'Ecole Polytechnique effectuée dans le Laboratoire d'Informatique de l'ENS (LIENS) au Groupe de Recherche En Complexité et Cryptographie (GRECC) : Recherche de performance dans l'algorithmique des corps finis. Applications à la cryptographie.

Etudes

- 1989-1992 : Ecole Polytechnique. Corps de l'armement (DGA).
- 1992-1994 : Ecole d'application du corps de l'armement : Ecole Nationale Supérieure de Techniques Avancées.
- 1992-1993 : En parallèle avec la scolarité de l'ENSTA, DEA Informatique Mathématiques et Applications, filière Complexité et Cryptographie (mention bien).
- 1993-1996 : Thèse de doctorat en informatique. Mention très honorable avec félicitations.

Recherche

Thème	Référence
Sécurité locale	Contrôle d'intégrité de la séquence de démarrage d'un ordinateur, F. Chabaud, and N. Cuillandre, extended abstract published in SECI'02, 2002.
Fonctions de hachage	Differential collisions in SHA-0, F. Chabaud, and A. Joux, extended abstract published in CRYPTO'98, H. Krawczyk ed., LNCS 1462, pp 56--71, 1998.
Cryptanalyse	Recherche de performance dans l'algorithmique des corps finis. Applications à la cryptographie., Thèse de doctorat, Ecole Polytechnique, Oct. 1996. (in french)
Calculs arithmétiques dans les extension d'anneaux finis	Bibliothèque de programmation ZEN (travail commun avec R. Lercier).
	A new algorithm for finding minimum-weight words in a linear code: Application to primitive narrow-sense BCH codes of length 511.,

Codes correcteurs d'erreur	A. Canteaut, and F. Chabaud published in IEEE Trans. Inform. Theory, 44(1):367--378, jan 1998. Preliminary version: Rapport de recherche 2685, INRIA, oct 1995.
Codes algébriques de Gabidulin	The cryptographic security of the syndrome decoding problem for rank distance codes, F. Chabaud, and J. Stern, extended abstract published in Advances in Cryptology: ASIACRYPT '96, volume 1163 of LNCS, pages 368--381. Springer-Verlag, 1996.
Cryptanalyse linéaire et différentielle	Links between differential and linear cryptanalysis, F. Chabaud, and S. Vaudenay, extended abstract published in A. de Santis, editor, Advances in Cryptology: Proceedings of EUROCRYPT'94, volume 950 of LNCS, pages 356--365. Springer-Verlag, 1995. Preliminary version: Report LIENS-94-3

Pour une liste plus détaillée de mes publications ou pour les télécharger cliquer ici

---

Informatique

- Langages C, BASH, TCL/TK, HTML, PHP, TCSH, AWK, PERL, LISP, PASCAL, C++, LEX, YACC, EXCEL, SQL, SPIP, XML...
- Systèmes Unix (linux), Windows 9x, 2000, XP

Langues

- Anglais : Conversation courante et technique.
- Allemand : Conversation élémentaire.

Loisirs

- Natation, Musique Lyrique, MX5.