Une clé personnalisée pour sécuriser les connexions mobiles

- Informatique - Sécurité Informatique -

Date de mise en ligne : vendredi 6 novembre 2009

Le DAIICT a mis au point un système de cryptographie qui repose sur l'installation, l'enregistrement et l'échange de clés authentifiées. Celui-ci verrouille les réseaux GSM lors de l'échange de données sensibles.

L'utilisation des téléphones portables comme plate-forme de paiement, de m-banking ou d'emails crée de nouveaux défis en terme de sécurité. Défis auxquels les protocoles de sécurisation actuels des réseaux GSM ne répondent pas, estiment des chercheurs indiens du DAIICT*. C'est pourquoi ils proposent un protocole de cryptographie reposant sur l'identité de l'utilisateur comme clé publique. C'est à dire que l'on crée une clé de chiffrement propre à chaque mobile, ce qui rend inutile la certification des clés publiques. Le protocole consiste en trois phases : l'installation, l'enregistrement et l'échange de clés authentifiées. Lors de l'installation, une clé propre à chaque abonné est générée.

Echange de clé temporaire

Celle-ci est chargée dans la carte SIM de l'appareil et une copie est stockée par le serveur d'authentification lors de l'enregistrement à un service mobile. Ces deux étapes ne se produisent qu'une seule fois. Elles permettent au mobile et au serveur de s'authentifier à chaque connexion. Une fois authentifiés, ils procèdent à un échange de clé temporaire qui sera utilisé pour sécuriser les données transmises durant cette session. Cette phase d'échange de clés est une opération dynamique qui se fait à chaque fois que cela est nécessaire.

Cryptographie symétrique ou asymétrique

D'après les chercheurs, l'avantage d'un tel protocole est qu'il ne consomme que peu de ressources informatique de l'appareil. Il n'est pas non plus nécessaire de créer un canal dédié entre les services proposés par l'opérateur et les serveurs réseaux. Jusqu'à présent, la plupart des protocoles de sécurisation des réseaux GSM reposaient sur la cryptographie symétrique, par opposition à la cryptographie à clé publique. La méthode proposée par les chercheurs se situe à l'intersection de ceux deux protocoles.

* *Dhirubhai Ambani Institute of Information and Communication Technology*

Post-scriptum :

http://www.atelier.fr/securite/10/0...