David Pointcheval
27 avril 2011

Quelles garanties nous apporte la cryptographie ?

Résumé:

La cryptographie vient à notre secours pour de nombreux problèmes de sécurité, et notamment l'authentification, la confidentialité et l'anonymat. Mais pour des raisons d'efficacité, le surcoût induit par la cryptographie, et la sécurité en général, doit être minimal tout en garantissant une protection adéquate. Ces primitives cryptographiques, que sont le chiffrement pour la confidentialité ou la signature pour l'authentification, sont également sollicitées dans de nombreux protocoles complexes. Des propriétés spécifiques sont attendues pour pouvoir garantir la sécurité globale.

La "sécurité prouvée" tente d'apporter une réponse à l'évaluation de la sécurité et du même coup au dimensionnement des systèmes et au choix des paramètres. Ces derniers ont ensuite un impact immédiat sur le coût en termes de puissance de calcul. La "sécurité prouvée" permet en effet de quantifier le temps de calcul d'un attaquant, pour mettre en défaut le système, en fonction de ses ressources et de la taille des paramètres. Pour cela, il faut définir précisément ce que l'on attend d'un schéma cryptographique et contre quelles menaces il doit protéger : quel type d'information l'attaquant veut-il compromettre et quels moyens est-il prêt à mettre en œuvre ?

On illustrera cela avec la confidentialité des données et le chiffrement asymétrique.