Ecole d'ingénieurs
du Canton de Vaud

Tél. : + 41 24 423 21 11
Fax : + 41 24 425 00 50

info@eivd.ch
http://www.eivd.ch

Travail de diplôme 2004

Département Electricité et Informatique

Ecole d'ingénieurs du Canton de Vaud
Route de Cheseaux 1, case postale
CH - 1401 Yverdon - les - Bains

Développement d'un outil de cryptage de disque dur intégré à une carte d'authentification forte

Pourquoi ce travail de diplôme

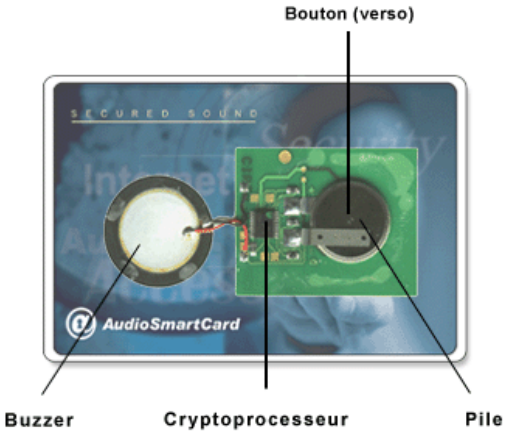
La problématique de l'informatique nomade ou "mobile computing" se caractérise principalement par des problèmes de sécurité. Ces problèmes sont liés à l'accès à distance du réseau d'entreprise, mais aussi à la protection des données sur le PC portable. Autant des solutions d'authentification pour l'accès distant se trouvent aujourd'hui sur le marché, autant les solutions de cryptage et de sécurisation du disque dur par authentification forte ne sont aujourd'hui pas satisfaisantes. Ce projet cherche à résoudre ce problème en développant un outil de cryptage de disque dur intégré à une carte d'authentification forte (AudioSmartCard).

PGPDisk

Pour le cryptage du disque dur, le logiciel PGPDisk a été choisi. Ce logiciel permet de chiffrer un répertoire de taille fixe. Ce répertoire peut être vu comme un disque dur. Ce disque est en permanence entièrement chiffré, si bien que pour l'utilisateur, l'accès à un fichier protégé se fait de la même manière que n'importe quel fichier. La seule différence que l'utilisateur peut voir entre un disque normal et un disque PGP est le fait qu'il doit s'authentifier lors du montage du disque PGP.

AudioSmartCard

La technologie AudioSmartCard permet des authentifications sécurisées par le biais d'une séquence sonore dynamique. Cette séquence est créée dans une carte à puce par un générateur aléatoire et un crypto processeur ce qui assure que le signal ne puisse être créé sans la carte. L'authentification se fait par un serveur dédié qui est capable de reconnaître la séquence sonore puis de définir si cette séquence correspond bien au propriétaire de la carte. Pour renforcer l'authentification de la personne, un code PIN peut être ajouté.



But du travail

Le but de ce travail est d'utiliser la carte d'authentification AudioSmartCard pour l'authentification de la personne lors du montage d'un disque PGP. Pour ce faire il a été indispensable de comprendre les technologies mises en œuvre, les solutions existantes ainsi que les concepts de sécurité informatique, cryptographie d'authentification etc...

Auteur: **Schmidt David**
Répondant externe:
Prof. responsable: **Buchs Christian**
Sujet proposé par: **Adventis Communications Engineering SA**

Hes·so
Haute Ecole Spécialisée de Suisse occidentale