La carte à puce

EAP-TLS

Une solution de sécurité forte

pour les réseaux Wi-Fi

utilisant des infrastructures à clés publiques.

Pascal Urien

Juin 2004

Introduction aux réseaux Wi-Fi

L'engouement des marchés informatiques pour les réseaux sans fil 802.11 (ou encore *Wi-Fi*) est freiné par l'absence d'infrastructures de sécurité standardisées et inter-opérables. A l'origine, les réseaux 802.11 ne sont que le prolongement naturel de réseaux câblés (Ethernet), l'utilisation de liens radio augmente le temps de connexion des internautes et accroît leur profitabilité économique ; elle répond au besoin naturel d'accéder au réseau de manière diffuse et transparente.

Infrastructure à clés publiques.

Beaucoup d'entreprises ou d'administrations exigent en pré-requis au déploiement du Wi-Fi l'assurance d'un niveau de sécurité élevé, basé par exemple sur des infrastructures à clés publiques (ou Public Key Infrastructure). Le principe est simple, l'entreprise dispose d'une autorité de certification (CA) qui s'est auto-délivré un certificat (le certificat racine ou *Root Certificate*). Cette autorité de certification délivre des certificats aux serveurs RADIUS d'authentification et aux utilisateurs du réseau sans fil, la figure 1 illustre cette procédure.

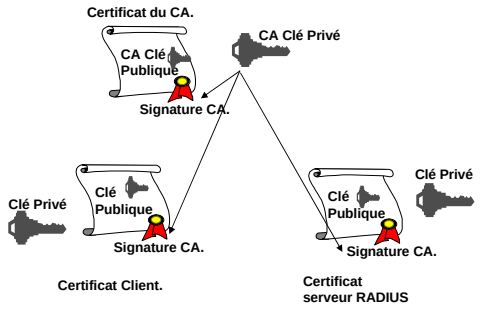


Figure 1. Principe d'une infrastructure à clé publique

Défauts de sécurité des plateformes standards.

A titre d'exemple nous examinons l'architecture de sécurité proposée par la plateforme logicielle *Windows 2003 Server*. Elle intègre un serveur baptisé IAS qui réalise les fonctions de serveur PKI (A) et de serveur d'authentification RADIUS (B). Le serveur d'authentification dispose d'un certificat, et de manière analogue le serveur PKI délivre des certificats aux utilisateurs du réseau sans fil (C). Un terminal (D) connecté au réseau Wi-Fi de l'entreprise est configuré avec d'une part le certificat racine, et d'autre part un certificat client et sa clé privée associée (figure 2).

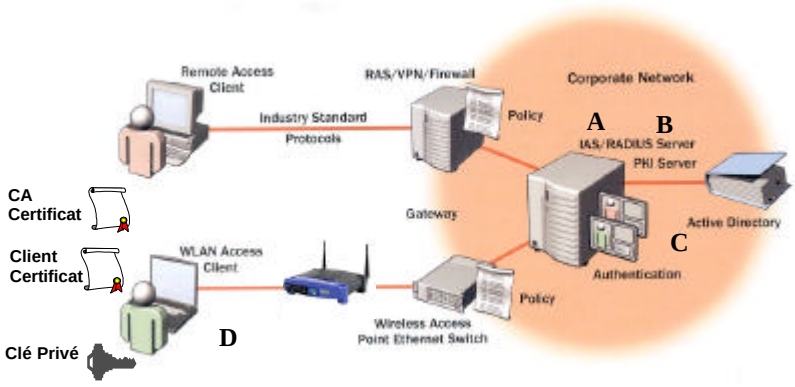


Figure 2. La plateforme *Windows Server 2003*

Nous allons à présent analyser les points de sécurité critiques rencontrés lors de l'installation et de l'usage de certificats , côté terminal client.

1- Les certificats clients sont généralement émis au format PKC12, dans lequel la clé privée est protégée à l'aide d'un mot de passe. La connaissance de cette information permet d'extraire cette clé, qui est la pierre angulaire de la sécurité dans une infrastructure PKI. Parfois le propriétaire du terminal installe lui même son certificat, il existe donc un risque de duplication de la clé privée, involontaire ou maligne. Dans ce mode de transport du certificat, la menace provient du fait que la clé secrète peut être dérobée à l'insu de son propriétaire.
2- Le terminal doit être configuré avec le certificat racine et le certificat client. En fait c'est le terminal qui est authentifié, si l'usager du réseau dispose de plusieurs terminaux il faudra installer un certificat différent sur chacun d'entre eux. La mobilité de l'utilisateur n'est pas gérée avec souplesse.
3- Lors d'une authentification par PKI il y a deux opérations importantes. La vérification du certificat du serveur, et l'émission d'une signature par le client avec sa clé privé. Il est important de souligner que ces actions sont réalisées par un système d'exploitation dont la vulnérabilité aux chevaux de Troie et autres vers est bien connu; en d'autres termes le risque de vol ou d'usage à distance de la clé privé est important.

L'approche cartes à puce EAP-TLS

Le concept carte à puce EAP-TLS est simple robuste et très sure. Les messages d'authentification ne sont pas traités par le terminal client, ce dernier se comporte comme un relais de communication passif entre serveur d'authentification et carte à puce. Celle ci traite intégralement les messages d'authentification, elle stocke toutes les informations nécessaires telles que certificat racine, certificat client et clé privée. Les avantages de cette approche sont les suivants :

1- Suppression du risque de vol de la clé privée. Cette clé est stockée dans la carte à puce, elle n'est pas connue de son utilisateur, ce qui rend impossible le clonage. La carte est protégé par un code PIN, qui garantie sa protection en cas de perte ou vol, à l'aide d'un mécanisme de blocage après trois essais infructueux.
2- Le terminal n'est pas configuré avec des certificats relatifs à son utilisateur. Il dispose d'un composant logiciel (DLL) qui relaye de manière passive les messages d'authentification depuis/vers la carte à puce. C'est l'usager du réseau Wi-Fi qui est identifié et non l'ordinateur personnel qu'il utilise, la mobilité est donc facilité.
3- Protection absolue contre les attaques des vers et autres chevaux de Troie. Les réseaux Wi-Fi utilisent le protocole SSL (le cadenas des navigateurs), dont la robustesse est universellement reconnue et éprouvée, puisqu'il assure la sécurité du commerce électronique. SSL est intégralement exécuté dans la carte à puce, toute modification par le terminal des messages émis ou reçus est détectée par cette dernière (et le serveur d'authentification) et provoque l'échec de la procédure d'authentification.

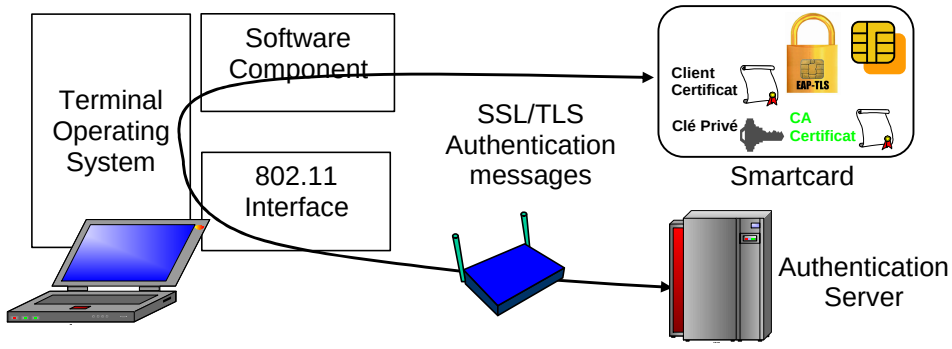


Figure 3. Infrastructure à clés publiques utilisant une carte EAP-TLS

La carte à puce EAP-TLS.

La carte EAP-TLS est dérivée du concept de la *Carte EAP*, inventé par Pascal Urien, enseignant chercheur à l'ENST (voir http://www.enst.fr/recherche/succes/carte_eap_innovation.php).

Elle permet le mariage de technologies réseau avec la sécurité éprouvée des cartes à puce, unanimement reconnues comme l'ordinateur le plus sure, garantissant par exemple la sécurité des transactions bancaires.

La *Carte EAP* est décrite par un draft IETF (*Internet Task Force Engineering*), qui, pour mémoire est l'organisme définissant les protocoles du réseau Internet (voir par exemple http://www.ietf.org/proceedings/03mar/slides/eap-9/index.html). Le comité *WLAN Smartcard Consortium*, qui comporte une vingtaine de membres industriels (Alcatel, Texas Instrument, Sagem, Visa, Gemplus, Axalto, …) soutien cette initiative (voir http://www.wlansmartcard.org/press_releases_1.html).

Elle a également remporté deux prix industriels, le Sésame de la *Meilleure Innovation Technologique*, au salon carte 2003 à Paris (le plus grand salon mondial de la carte à puce) ainsi que un *Innovation Breakthrough Awards* à Washington lors du salon CardTech/SecureTech, en avril 2004.

La technologie carte EAP-TLS

La carte EAP-TLS est une application Java exécutée par un carte à puce embarquant une machine virtuelle Java (JVM). Cette approche permet d'utiliser de multiples cartes disponibles sur le marché, et d'offrir des niveaux de sécurité, et performances et de prix variables en fonction des constructeurs.

Elle fonctionne sur les systèmes Windows standards (2000, XP, …) et requiert l'installation d'un composant logiciel particulier (DLL).

Le marché de la sécurité à base de clés publiques dans les entreprises est important mais fragmenté. La personnalisation des cartes EAP-TLS, c'est à dire le chargement des informations propres à l'entreprise (certificat racine, certificat client et clé privée) est un défi industriel majeur, qui doit concilier exigences de production et mise en place d'une solide chaîne de sécurité depuis la génération des certificats client par le serveur PKI de l'entreprise, jusqu'à son chargement dans la carte de l'utilisateur.

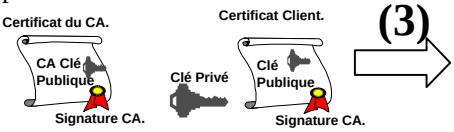
Ou voir une démonstration ?

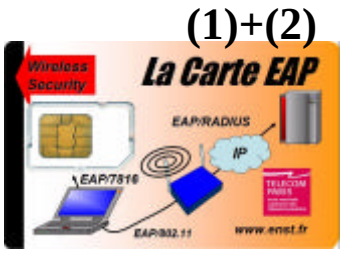
L'ENST Paris dispose d'un réseau Wi-Fi, dont la sécurité est assurée par une infrastructure à clé publique. Un prototype est opérationnel sur ce site. Il se présente sous la forme d'un PC, muni du système d'exploitation *Windows XP*, et se connectant au réseau à l'aide d'une carte EAP-TLS, utilisant un composant *javacard* commercial, personnalisé avec les informations produites par le serveur PKI.

ANNEXE.

I- Etape de la production d'une carte EAP-TLS.

(1) Analyse des besoins du client, sélection d'une Javacard.
(2) Chargement de l'Application
(3) Personnalisation





II- Mise en œuvre sur une plateforme Windows.

(1) Installation d'un composant logiciel (eapcard.dll).
(2) Sélection d'un certificat, si la carte en comporte plusieurs.
(3) Gestion des connexions Wi-Fi par la carte. Protection par code PIN.