Véronique Cortier
18 mai 2011

Comment prouver la sécurité des protocoles cryptographiques ?

Résumé:

De nombreux dispositifs électroniques visent à améliorer la sécurité des échanges sur des réseaux ouverts comme Internet. Ces dispositifs, tels que les protocoles cryptographiques, reposent souvent sur le chiffrement des données et plus généralement sur des fonctions cryptographiques. Chiffrer les données sensibles est cependant loin d'être suffisant pour assurer la sécurité des communications. Ainsi, les protocoles cryptographiques peuvent comporter des failles subtiles, qui ne sont révélées que plusieurs années après. Il est donc nécessaire de concevoir des techniques rigoureuses pour analyser la sécurité de systèmes électroniques comme les protocoles. Est-il possible d'aller plus loin et de prouver la sécurité d'un système, quel que soit le comportement d'adversaires malicieux ?
Nous verrons dans quels cadres (ou modèles) des preuves de sécurité sont possibles. Nous évoquerons ainsi les modèles symboliques, où les messages sont représentés par des objets abstraits et les modèles cryptographiques, où les messages sont représentés beaucoup plus fidèlement. Les premiers offrent un cadre simplifié, plus accessible à la preuve tandis que les seconds offrent des garanties de sécurité plus fortes. Nous illustrerons nos propos avec un exemple important : les protocoles de vote électronique.