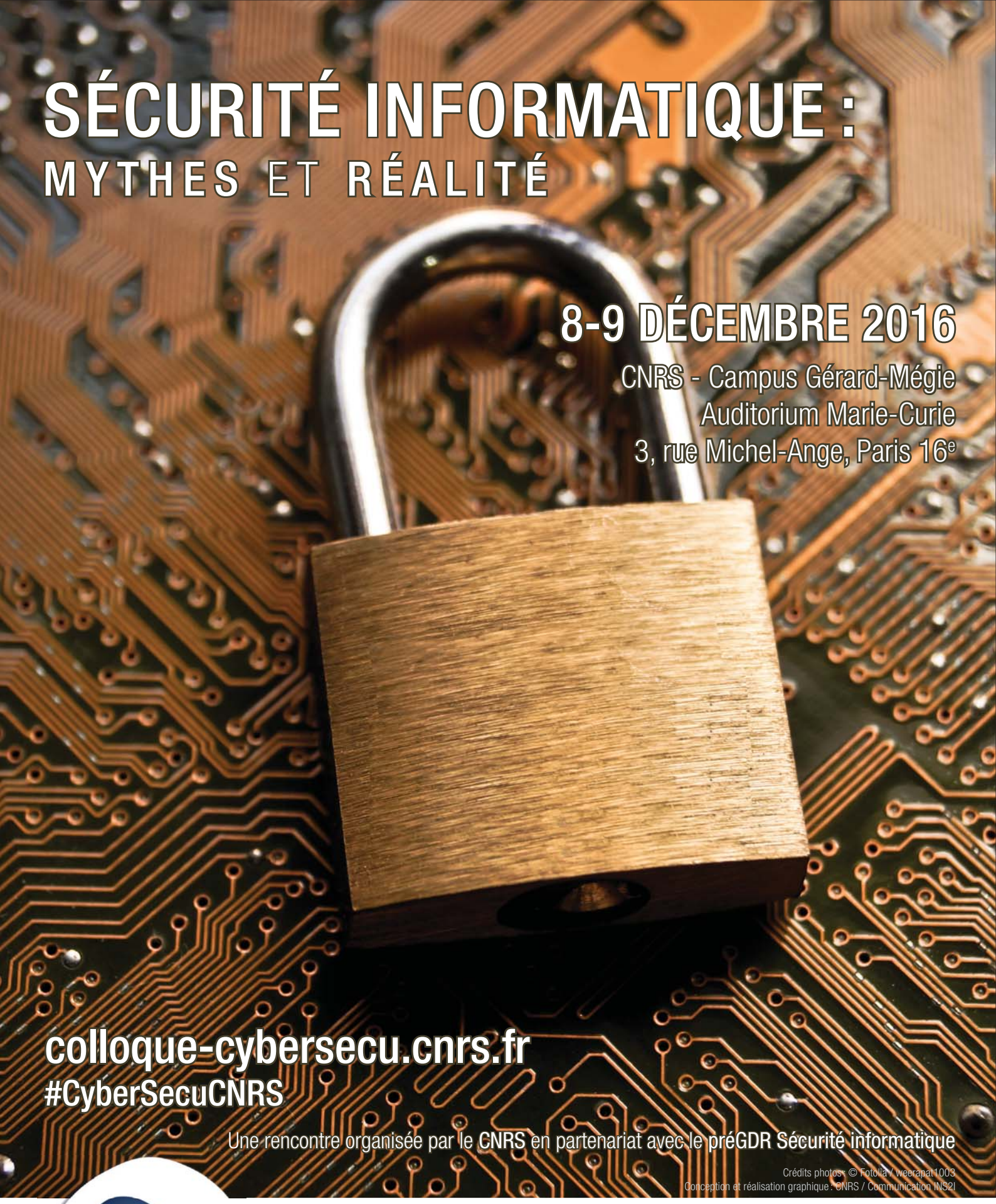
SÉCURITÉ INFORMATIQUE :
MYTHES ET RÉALITÉ



8-9 DÉCEMBRE 2016

CNRS - Campus Gérard-Mégie
Auditorium Marie-Curie
3, rue Michel-Ange, Paris 16e

colloque-cybersecu.cnrs.fr
#CyberSecuCNRS

Une rencontre organisée par le CNRS en partenariat avec le préGDR Sécurité informatique

Conception et réalisation graphique : CNRS / Communication INS2I

cnrs
www.cnrs.fr

COLLOQUE SÉCURITÉ INFORMATIQUE :
MYTHES ET RÉALITÉ

La sécurité du numérique est une discipline scientifique récente, à la croisée des mathématiques, de l'informatique et de l'électronique. Bien qu'omniprésente dans notre société connectée, sa technicité la rend mystérieuse à qui n'a jamais tenté de pénétrer ses secrets. **L'actualité quotidienne place pourtant la sécurité du numérique aux avant-postes des préoccupations** : fuite de données personnelles et espionnage économique, infection de systèmes informatiques sensibles, usurpation d'identité et craintes vis-à-vis des paiements par carte ne sont que quelques exemples qui hantent les actualités. À travers ce flux d'information continue et massif, il est difficile d'appréhender sereinement la portée des problèmes et de leurs solutions.

Seize questions pragmatiques ont été posées à des chercheurs de la sécurité du numérique pour aider tout un chacun à distinguer les mythes de la réalité. Ces questions reflètent des préoccupations majeures de notre société sur son présent et son avenir. Qui ne s'est en effet jamais interrogé sur la valeur des données à caractère personnel, sur la robustesse des mots de passe ou la possibilité de voter avec un téléphone portable ? Ces experts auront chacun quarante minutes pour exposer le contexte de la question qui leur a été posée, présenter leur point de vue scientifique et répondre aux questions de l'auditoire.

Ce colloque, incontestablement orienté vers la société, vise les acteurs institutionnels et industriels, mais aussi les scientifiques issus de champs disciplinaires variés, sans exclure le grand public déjà sensibilisé à la thématique. Comprendre ce qui est possible aujourd'hui et ce qui le sera demain, exprimé dans des termes compréhensibles aux non-experts, est l'objectif qui a été fixé à ces quinze chercheurs. Reconnus internationalement, médaillés de prix prestigieux, membre de l'Institut Universitaire de France ou lauréats de récompenses internationales, ils ont tous acceptés de relever le défi, de se prêter à l'exercice difficile de répondre avec des mots simples à une question sur leur domaine de recherche, sans perdre la rigueur scientifique qui les caractérise.

PROGRAMME

Jeudi 8 décembre

9h20 - 9h40

Ouverture du colloque

Michel Bidoit

9h40 - 10h

Panorama de la sécurité informatique

Gildas Avoine

SÉCURITE DES SYSTÈMES LOGICIELS

10h - 10h40

De la puce au cloud, comment fonctionne l'expertise judiciaire ?

David Naccache

10h40 - 11h10 - Pause

11h10 - 11h50

Pourra-t-on un jour éradiquer les virus informatiques ?

Jean-Yves Marion

11h50 - 12h30

Pourquoi chiffrer les informations ne suffit pas ?

Stéphanie Delaune

12h30-14h - Déjeuner

PROGRAMME

Jeudi 8 décembre

PROTECTION DES DONNÉES PERSONNELLES

14h - 14h40

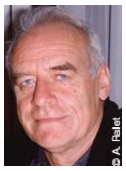
La génomique va-t-elle briser la sphère privée ?

Jean-Pierre Hubaux

14h40 - 15h20

Quel futur pour les mots de passe ?

Christophe Rosenberger



15h20 - 16h

Peut-on vendre des données personnelles ?

Alain Rallet

16h - 17h

Table ronde :

Les données privées ont-elles un avenir ?

Jean-Pierre Hubaux / Bart Preneel / Christophe Rosenberger / Alain Rallet, animée par Marc-Olivier Killijian

17h - 17h30 - Pause

17h30 - 18h10

Y a-t-il une ère post-Snowden ?

Bart Preneel

PROGRAMME

Vendredi 9 décembre

9h - 9h20

Ouverture de la journée

Alain Fuchs

VOL DE DONNÉES

9h20 - 10h

Comment prévenir l'usurpation d'identité ?

Éric Freyssinet

10h - 10h40

Comment protéger les droits d'une image ou d'un film ?

Patrick Bas

10h40 - 11h10 - Pause

CRYPTOGRAPHIE

11h10 - 11h50

Le chiffrement homomorphe constitue-t-il une révolution ?

Damien Stehlé

11h50 - 12h30

Quelle sécurité pour le cloud ?

David Pointcheval

12h30 - 14h - Déjeuner

PROGRAMME

Vendredi 9 décembre

14h - 14h40

Sommes-nous prêts pour l'ère post-quantique ?

Antoine Joux

14h40 - 15h20

Pourquoi essaie-t-on de casser les fonctions cryptographiques ?

María Naya-Plasencia

15h20 - 15h50 - Pause

PREUVES DE SÉCURITÉ

15h50 - 16h30

Voter de façon sûre par Internet : opportunité ou illusion ?

Steve Kremer

16h30 - 17h10

Peut-on prouver la sécurité des communications ?

Hubert Comon

PLUS D'INFORMATIONS,
ENTRÉE LIBRE SUR INSCRIPTION :
colloque-cybersecu.cnrs.fr

Suivez le colloque sur Twitter :
#CyberSecuCNRS