
# Dossier Mobilité & Sécurité

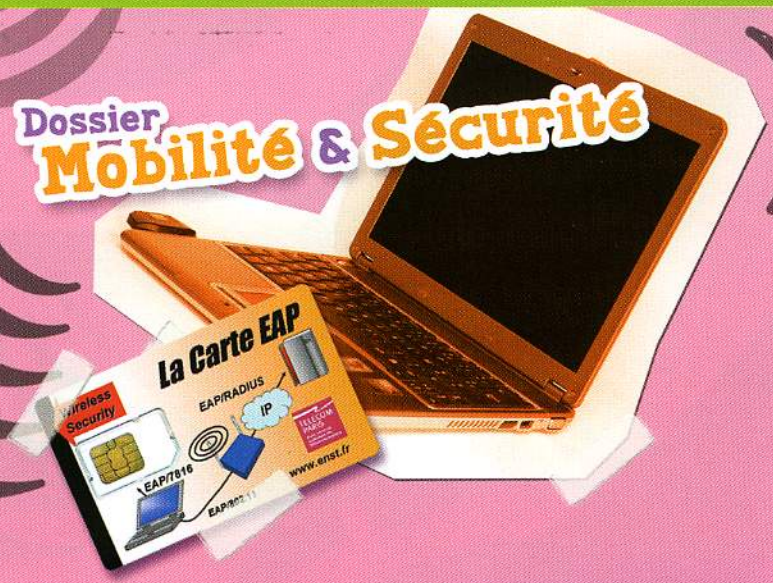
Dossier par
Marc Jacob
& Maurice Louis

# L'expertise est de rigueur

**La mobilité et les liaisons radio sont sources d'accroissement de performance dans l'entreprise :**

- **Plus grande facilité d'accéder à l'information, donc hausse de la productivité.**
- **Suppression des câbles informatiques coûteux et consommateurs de main d'œuvre, donc réduction des dépenses.**

**Néanmoins, ces solutions ont mauvaise presse sur le plan de la sécurité des systèmes d'information.**
**Nous faisons le point dans ce dossier sur les risques et présentons les nouvelles solutions de sécurisation. Bien configurées, ces technologies deviennent exploitables en toute sérénité et conservent leurs qualités : accès facile à l'information et réduction de coûts.**




Paroles de PROFESSEUR

Pascal Urien, professeur à l'ENST

# Sécuriser le Wi-Fi avec une carte à puce

Pascal Urien, professeur à l'ENST

**L'engouement des marchés informatiques pour les réseaux sans fil 802.11, appelés encore Wi-Fi, est freiné par l'absence, à ce jour, d'infrastructures de sécurité standardisées et inter-opérables. Les réseaux sans fil paraissent donc aussi séduisants que dangereux, et requièrent une analyse attentive des besoins de sécurité, préalablement à leur déploiement. A l'origine, les réseaux 802.11 n'étaient 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. Selon nopworld, www.nopworld.com, un accroissement du temps de connexion de 45 minutes par jour augmente la productivité d'un employé de 20 %. Cette technologie permet de mettre en place des infrastructures bon marché, mais cependant capables de supporter plusieurs milliers d'utilisateurs. Pascal Urien, professeur à l'Ecole Nationale Supérieure des Télécommunications présente une nouvelle génération de cartes à puce, les cartes EAP, qui renforce les éléments de sécurité indispensables au déploiement des réseaux sans fil 802.11. Cette technologie se présente comme une alternative aux protocoles de sécurisation, tant sous Windows que sous Linux, qui devraient déferler en 2006.**

L'émergence des réseaux sans fil IP, propulsée par l'usage exponentiel des réseaux Wi-Fi, accélère le déploiement de services IP mobiles. La mobilité IP consiste, dans cette première étape à utiliser les services déjà disponibles dans les infrastructures câblés, tels que courrier électronique, forum de messageries, multimédia, consultation de base de données, accès au WEB. Dans le modèle actuel de l'Internet un terminal se connecte à son réseau mère, géré par un fournisseur d'accès, le FAI, qui délivre une adresse IP et loge différents serveurs. Dans le milieu des années 90, c'est le protocole PPP (RFC 1661, 1994) qui a permis de relier un parc d'un demi milliard d'ordinateurs personnels équipés de modems, aux fournisseurs de services. La mobilité IP s'est donc développée grâce au réseau téléphonique (RTC), et en particulier avec une sécurité logique relativement modeste puisque les écoutes téléphoniques sont répu-

tées difficiles et de surcroît illégales. Parallèlement à cette tendance, le réseau GSM a connu durant la même période un formidable succès, en raison du réel besoin du marché de disposer d'un service de transport de voix universel, mobile et sans fil.

## Au début de l'Internet les mots de passe pouvaient être échangés en clair

Les mécanismes de sécurité de l'Internet de première génération sont basés sur des mots de passe, parfois échangés en clair, ou sur des scénarii de défi dont la plupart utilisent la fonction MD5, dont de nouvelles collisions furent récemment démontrées par Wang X et al, en 2004. A l'opposé, l'architecture du GSM est plus novatrice, elle se compose d'une infrastructure matérielle à deux niveaux, une base de données centrale (Host Location Register) délivrant des vecteurs d'authentification, et des agents distribués (Visitor Location Register) en charge de l'identification des utilisateurs, à l'aide des triplets d'authentification. Une carte à puce SIM authentifie un usager par un double mécanisme, d'une part un PIN code réalise le lien entre le module de sécurité et son porteur, et d'autre part la carte stocke une clé secrète de 128 bits, et effectue les calculs cryptographiques nécessaires.

Les normes IEEE 802.1x (IEEE 802.1x, 2001) et IEEE 802.11i (IEEE 802.11i, 2004) ont bâti une architecture de sécurité à trois niveaux, le Supplicant, un usager muni d'un terminal IP, l'Authenticator, un point d'accès qui bloque les trames des clients non authentifiés, et le serveur d'authentification Radius qui conduit l'authentification du Supplicant. Ce schéma présente de nombreuses similitudes avec celui du GSM ; le système peut être centralisé, par exemple le réseau sans fil de la société Microsoft, environ 50,000 employés, s'appuie sur quelques serveurs Radius, ou distribué si une infrastructure PKI est disponible.

## La carte à puce une technologie sûre et rapide

Les cartes à puce sont généralement considérées comme le système informatique le plus sécurisé, c'est-à-dire qu'il est très difficile, voire impossible, de déduire par quelque méthode, physique ou logique, que ce soit, les clés utilisées lors de l'exécution d'un algorithme cryptographique (RSA, DES, AES, ...) par le processeur de la puce sécurisée. Les composants actuels réalisent un calcul RSA (2.048 bits) en moins d'une demi seconde, et intègrent une capacité mémoire de l'ordre de 128 koctets ; cette valeur atteint plusieurs Moctets grâce à la technologie flash. Ces dispositifs offrent des performances satisfaisantes (temps d'authentification de l'ordre de la seconde) et des capacités de stockage confortables pour la gestion de plusieurs réseaux (la taille d'un certificat X509 est de l'ordre de quelques koctets). De surcroît, la puissance de calcul des processeurs (jusqu'à 100 MIPS) permet d'exécuter tout ou partie du protocole EAP dans une carte spécifique, la carte EAP. L'EAP (RFC 3748, 2004) est un protocole issu de la problématique de la gestion sécurisée de PPP. Il répond au classique paradigme de requêtes/réponses, et peut transporter différentes classes de scénarii d'authentification, identifiées par un type. Le concept de la carte EAP est fort simple (Urien et al, 2003), les messages EAP sont traités côté Supplicant par une puce spécialisée qui analyse les requêtes et

AN ACADEMIC VIEWPOINT:
PASCAL URIEN, PROFESSOR AT ENST

### USING SMART CARDS TO INCREASE WI-FI SECURITY

Information-system market enthusiasm for 802.11 wireless networks or Wi-Fi has been dampened by the current lack of standardised and interoperable secure infrastructures. Wireless networks are as attractive as they are dangerous and the security requirements need to be analysed carefully before deployment. In the beginning, 802.11 networks were simply a natural extension of Ethernet cable networks; the use of radio links increases user connection time and therefore profitability. According to Nopworld (www.nopworld.com) an increase of 45 minutes of connection time per day, increases productivity by 20%. This technology allows low-cost infrastructures to be set up capable of supporting several thousand users. Pascal Urien, professor at the Ecole Nationale Supérieure des Télécommunications, presents a new generation of smart cards called EAP cards, designed to reinforce the security aspects essential for deploying wireless 802.11 networks. This technology is an alternative to the Windows and Linux security protocols due to flood the market in 2006.

génère les réponses appropriées.
L'ajout de cartes à puce dans les architectures sans fil introduit un niveau de sécurité supplémentaire puisque l'utilisateur n'a pas accès aux clés cryptographiques requises pour son authentification. De manière analogue au réseau GSM, la puce est la propriété d'un fournisseur de service réseau (entreprise, administration, opérateur, ...), il est difficile de cloner un tel composant. Il existe quelques similarités entre l'infrastructure GSM et le modèle de sécurité 802.11. La carte SIM stocke l'identité de son utilisateur (IMSI) et implémente un algorithme d'authentification A3/A8 associé à une clé secrète Ki (128 bits). Cette procédure utilise un argument d'entrée RAND (16 octets) et produit deux valeurs, une signature SRES (32 bits) et une clé Kc (64 bits) utilisée pour le chiffrement de la communication entre la station de base (BTS) et le mobile (ME). Une base de données centrale (HLR, Host Location Register) stocke pour chaque utilisateur, identifié par son IMSI, ses droits (le type d'abonnement souscrit) et la clé Ki. HLR se comporte comme un serveur d'authentification produisant des triplets (RAND, SRES, Kc). Un abonné est authentifié par une entité du réseau visité (le MSC, Mobile Switching Center) qui stocke dans une base de données locale (le VLR, Visiting Location Register) des triplets délivrés à sa demande par le serveur HLR.

Les téléphones portables sont nativement conçus pour fonctionner avec une carte à puce. La situation est différente dans le monde des technologies de l'information, utilisant principalement des ordinateurs personnels (plus d'un demi milliard d'unités connectées à Internet).

Le Wlansmartcard Consortium créé en février 2003, comporte 19 membres fondateurs académiques ou industriels : Alcatel, Aspects Software Ltd, Atmel, Dai Nippon Printing, ENST, Gemplus, Infineon Technologies AG, Jurgensen Consulting, Koolspan, Oberthur Card Systems, Raak Technologies, Schlumberger, Texas Instruments, Transat, Trusted Logic, Ucopia, Visa. Il permet d'apporter un support industriel aux infrastructures sans fil sécurisées par carte à puce. Un des défis majeurs est la mise sur pied d'une infrastructure de personnalisation et de gestion (mécanismes de révocation) d'un parc important de cartes à puce. Cependant, cette technologie a déjà prouvé sa capacité à passer le facteur d'échelle. Plus d'un milliard de cartes ont été produites en 2004. Plusieurs approches sont envisageables pour la mise en œuvre de cartes dans les réseaux sans fil :

- L'utilisation de cartes propriétaires, dont l'interface fonctionnelle n'est conforme à aucune norme. Généralement les particularités de tels composants sont masquées par une API, c'est-à-dire une interface logicielle offrant des services cryptographiques conformes à des standards par exemple PKCS#11, édité par la société RSA, ou CSP (Crypto Service Provider) déployés sur les systèmes Microsoft.
- L'usage de cartes à puce bien connues, tels que les modules SIM (par exemple pour implémenter le protocole EAP-SIM) ou bien des cartes bancaires (BO', EMV...) capables de réaliser des signatures.
- La définition d'une carte dédiée : la carte EAP.

## La carte EAP offre quatre catégories de service

Les services offerts par la carte EAP peuvent se répartir en quatre catégories :

- L'interface réseau. Les paquets EAP reçus par le terminal IP sont routés de manière transparente par son système d'exploitation vers/depuis la carte. A la fin du scénario d'authentification, la carte calcule une clé de session (Pairwise Master Key, PMK) qui est mise à disposition du système d'exploitation du terminal.
- L'interface système d'exploitation. Une carte EAP gère plusieurs identités (c'est à dire différentes méthodes EAP et les lettres de crédit associées). Un service de découverte permet d'obtenir la liste des identités disponibles et d'en sélectionner une.
- L'interface de sécurité. C'est un ensemble de deux PIN codes (utilisateur et émetteur de la carte) protégeant le contenu ou l'usage de la carte.
- L'interface de personnalisation. Les puces sont émises sans éléments d'authentification spécifiques, et sont personnalisées ultérieurement pour les utilisateurs du réseau.

## Carte EAP et Java

De nombreuses cartes embarquent une machine virtuelle java permet-

tant d'embarquer des applications écrites en langage Java. Le javacard est un sous ensemble de Java, normalisé par le Javacard forum, les versions disponibles sont JC2.1 ou JC2.2. D'un point de vue matériel, les plateformes offrent des capacités de mémoires volatiles (RAM) voisine de 4 koctets, et de mémoire non volatile (E2PROM), de l'ordre de 32 koctets ; le code byte est stocké dans cette dernière mémoire.

La faisabilité d'une carte EAP repose d'une part sur la complexité du protocole embarqué, et d'autre part sur les contraintes de temps de réponse.

La norme javacard a défini un paquetage cryptographique relativement complet qui intègre un générateur de nombre aléatoire, des fonctions de HASH (MD5 ou SHA1), des algorithmes de chiffrement symétrique (DES, 3DES, AES) et asymétrique (RSA jusqu'à 2048 bits).

Pour des raisons de coût, les cartes sont généralement basées sur des processeurs 8 bits ; cependant les opérations cryptographiques complexes telles que génération de nombre aléatoire, DES, AES ou RSA sont conduites par un crypto processeur. L'interprétation d'un protocole par une machine java 8 bits est donc relativement lente, bien que l'appel aux fonctions cryptographiques soit optimisé.

## EAP-TLS embarqué, des apports sécuritaire pertinents

TLS est la version normalisée par l'IETF (RFC 2246, 1999) du célèbre protocole SSL (le cadenas des navigateurs). La méthode EAP-TLS (RFC 2717, 1999) transporte TLS de manière quasi transparente. Dans EAP-TLS le mode d'authentification mutuelle, rarement utilisé sur le WEB, est obligatoire. Le Supplicant possède donc un certificat et la clé privée RSA associée. Le tunnel sécurisé (fourni par Record Layer), dont les clés sont déterminées au terme de la phase Handshake n'est pas utilisé pour l'échange d'information ; cependant une fois le tunnel disponible une clé PMK est calculée et mise à disposition du protocole de sécurité radio.

L'analyse de validité d'un certificat implique l'existence d'un composant logiciel embarqué, analogue au magasin de certificats (Certificats Store), disponible sur les plateformes Windows. La disponibilité d'une telle entité dans un espace sûr est un élément de sécurité important ; la vérification des chaînes de certificat est une opération critique dans un environnement SSL/TLS. Une des attaques classiques du protocole SSL, consiste à neutraliser le logiciel qui contrôle les certificats et donc à accepter les connexions avec tout type de serveur.

Un des points faibles de mise en œuvre de carte à puce, est l'éventualité d'une attaque par un cheval de Troie, logé dans un terminal non sûr, par exemple un ordinateur personnel. Le porteur de la carte renseigne son code personnel (PIN), dès lors le cheval de Troie, ainsi que les autres composants logiciel de l'hôte, accède aux ressources de la puce sécurisée. Ce type d'attaque est difficile à mettre en œuvre avec une pile TLS embarquée dans une carte EAP pour les raisons suivantes :

- Grâce au magasin de certificats la puce vérifie, de manière autonome, le certificat du serveur. La clé PMK déduite de la phase d'authentification ne sera disponible que pour le propriétaire de la clé privée associée.
- Le protocole TLS vérifie l'intégrité des informations à trois reprises, notamment lors du dernier message reçu par le client. La puce a donc la certitude que le serveur a obtenu les données sans altération.

L'architecture EAP-TLS embarquée est similaire au classique modèle SAM (Secure Access Module) couramment déployé dans des infrastructures sécurisées par carte à puce. Le protocole TLS est exécuté côté Supplicant dans un coffre fort de silicium, et côté RADIUS par un serveur, idéalement installé dans une chambre forte.

La taille d'un message TLS peut atteindre 16.384 octets (214), une taille très supérieure à la dimension maximale d'une trame MAC (de l'ordre de 1500 octets). En conséquence EAP-TLS définit un mécanisme de segmentation réassemblage compatible avec les charges utiles des LANs. Cependant les messages de 1.500 octets ne peuvent être transmis directement à une puce conforme aux normes ISO 7816, il est nécessaire d'introduire un nouveau mécanisme de segmentation/réassemblage en des paquets de plus petite taille (environ 256 octets).

## Des limites liées à la mémoire et à la rapidité de calcul

Les contraintes fondamentales à respecter sont d'une part la possibilité d'implémenter TLS dans un espace mémoire modeste (inférieur à 32 koctets) et d'autre part d'obtenir une rapidité d'exécution compatible avec la norme IEEE 802.1x, qui recommande un temps de réponse du Supplicant inférieur à 30 secondes par défaut.

La carte EAP-TLS la plus rapide que nous ayons testée réalise une authentification en moins de 10 secondes. Le prix de ce composant est de l'ordre de 10 $, auquel s'ajoute le coût d'un lecteur de carte, par exemple une clé USB (environ 40$).

## Et pour demain

L'apparition d'une application EAP-TLS embarquée dans une puce sécurisée ouvre de nombreuses perspectives d'applications pour la sécurité des réseaux sans fil. En particulier de nombreuses plateformes démunies d'infrastructures PKI, proposent des tunnels basés sur TLS, utilisant d'une part une authentification simple du serveur Radius et d'autre part une méthode symétrique pour le Supplicant (mot de passes, secrets partagés,...) protégée par un tunnel TLS. La carte EAP embarquera diverses méthodes basées sur ces tunnels.

## Une technique au point, mais...

La première carte EAP-TLS opérationnelle permet de disposer d'une véritable PKI de poche. Les performances restent cependant proches des valeurs limites de fonctionnement. Les contraintes technologiques ont été clairement identifiées et seront partiellement levées si les enjeux liés à la sécurité des réseaux sans fil deviennent importants et conduisent à l'optimisation des cartes à puce pour cet usage. Cette nouvelle classe de cartes à puce dédiées aux environnements sans fil Wi-Fi (et bientôt WiMax) est de plus compatible avec les caractéristiques des puces actuelles en termes de capacité mémoire ou de puissance de calcul; de surcroît, elle intègre ces composants aux plateformes Windows. Tous les éléments techniques sont donc réunis pour le déploiement de telles infrastructures ; cependant il n'est pas certain que cette approche, basée sur une technologie typiquement européenne, résistera au syndrome NIH (Not Invented Here).

## Bibliographie


- Site WEB http://www.enst.fr/~urien/openeapsmartcard
- RFC 1661 "The Point-to-Point Protocol (PPP)" 1994.
- RFC 2104, "HMAC: Keyed-Hashing for Message Authentication", 1997.
- RFC 2246 "The TLS Protocol Version 1.0", 1999.
- RFC 2716 "PPP EAP TLS Authentication Protocol", 1999.
- Institute of Electrical and Electronics Engineers, "Local and Metropolitan Area Networks: Port-Based Network Access Control", IEEE Standard 802.1X, September 2001.
- Urien P, "Réseaux locaux sans fil : aussi dangereux que séduisant", Sécurité Informatique, numéro 40, juin 2002.
- Urien P, Pujolle G, "Architecture sécurisée par carte à puces, pour des réseaux sans fil sures et économiquement viables" Gestion de réseaux et de services, GRES 2003, Fortaleza, Ceara, Bresil, 24-27 février 2003.
- Urien P, Loutrel M, "La carte à puce EAP, un passeport pour la sécurité des réseaux émergents Wi-Fi", Journées Réseaux 2003 (JRES'2003), Lille, Novembre 2003.
- Institute of Electrical and Electronics Engineers, "Supplement to Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11:Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security", IEEE Standard 802.11i, 2004.
- RFC 3748 "Extensible Authentication Protocol (EAP)", 2004.
- Internet Draft, "draft-urien-eap-smartcard-08.txt", June 2005.
- Microsoft, "Le Wireless chez Microsoft", Journées Microsoft de la sécurité, Paris, 4-6 mai 2004.
- Urien P, Badra M, Dandjinou M, "EAP-TLS smartcards, from dream to reality", 4th Workshop on Applications and Services in Wireless Networks, Boston, Massachusetts, USA, August 8-11 2004.
- Wang X, Lai X, Feng D, Yu D, "Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD", CRYPTO 2004, Santa Barbara, California, USA, August 15-19, 2004.
- Rouault H, Crochon E, Martinet S, Sourgen L Martin M, "PEA or Power Embedded Active Card Power Embedded Active Card", e-Smart, Sophia Antipolis, France, 23-25 September 2004.