LA VÉRIFICATION FORMELLE APPLIQUÉE AUX PROTOCOLES CRYPTOGRAPHIQUES

le 27 septembre 2016 15h30 - 17h00

ENS Rennes, Salle du conseil
Plan d'accès

Dans le cadre d'un séminaire du département Informatique et télécommunications : Intervention de Stéphanie Delaune, directrice de recherche (DR) CNRS à l'IRISA, membre de l'équipe EMSEC qui s'intéresse à la sécurité et la cryptographie embarquées.

Cet exposé présentera la problématique de la sécurité des protocoles cryptographiques et l'application à ce domaine des techniques de logique mathématique et de vérification automatique / assistée.

Résumé
Les protocoles cryptographiques sont les algorithmes et programmes qui permettent d'établir une communication sécurisée. Ils sont fragiles et sont le principal point d'entrée pour les attaques de sécurité, comme le montreront quelques exemples. Ils sont aussi très difficiles à analyser. La preuve formelle est de plus en plus vue comme le meilleur moyen (voire le seul) d'assurer le bon fonctionnement de ces protocoles. Elle demande souvent la mise en œuvre de techniques très élaborées.

https://www.irisa.fr/fr/equipes/emsec

THÉMATIQUE(S)

Formation, Recherche - Valorisation

CONTACT

David Cachera & François Schwarzentruber

CONTACT

Raphaël Truffet

ARCHIVES