heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

Tél. : 024 557 63 30
Fax : 024 557 64 04

info@heig-vd.ch
http://www.heig-vd.ch

Travail de diplôme 2005

Département Electricité et Informatique

HEIG-VD
Route de Cheseaux 1
CH - 1401 Yverdon-les-Bains

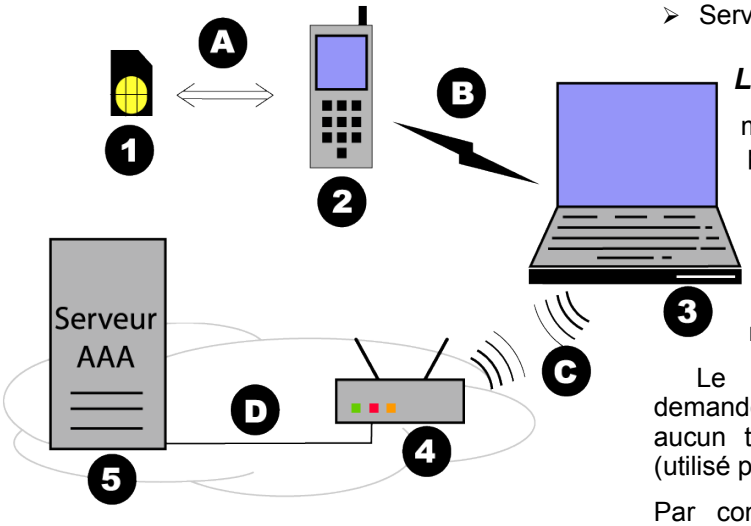
Développement d'un gateway d'authentification avec RADIUS, utilisable avec un Natel ou une carte SIM comme client

L'authentification

met en oeuvre des mécanismes permettant de s'assurer de l'identité d'une personne. En utilisant simplement un nom d'utilisateur et un mot de passe, l'authentification est faible.

Les réseaux GSM (téléphonie mobile) utilisent une carte SIM pour l'authentification. Le système est réputé sûr.

EAP-SIM utilise les même principes que GSM en les adaptant pour les réseaux de données et renforce même sur certains points le niveau de sécurité. Il est une extension d'un protocole plus général, EAP (Extensible Authentication Protocol) qui utilise différents supports comme 802.1x ou RADIUS pour transiter à travers le réseau.



Le travail de diplôme

visait donc à étudier le protocole EAP-SIM et voir comment cette méthode pouvait permettre une authentification sûre d'un ordinateur, moyennant l'utilisation d'un objet très répandu, le Natel. Il a également fallu évaluer sa mise en place tout au long de la chaîne allant de la carte SIM au serveur AAA (voir illustration).

Les technologies et protocoles

nécessaires pour un tel projet sont très variés:

- Java Card pour les applications sur la carte SIM (1).
- Le protocole APDU pour les transmissions (A) entre la SIM et le téléphone.
- J2ME et sa nouvelle API SATSA (JSR-177) sur le mobile (2).
- Bluetooth (B) pour la communication vers l'ordinateur (3).
- 802.1x pour la liaison (C) avec le point d'accès (AP) Wi-Fi (4).
- Le protocole RADIUS (D) pour les échanges avec le serveur.
- Serveur AAA (5) (FreeRADIUS)

Les résultats

montrent que le protocole EAP, et en particulier EAP-SIM, peut être utilisé d'un bout à l'autre, moyennant la définition d'encapsulation EAP pour Bluetooth (B) et APDU (A). En créant une application sur mesure, la carte SIM peut effectuer tout le traitement nécessaire au protocole EAP-SIM

Le déploiement d'un tel système demandera encore un peu de patience car aucun téléphone actuel implémente SATSA (utilisé pour communiquer avec la SIM).

Par conséquent, le projet s'est finalement recentré, pour la partie développement, sur le une autre extension EAP, EAP-MD5. Le système actuel stoque le mot de passe sur le téléphone portable et le communique via Bluetooth au PC. Ceci pourra servir de base à un prochain projet visant à implémenter l'authentification EAP-SIM .

Auteur: **Raphael KOENG**
Répondant externe:
Prof. responsable: **Juergen EHRENSBERGER**
Sujet proposé par: **HEIG-VD/IICT**

Hes·so
Haute Ecole Spécialisée
de Suisse occidentale