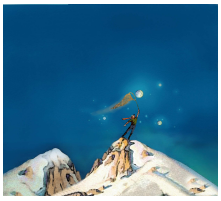

printemps des sciences
Avec le soutien de la Ministre de l'Enseignement supérieur et de la Recherche scientifique

Sciences extrêmes 19 - 25 mars 2007

PROTOCOLES D'IDENTIFICATION

Nadia Kabbali
Département d'Informatique

Le besoin d'identification ne date pas d'hier, l'histoire est pleine de récits relatifs à ce besoin. A une époque où la signature et la carte d'identité n'existaient pas encore, la preuve d'identité passait nécessairement par la reconnaissance physionomique, la connaissance d'un secret ou encore la possession d'un objet. Comme le besoin d'identification, le besoin de tromper le contrôleur a également toujours existé.

Aujourd'hui il en va de même : nous devons à plusieurs reprises prouver notre identité durant une journée (avec notre carte d'identité, différents abonnements, …).
Lorsque nous quittons le monde réel pour pénétrer dans le monde des technologies de l'information, nous ne sommes plus confrontés à des hommes mais à des machines; ce sont ces machines qui prennent dès lors la décision de refuser ou d'accepter l'identité d'une entité (personne ou machine). Pour permettre aux machines de prendre la bonne décision, l'homme a développé des protocoles (règles de communication) d'identification.

Chacun de nous est confronté à de tels protocoles où qu'il aille et quoi qu'il fasse, dans des utilisations diverses comme :

- le retrait de billets dans un distributeur de billets grâce à une carte et un code PIN (*Personnal Identification Number*),
- l'accès aux opérations bancaires à partir de chez soi grâce à un service de banque par internet et à une calculette fournie par la banque (*digipass*),
- login à son service de courrier électronique au moyen d'un nom d'utilisateur (*login*) et d'un mot de passe (*password*). Ces protocoles ne cessent d'évoluer pour rendre l'identification plus fiable,
- …

L'un des premiers protocoles d'identification utilisés dans le monde informatique et qui reste jusqu'à aujourd'hui, malgré ses faiblesses, l'un des protocoles les plus utilisés est le **mot de passe**.

Il existe, malgré tout, beaucoup d'autres types de protocole d'identification en application aujourd'hui, moins répandu que le précédent pour des raisons de coûts mais qui deviennent indispensables lorsque l'application à laquelle ils sont destinés demande un haut degré de sécurité.

Mon rapport explique les principes généraux de ces différents types de protocole et détaille le fonctionnement de certains d'entre eux.