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

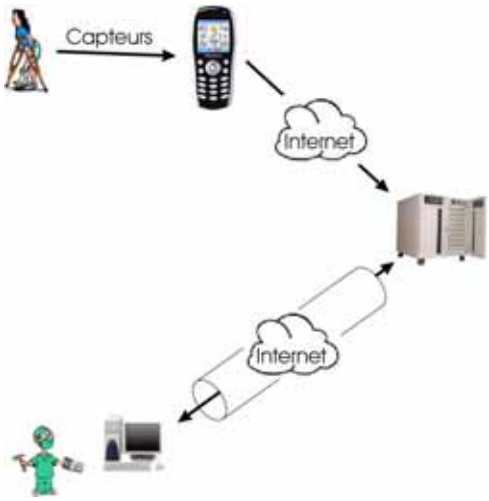
Personal Assistance Networks. Télésurveillance de patients en milieu non hospitalier

Principe du projet :

On a pu remarquer ces dernières années l'explosion des coûts pour la santé. Beaucoup de pathologies nécessitent une surveillance constante afin de pouvoir réagir en cas de problèmes. Hélas cette surveillance doit se faire en milieu hospitalier.

Equipé d'un téléphone portable GSM et d'un réseau de capteurs, le patient est surveillé en permanence et envoie automatiquement les paramètres mesurés (température, pression sanguine, ECG) via Internet sur un serveur.

En cas d'alarme, un médecin est alerté et il pourra aller consulter les données du patient via Internet.



Consultation sécurisée :

Les données sur les patients résidant sur le serveur sont des données hautement sensibles et on besoin d'une protection particulière au niveau de l'accès aux données et de la transmission.

Mon travail de diplôme consiste à mettre en œuvre ce qu'il faut pour garantir cette confidentialité.

Consultation via un tunnel :

Le but était de pouvoir utiliser des services Web classiques (Browser Internet, Serveur Web CMS) sans devoir développer des systèmes propriétaire pour l'accès aux données et l'affichage de celles-ci.

C'est dans cet état d'esprit que l'idée du tunnel est venue. Au lieu de se connecter directement sur le service Web, on se connecte au tunnel qui lui établit une ligne crypté avec une authentification forte.

Authentification avec RSA :

L'authentification utilise la paire de clefs asymmétriques de RSA pour une authentification forte sans failles. La demande d'authentification du client par exemple ne peut être décryptée en dehors du serveur (et le serveur sait de qui elle vient). La réponse du serveur ne peut que provenir du serveur, et seul le client concerné est capable de la décrypter.

Transmission de données cryptées AES :

Le cryptage asymmétrique a un énorme désavantage par rapport au cryptage symmétrique : le temps de calcul pour traiter les données. Pour pallier à ce problème, une fois l'authentification réussie, le tunnel crypte les données avec AES (succésseur à DES), ce qui limite fortement le besoin de ressources en temps processeur. L'échange de clefs se fait durant l'authentification.

Auteur: **Bouvier Patrice**
Répondant externe:
Prof. responsable: **Jaton Markus**
Sujet proposé par: **EIVD (institut TCOM) et FRBT (Fédération romande de télé-vigilance)**

Hes·so
Haute Ecole Spécialisée de Suisse occidentale