



Mardi 24 mars 2015 de 14h30 à 17h30

Académie des sciences – Grande salle des séances
23 quai de Conti, Paris 6^e

SÉCURITÉ DES SYSTÈMES INFORMATIQUES : MYTHES, RÉALITÉS ET PERSPECTIVES

Organisé par **Maurice NIVAT** et **Joseph SIFAKIS**, de l'Académie des sciences

14h30 Introduction

Maurice NIVAT, *professeur honoraire à l'université Paris Diderot, Académie des sciences*

14h45 Cyber-sécurité : problématique et défis scientifiques, technologiques et sociétaux

Claude KIRCHNER, *directeur de recherche Inria, Conseiller du Président d'Inria, Paris*

15h15 Défis de recherche récents en cryptologie et en sécurité de l'information

David NACCACHE, *professeur à l'université Panthéon-Assas, Paris II et membre du laboratoire informatique de l'ENS*

15h45 La sécurité des grands systèmes informatisés

Jacques PRINTZ, *professeur émérite du Cnam, Chaire de Génie Logiciel - Membre de l'Institut de la Transformation Numérique des Entreprises (ITNE), Paris*

16h15 Cybersécurité : de la souveraineté de l'Etat à la défense du citoyen

Guillaume POUPARD, *directeur général de l'agence nationale de la sécurité des systèmes d'information, Paris*

16h45 - 17h30 Débat

JOSEPH SIFAKIS, *directeur de recherche émérite au CNRS, professeur à l'Ecole Polytechnique Fédérale de Lausanne, Académie des sciences*



Cyber-sécurité : Problématique et défis scientifiques, technologiques et sociétaux

Claude KIRCHNER

La sécurité des systèmes d'information ou cyber-sécurité est au cœur de l'informatisation globale de notre société, elle constitue donc un enjeu fondamental pour la citoyenneté, la compétitivité industrielle et la souveraineté des nations. En étant au cœur de toutes les infrastructures critiques (énergie, eau, communication, finance, ...) et de toutes les organisations, la cyber-sécurité joue un rôle crucial comme le montrent les nombreuses failles révélées ces dernières années, laissant entrevoir les conséquences dramatiques de sa non-maîtrise tant pour les citoyens que pour les entreprises ou les états. Dans ce contexte, cette présentation donnera des exemples de problèmes de cyber-sécurité qui peuvent se poser et des questions de recherche qui en découlent.

Défis de recherche récents en cryptologie et en sécurité de l'information

David NACCACHE

Lors de cet exposé, nous allons présenter quelques-uns des principaux défis scientifiques en cryptologie et sécurité de l'information. En particulier nous expliquerons le chiffrement pleinement homomorphe, le chiffrement fonctionnel et l'obfuscation indistinguable. Enfin, nous soulignerons les enjeux de mise en œuvre de ces technologies et leurs impacts sociétaux.

La sécurité des grands systèmes informatisés

Jacques PRINTZ

Dans cet exposé nous définirons ce qu'est aujourd'hui un grand système informatisé, en prenant des exemples dans le monde Défense-Sécurité et/ou Énergie. Nous montrerons que la sécurité est tout à la fois un problème technique difficile compte tenu de la transversalité de la notion de sécurité et de l'état des technologies de l'information et de la communication, mais aussi un problème de sociologie des organisations et des usagers compte tenu de la maturité des populations qui gravitent étroitement autour de ces systèmes, et en premier lieu les équipes d'ingénierie avec leurs milliers d'ingénieurs. Nous devons et devons vivre avec les erreurs inévitables, en limitant leurs conséquences néfastes et en minimisant les risques pour les usagers et l'environnement.

Cybersécurité : de la souveraineté de l'Etat à la défense du citoyen

Guillaume POUPARD

Le rapide développement des menaces informatiques, corollaire du formidable développement des technologies et nouveaux usages liés au numérique, pose des questions essentielles et parfois originales pour la sécurité de la Nation. Au-delà des questions classiques mais néanmoins fondamentales liées à la souveraineté, les questions de cybersécurité doivent être appréhendées dans de nombreux domaines, celui de la recherche, celui des entreprises ainsi qu'à l'échelle du citoyen. Une approche à la fois globale, ambitieuse, pragmatique et adaptée à chaque cible doit être conduite par les nombreux acteurs concernés afin de relever les formidables défis qui s'offrent à nous.