La sécurité des réseaux sans fil 802.11

Pascal Urien

Le succès du réseau internet, véritable moteur de la nouvelle économie de la dernière décennie, a imposé le protocole IP comme un standard *de facto* pour l'échange des données numériques. Surfant sur cette vague les entreprises ont adopté cette technologie pour le stockage et la diffusion de leurs informations stratégiques ; intranet, courrier électronique, bases de données, annuaires LDAP sont des services aujourd'hui indispensables à la compétitivité et la survie de toute activité économique.

Si la prédominance des réseaux IP est actuellement incontestable, il convient également de remarquer que les technologies des réseaux locaux tendent également vers un standard de fait, le réseau Ethernet. Cette technologie, initialement basée sur le partage d'un guide d'onde (un câble en fait) a petit à petit migré vers une infrastructure basée sur des commutateurs de trames (les *switchs*).

A la base, les réseaux sans fil 802.11 ne sont que l'extension naturelle des réseaux Ethernet câblés. La croissance exponentielle de ce marché s'explique par un réel besoin des utilisateurs d'accéder au réseau de manière quasi transparente, sans l'obligation de connecter leur ordinateur personnel à une prise. Le réseau sans fil remplace le câble par un lien radio ; cependant, en raison des lois de propagation des ondes électromagnétiques, cette prise virtuelle est utilisable dans un rayon de l'ordre de 100 m, c'est-à-dire dans certains cas à l'extérieur des murs de l'entreprise.

LCN, volume 4, n° 3-4/2003, pages 167 à 184

On introduit donc de nouveaux risques d'intrusion ou de fuite d'information, parfois qualifiés (Arbaugh *et al.*, 2001) d'attaque par le parking (*parking lot attack*).

L'apparition de l'IP sans fil dans des architectures câblées préexistantes implique donc la mise en place de nouvelles mesures de sécurité. Jusqu'à présent les entreprises ont déployé leurs réseaux locaux sans protection particulière des points d'accès. Précisément le réseau est organisé autour d'un arbre de commutateur de paquets (HUB), auquel sont reliées des stations de travail, à l'aide de prises marquant les points d'accès au réseau (souvent dénommées *port d'accès*). L'entrée de l'établissement étant contrôlé et réservé au personnel autorisé, les ports d'accès ne sont pas communément sécurisés, en particulier pour permettre une libre connexion des ordinateurs portables. La mobilité des usagers s'appuie sur le protocole DHCP allouant dynamiquement une adresse, compatible avec l'organisation logique et géographique de l'intranet. Celui-ci ne conduisant pas en règle générale une procédure d'authentification avant l'allocation des paramètres de configuration[1], il est très facile d'accéder à l'intranet d'une entreprise depuis un port d'accès.

En conséquence, le contrôle des accès, quasi inexistant dans le cas des réseaux câblés, devient un prérequis pour le déploiement des réseaux 802.11. De même, la signature des trames est également indispensable : en son absence, un pirate peut facilement usurper l'adresse MAC d'un utilisateur authentifié (*MAC spoofing*) et accéder aux ressources numériques disponibles. Le chiffrement des données transitant sur le lien radio est également souhaitable afin de garantir la confidentialité des échanges ; cependant de nombreuses méthodes (IPSec, SSL, SSH…) sont déjà en mesure d'assurer ce service.

En résumé les services sécurisés indispensables aux extensions IP sans fil sont les suivants :

– identification et authentification des utilisateurs du réseau ;

– signature des trames échangées (intégrité, authentification) ;

– chiffrement des données (confidentialité).

1. RFC 2131, Chap. 7 - Security Considerations, « …Therefore, DHCP in its current form is quite insecure ».

Wi-Fi

Un réseau 802.11 (voir figure 1) est un ensemble de cellules de base (encore dénommées BSS, *Basic Set Service*), chacune d'entre elles comportant un point d'accès (*Access Point*, AP) matérialisé par un dispositif d'émission-réception analogue aux stations de base du GSM. L'ensemble de ces cellules est relié par une infrastructure de communication fixe (*Distribution System* DS), qui incorpore en particulier un portail (*Portal*) assurant l'interface avec un réseau local (Ethernet) classique.

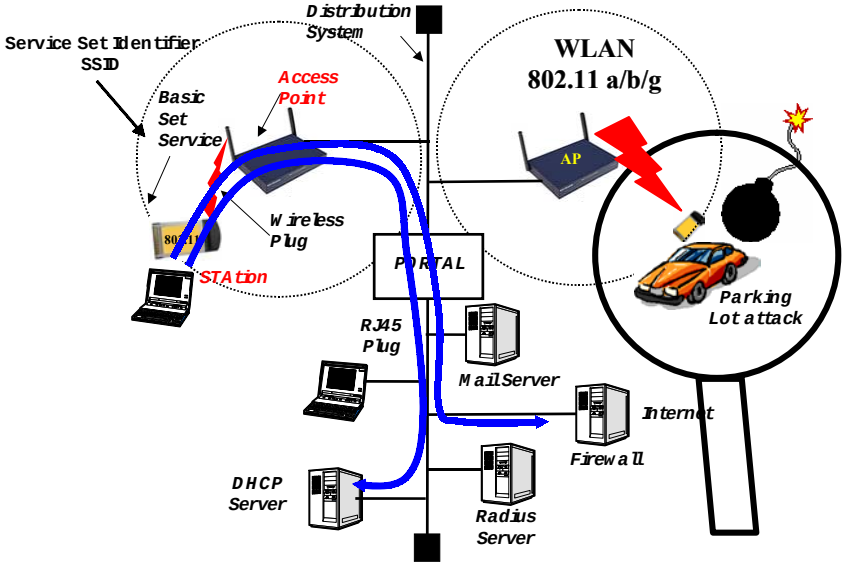

Figure 1. Une architecture caractéristique 802.11

La norme 802.11 (IEEE Std 802.11, 1999) définit un protocole de sécurité radio, le WEP[2]. Son principe consiste à chiffrer les trames (voir figure 2) à l'aide de l'algorithme RC4 et d'une clé, obtenue par la concaténation d'un secret partagé et d'un indice (IV) transporté en clair dans chaque paquet.

L'algorithme RC4 réalise le chiffrement des données en mode flux octets (*stream cipher*) ; à partir d'une clé de longueur comprise entre 8 et 2048 bits, il génère (à l'aide d'un *pseudo random generator* PRNG) une suite d'octets

2. *Wireless Equivalent Privacy.*

pseudo-aléatoire nommée *KeyStream*. Cette série d'octets (Ksi) est utilisée pour chiffrer un message en clair (Mi) à l'aide d'un protocole classique de Vernam, réalisant un *ou exclusif*.

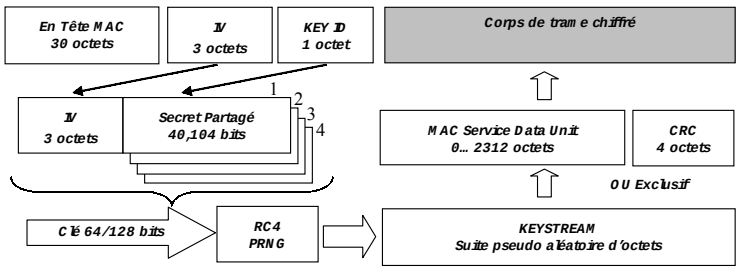

Figure 2. Le protocole WEP

Le WEP présente de nombreuses failles de sécurité (Borisov *et al.*, 2001), en voici un bref résumé :

– le nombre de *KeyStream* est limité à 16 millions. Un pirate peut facilement générer des trames, enregistrer leur forme chiffrée puis déduire et stocker les *KeyStream* identifiés par leur indice *IV* ;

– l'intégrité des trames est assurée par le chiffrement du CRC. Cette fonction étant linéaire par rapport à l'opération *ou exclusif*[3], il est possible de modifier un bit dans une trame chiffrée tout en recalculant une valeur correcte du CRC, c'est la technique d'attaque dite *bit flipping* ;

– l'attaque démontrée par Fluhrer (Fluhrer *et al.*, 2001) permet de recouvrer le secret partagé après l'émission d'approximativement quatre millions de trames chiffrées. Elle utilise des valeurs *IV* dites *résolvantes*[4], dont environ une soixantaine d'échantillons suffisent pour casser un octet du secret partagé ;

– de manière optionnelle l'authentification est réalisée par une méthode de défi (nommée *Shared Authentication*), le point d'accès délivre un nombre aléatoire, la station chiffre cette valeur. Cette méthode est inefficace car rejouable, l'attaquant enregistre le couple (aléa, aléa chiffré) d'où il déduit la

3. Soit T1 et T2 deux trames de même longueur, CRC(T1 exor T2) = CRC(T1) exor CRC(T2).

4. Dans ce cas, IV est de la forme (3+B,255,N) avec B un octet du secret partagé et N une valeur quelconque comprise entre 0 et 255.

valeur du *KeyStream* associé à un indice *IV ;* dès lors, il est capable d'usurper l'identité d'un client autorisé du réseau.

En raison des problèmes évoqués précédemment, il est fortement conseillé de changer la clé WEP fréquemment, par exemple toutes les 10 000 trames. Cependant cette technique ne garantit pas l'intégrité de l'information et les attaques *bit flipping* restent possibles.

Une particularité du protocole 802.11 est que l'authentification est obligatoire avant toute association avec un point d'accès. Une station sans fil se trouve en conséquence dans l'un des trois états suivants :

– non authentifié et non associé ;

– authentifié et non associé ;

– authentifié et associé.

Lorsque la station ne souhaite pas utiliser une méthode d'authentification (*Shared Authentication*) basée sur WEP, elle dispose d'une procédure volontaire sans aucun élément de sécurité, baptisée *Open Authentication*.

Une difficulté de déploiement d'une architecture basée sur WEP est la nécessité de partager un même secret entre station et point d'accès. Cette contrainte freine considérablement le passage à l'échelle ; elle souligne l'importance de la disponibilité d'une infrastructure de distribution des clés telle que par exemple définie par la norme 802.1X (IEEE Std 802.1X, 2001).

IEEE 802.1X

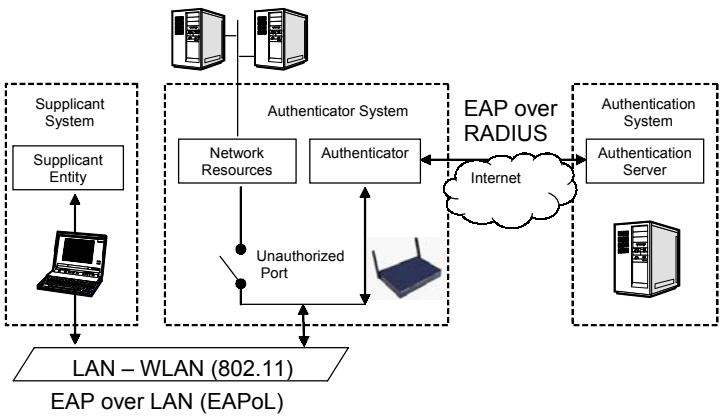

Figure 3. L'architecture 802.1X

Le protocole IEEE 802.1X (ou *Port Based Network Access Control*) était initialement conçu pour la gestion sécurisée des accès des réseaux (câblés) à base de commutateurs de paquets (*switchs*). L'idée centrale est de bloquer le flux de données d'un utilisateur non authentifié. Ce modèle s'appuie sur trois entités fonctionnelles (voir figure 3) :

– le *Supplicant*, un terminal informatique désirant utiliser les ressources offertes par un réseau de communication ;

– l'*Authenticator*, le système qui contrôle un port d'accès au réseau. Le flux de données du supplicant est divisé en deux classes, la première comprend les trames utilisées par le protocole d'authentification EAP[5], la deuxième regroupe les autres paquets, qui sont bloqués lorsque le port se trouve dans l'état *non autorisé*. En cas de succès du processus d'authentification, le port passe à l'état *autorisé* et offre un libre passage à toutes les trames ;

– le *serveur d'authentification* (RADIUS[6]), il réalise la procédure d'authentification avec le supplicant. Durant cette phase l'*Authenticator* n'interprète pas le dialogue entre ces deux entités, il agit comme un simple relais passif.

Le protocole EAP est la clé de voûte de cette approche. Il est tour à tour encapsulé dans des trames MAC 802 (EAPoL[7]) ou par le protocole RADIUS qui est routable (puisque transporté par IP et UDP).

Schématiquement l'insertion d'un terminal sans fil dans un environnement 802.1X se déroule de la manière suivante :

– dans un premier temps la station s'authentifie puis s'associe à un point d'accès, identifié par un nom (le *SSID*) ;

– la station émet alors périodiquement (toutes les 30 secondes) une trame EAPoL-Start, indiquant son intention d'ouvrir une session d'authentification ;

– le point d'accès transmet une demande d'identification (*EAP-Request.Identity*) au *Supplicant* qui produit en retour une réponse (*EAP-Response.Identity*) comportant l'identité (*EAP-ID*) du terminal sans fil ;

– à partir de ce paramètre le point d'accès déduit l'adresse (IP) du serveur d'authentification et transmet à ce dernier le message *EAP-Response.Identity* encapsulé dans une requête RADIUS ;

---

5. EAP, *Extensible Authentication Protocol*, RFC 2284, March 1998.
6. RADIUS, *Remote Authentication Dial In User Service*, RFC 2865, June 2000.
7. EAPoL, *EAP Over LAN*.

– dès lors, des messages EAP (requêtes et réponses) sont échangés entre serveur RADIUS et *Supplicant*, le point d'accès ne jouant qu'un rôle passif de relais ;

– le serveur RADIUS indique le succès ou l'échec de cette procédure grâce à un message *EAP-Success* ou *EAP-Failure*. En fonction de cette information le port transite à l'état autorisé ou non autorisé.

A la fin d'un scénario d'authentification réussi, *Supplicant* et serveur d'authentification calculent un secret partagé, baptisé *Unicast Key*. Le serveur d'authentification transmet cet élément, grâce au protocole RADIUS, au point d'accès. Ce dernier choisit alors une clé WEP, et la pousse vers le *Supplicant*, de manière sécurisée, dans une trame EAPoL-Key, chiffrée et signée à l'aide de la clé *Unicast*.

EAP

Le problème de la gestion de la mobilité des utilisateurs est devenu critique dès lors que les internautes ont massivement utilisé des modems et le protocole PPP pour accéder aux ressources offertes par leur ISP (*Internet Service Provider*). Les systèmes d'exploitation ont donc intégré des fonctionnalités renforçant la sécurité des nomades, telles que :

– l'authentification des utilisateurs par des méthodes de défi, afin d'éviter la transmission en clair des mots de passe ;

– le chiffrement des messages PPP, et les méthodes de calcul des clés nécessaires ;

– la distribution de telles clés par le protocole RADIUS.

Le besoin de compatibilité avec des infrastructures d'authentification diversifiées et la nécessité de disposer de secrets partagés dans des environnements multiples ont naturellement conduit à la genèse du protocole EAP, capable de transporter des méthodes d'authentification indépendamment de leurs particularités.

Le protocole EAP fournit un cadre peu complexe pour le transport de protocoles d'authentification ; un message comporte un en-tête de cinq octets et des données optionnelles. Il existe quatre type de messages, requête, réponse, succès et échec. Un protocole d'authentification particulier est identifié par un numéro (le type) compris entre 0 et 255, par exemple :

– type = 1, message relatif à l'identité,

– type = 4, protocole d'authentification à base de défi MD5 (EAP-MD5),

– type = 13, transport de TLS (EAP-TLS), plus connu sous le sigle SSL,

– type = 18 méthode d'authentification basée sur une carte SIM (EAP-SIM),

– type = 26, MSCHAPv2, protocole utilisé dans les environnements Windows.

L'identité de l'utilisateur est indiquée par la valeur *EAP-ID* contenue par le message *EAP-Response.Identity*. Lorsque ce paramètre est similaire à une adresse de courrier électronique[8] le point d'accès interprète la partie gauche avant le caractère @) comme un *login* utilisateur et la partie droite comme le nom de domaine d'un serveur RADIUS.

Une session d'authentification (voir figure 4) est initialisée par le point d'accès grâce au message *EAP-Request.Identity*. Elle se poursuit par une suite de requêtes et de réponses (*EAP-Request.Type* et *EAP-Response.Type*), relatives à un type particulier (un scénario d'authentification) et échangées entre serveur RADIUS et *Supplicant*. Elle se termine par un message *EAP-Success* ou *EAP-Failure*.

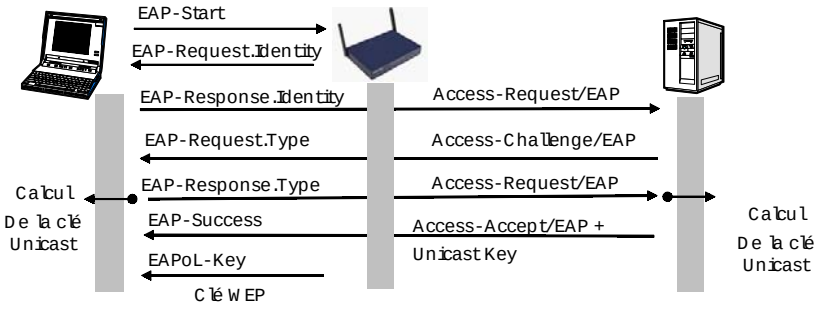

Figure 4. Une session typique d'authentification 802.1X

Un des points faibles du protocole EAP est le déni de service (Mishra *et al.*, 2002) : un pirate peut écouter une session EAP et émettre à l'intention du *Supplicant* un message *EAP-Failure*. Cependant il ne pourra pas obtenir la clé WEP délivrée par le message *EAPoL-Key* parce que cette dernière est chiffrée et signée par la clé *unicast* dont il ne connaît pas la valeur.

Nous allons à présent examiner brièvement trois types de méthodes d'authentification liées à des environnements différents.

8. *The Network Access Identifier*, RFC 2486, June 1999.

EAP-MSCHAPv2

Dans l'univers Microsoft, la sécurité d'un ordinateur personnel est fortement corrélée au mot de passe de son utilisateur. Ce dernier n'est jamais stocké en clair dans la mémoire de la machine. A partir d'un mot de passe on calcule une empreinte de 16 octets, mémorisée par le système hôte. Cette valeur, parfois nommée *clé NT* ou *NtPasswordHash*, est complétée par cinq octets nuls. On obtient ainsi 21 octets interprétés comme une suite de trois clés DES. La méthode MSCHAPv1 est une authentification simple, le serveur d'authentification produit un nombre aléatoire de 8 octets, le client utilise ses trois clés DES pour chiffrer cet aléa, ce qui génère une réponse de 24 octets.

MSCHAPv2 est une extension du protocole précédent, le serveur d'authentification délivre un nombre aléatoire de 16 octets (*AuthenticatorChallenge*), le *Supplicant* calcule une nombre 8 octets à partir de cette valeur, d'un aléa (*PeerChallenge*) qu'il génère et du nom de l'utilisateur (login). Ce paramètre est chiffré de manière analogue à MSCHAPv1 par la clé NT et l'on obtient une valeur de 24 octets. Dans une plate-forme Microsoft un annuaire (*Active Directory*) stocke le nom des utilisateurs et leur clé NT.

EAP-SIM

Les opérateurs de téléphonie mobile utilisent une carte à puce SIM pour identifier et facturer leurs abonnés. Cette dernière stocke l'identité de l'utilisateur (*International Mobile Subscriber Identity*, IMSI) et une clé secrète notée Ki. Le réseau authentifie un client à l'aide d'un triplet RAND (64 bits) SRES (32 bits) et Kc (64 bits).

RAND est un nombre aléatoire généré par le serveur d'authentification. Un algorithme cryptographique, associé à la clé Ki, et appliqué à la valeur d'entrée RAND, fournit une valeur de 96 bits, qui représente la concaténation des attributs SRES et KC. SRES est interprété comme une signature prouvant l'identité de l'utilisateur et KC est utilisé pour le chiffrement de la conversation téléphonique. Parce que les opérateurs envisagent de prolonger le réseau GPRS par des *hotspots* Wi-Fi, ils proposent un protocole d'authentification EAP-SIM[9], basé sur la carte SIM et se déroulant schématiquement de la manière suivante :

9. H. Haverinen, J. Salowey, EAP SIM Authentication, draft-haverinen-pppext-eap-sim-11.txt June 2003.

– l'identité (*EAP-ID*) est obtenue par la concaténation du caractère '1' de la valeur exprimée en ASCII de l'IMSI (une suite de chiffres) du caractère @ et du nom de domaine de l'opérateur (EAP_ID == 1IMSI@operator.com) ;

– le *Supplicant* génère un nombre aléatoire (NONCE) ;

– le serveur RADIUS délivre une suite de valeurs RANDi, ce message comporte une signature prenant en compte la valeur précédente NONCE ;

– le *Supplicant* calcule les valeurs SRESi et KCi à l'aide de son module SIM. Il prouve sa connaissance de SRESi en incluant une signature, prenant en compte ces valeurs secrètes, dans le message de réponse. Le nombre NONCE et les attributs KCi sont utilisés pour le calcul de la clé Unicast.

Grâce à la technologie EAP-SIM les opérateurs de téléphonie peuvent utiliser leur base de données clients (*Host Location Register*) pour assurer la facturation des services sans fil.

EAP-TLS

TLS est la version standardisée par le comité IETF[10] du populaire protocole SSL, largement utilisé pour sécuriser le commerce électronique. Contrairement à l'usage courant mettant en œuvre une authentification simple du serveur, EAP-TLS impose une authentification mutuelle entre serveur RADIUS et *Supplicant.* Ce dernier dispose donc d'un certificat X509 et d'une clé de signature.

L'usage de cette clé privée soulève l'épineux problème de la sécurité requise pour son stockage et sa mise en œuvre. Dans les systèmes informatiques usuels, cette sécurité est assurée par des mots de passe permettant de déchiffrer et d'utiliser la clé privée. La carte à puce constitue une alternative à cette méthode, lorsque la sécurité de la plate-forme informatique est jugée insuffisante.

Vers la carte à puce EAP

Dans la section précédente, nous avons évoqué l'usage de cartes à puce pour des réseaux liés aux opérateurs de téléphonie mobile (cartes SIM), ou utilisant des infrastructures à clés publiques (PKI). Cette technologie a permis aux opérateurs d'exploiter leur réseau en limitant très fortement le nombre de fraudes (et par conséquent d'assurer une rentabilité financière) ;

10. *Internet Engineering Task Force*.

elle est également le support légal de la signature électronique reconnue par de nombreux pays.

La carte à puce EAP est un projet décrit par un *draft IETF*[11], auquel participe les principaux industriels de ce secteur, qui propose de traiter directement le protocole EAP dans la puce sécurisée. Bien que cette liste ne soit pas exhaustive, les principales applications visées sont EAP-SIM et EAP-TLS.

Schématiquement une carte EAP (Urien *et al.*, 2003b) assure quatre services de base (voir figure 5) :

– la gestion de multiples identités. Le porteur de la carte peut utiliser plusieurs réseaux sans fil. Chacun d'entre eux nécessite un triplet d'authentification, EAP-ID (la valeur délivrée dans le message EAP-Response.Identity), EAP-Type (le type de protocole d'authentification supporté par le réseau), et les crédits cryptographiques, c'est-à-dire l'ensemble des clés ou paramètres utilisés par un protocole particulier (EAP-SIM, EAP-TLS, MSCHAPv2). Chaque triplet est identifié par un nom (l'identité) dont l'interprétation peut être multiple (SSID, nom d'un compte utilisateur, mnémonique…) ;

– l'affectation d'une identité à la carte, en fonction du réseau visité ;

– le traitement des messages EAP ;

– le calcul de la clé *unicast* en fin de session d'authentification et sa mise à disposition pour le terminal désirant accéder aux ressources du réseau sans fil.

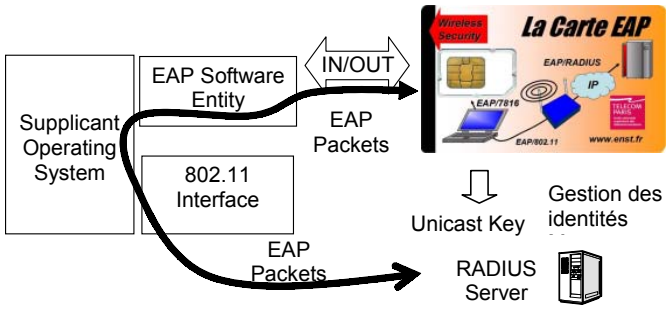

Figure 5. La carte à puce EAP

11. P. Urien, A.J. Farrugia, G. Pujolle, M. Groot, J. Abellan, « EAP support in smartcards », draft-urien-eap-smartcard.txt

RADIUS

Outre-Atlantique, les fournisseurs de services internet utilisent fréquemment des *pools* de modem installés dans les centraux téléphoniques urbains. Cette infrastructure, permettant des accès bon marché, est baptisée point de présence ou POP (*point of presence*). Plutôt que de dupliquer et de mettre à jour dans chaque POP la base de données des comptes clients, les ISPs ont déployé une architecture centralisée, assurant la gestion à distance de leurs clients (*roaming*) et s'appuyant sur trois niveaux fonctionnels :

– l'utilisateur muni d'un login et d'un mot de passe (un *supplicant* en fait) ;

– le Network Access Server (NAS). Cette entité contrôle l'ensemble des modems et assure l'interface avec le serveur d'authentification, elle est analogue à un *authenticator* 802.1X ;

– le serveur RADIUS, jouant le rôle d'un serveur d'authentification 802.1X.

Ce dernier système assure l'interface avec la base de données gérant les comptes utilisateurs.

Le NAS réalise un pont applicatif entre des protocoles d'identification transportés par PPP et le serveur RADIUS. Par exemple, il transmet à ce dernier l'identité de l'utilisateur et son mot de passe. Le serveur RADIUS analyse ces paramètres et indique en retour le succès ou l'échec de cette investigation. Le NAS mesure également le temps d'utilisation du service par le client, et transmet une requête de facturation lorsque ce dernier quitte le POP.

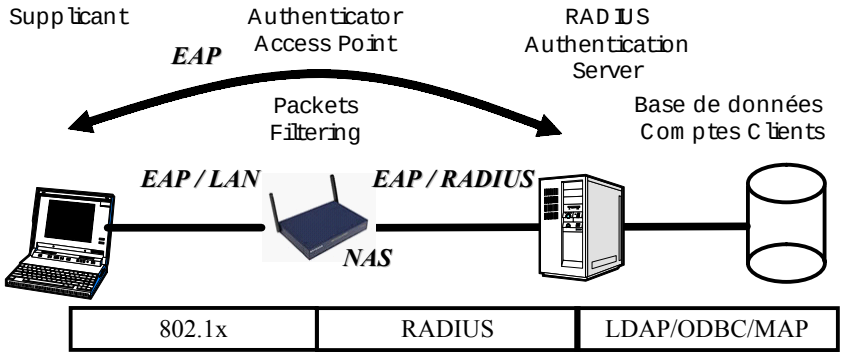

Figure 6. RADIUS et base de données clients

Le transport[12] quasi transparent du protocole EAP par RADIUS, permet de mettre en place une architecture générique, indépendante des méthodes d'authentification déployées par les ISPs.

La sécurité des échanges RADIUS est assurée à l'aide d'un secret partagé (mot de passe) entre serveur d'authentification et NAS. Elle emploie des signatures basées sur l'algorithme MD5 ; cependant certaines architectures utilisent IPSec pour renforcer la sécurité du lien avec le serveur d'authentification.

Bien que non standardisée, l'interface entre le serveur RADIUS et la base de donnée des comptes clients (SGBD, annuaire LDAP…) est un point essentiel. Dans certain cas, ces deux entités sont logées dans la même machine ; des locaux sécurisés sont cependant nécessaires pour éviter le pillage des données critiques. Lorsque la base cliente et le serveur RADIUS sont distants, un lien sécurisé est nécessaire (SASL[13], SSL, IPSec…).

IEEE 802.11i et WAP

Nous avons précédemment souligné les faiblesses du protocole WEP. La norme 802.1x définit un cadre pour l'authentification mais ne spécifie pas de manière détaillée la méthode de distribution des clés. D'autre part, le *Supplicant* ne participe pas au calcul de la clé WEP, il n'y a pas de procédure de mutuelle authentification entre *Supplicant* et point d'accès tirant profit de la disponibilité d'un secret partagé (la clé *unicast*).

Le groupe de travail IEEE 802.11i (IEEE Std 802.11i/D5.0, 2003) propose une architecture destinée à combler ces lacunes. Bien que ces travaux ne soient encore pas encore finalisés, un comité industriel a déjà édité une recommandation (WPA[14]) basée sur un sous-ensemble de cette norme émergente.

Nous classerons les apports de la norme IEEE 802.11i en trois catégories, définition de multiples protocoles de sécurité radio, éléments d'information permettant de choisir l'un d'entre eux et nouvelle méthode distribution de clés.

Le standard est dédié aux réseaux sans fil 802.11 et utilise 802.1x pour l'authentification et le calcul d'une clé maître nommée PMK (*Pairwise Master*

12. Ce transport est décrit dans la RFC 2869, RADIUS extensions, June 2000.
13. *Simple Authentication and Security Layer* (SASL), RFC 2222, October 1997.
14. *Wi-Fi Protected Access*, Version 2.0, April 29, 2003.

Key). Dans certain cas (mode *ad hoc* par exemple), cette clé rebaptisée PSK (*Pre Shared Key*) est distribuée manuellement.

Protocoles de sécurité radio

Deux protocoles de sécurité sont proposés :

– TKIP (*Temporal Key Integrity Protocol*), le successeur de WEP. Il met en œuvre l'algorithme de chiffrement RC4, et ajoute à chaque SDU[15] MAC une signature de 64 bits baptisée MIC (*Message Integrity Code*). La clé RC4 (128 bits) est calculée à partir d'un compteur de 48 bits (*Transmit Sequence*) transmis en clair dans chaque trame et d'une clé TK (*Temporal Key*) ;

– CCMP (*Counter-Mode/CBC-MAC*), utilise l'algorithme de chiffrement AES et une signature MIC. Les paramètres de chiffrement sont déduits d'un compteur de 48 bits (*Packet Number*) transmis en clair dans chaque trame et d'une clé TK.

Eléments d'information

Un point d'accès diffuse dans ses trames *Beacon* ou *Probe* des éléments d'information (IE, *Information Element*) afin de notifier au *Supplicant* les indications suivantes :

– la liste des infrastructures d'authentification supportées (typiquement 802.1X) ;

– la liste des protocoles de sécurité disponibles (TKIP, CCMP…) ;

– la méthode de chiffrement pour la distribution d'une clé de groupe (GTK).

Une station 802.11 notifie son choix par un élément d'information inséré dans sa demande d'association.

Distribution des clés

A la fin de la procédure d'authentification 802.1x, le *Supplicant* et le serveur d'authentification partagent la clé *unicast* rebaptisée *PMK*. Cette valeur est délivrée au point d'accès *via* le protocole RADIUS. A l'aide d'un protocole à quatre passes (*4-way Handshake*), transporté par des trames EAPoL-Key (voir figure 7), le supplicant et le point d'accès calculent une clé *PTK*. Cette valeur est générée par une fonction PRF (*Pseudo Random Function*)

15. *Service Data Unit*, la charge utile d'une trame.

avec comme arguments d'entrée les nombres aléatoires (*ANonce* et *SNonce*) fournis par le *Supplicant* et le point d'accès, ainsi que le secret partagé PMK.

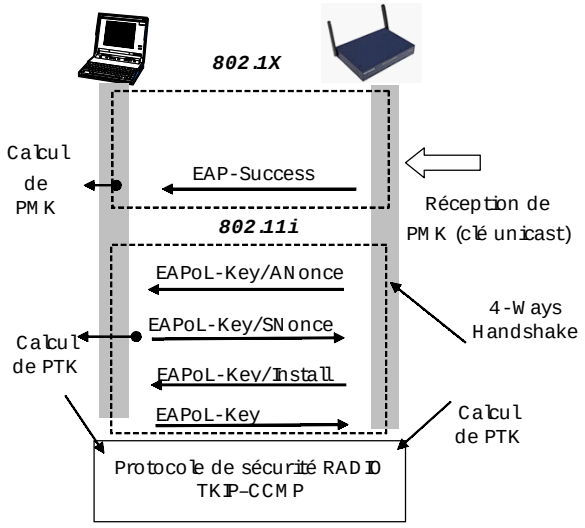

Figure 7. Le protocole à quatre passes 802.11i

La valeur PTK (voir figure 8) se décompose en plusieurs sous-clés, KCK qui assure la signature des messages EAPoL-Key, KEK associée au chiffrement de la clé GMK, et TK utilisée pour la sécurité des trames de données.

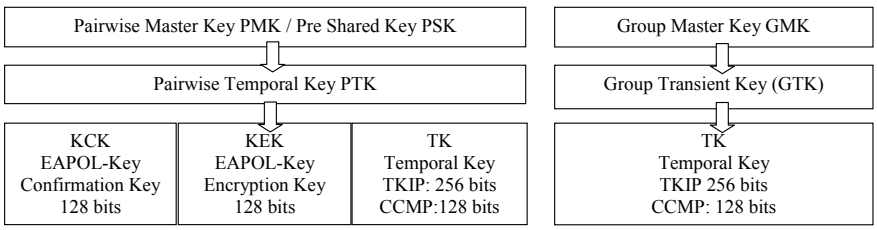

Figure 8. Hiérarchie des clés 802.11i

Le point d'accès dispose également d'une clé de groupe (*GMK*). Un protocole à deux passes (*2-way handshake*) permet de délivrer cette valeur

(chiffrée par *KEK*) et de déduire à l'aide d'un nombre aléatoire *GNonce* une clé temporaire de groupe (*GTK*).

Une approche verticale

Nous avons récemment proposés (Urien *et al.*, 2003a) un modèle à cinq niveaux décrivant l'architecture de sécurité des environnements sans fil Wi-Fi. Nous présentons ici brièvement les éléments du modèle.

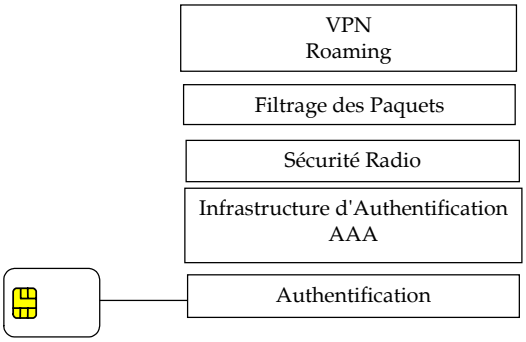

Figure 9. Modèle à cinq couches de la sécurité des réseaux 802.11

La *procédure d'authentification*. C'est la clé de voûte d'une infrastructure sécurisée. Il y a deux choix de base. L'utilisateur connaît ses clés d'authentification (symétriques, asymétriques…), et les protège à l'aide de mots de passe (par exemple, de manière analogue au logiciel libre *openssl*, une clé RSA privée est chiffrée par un triple DES, dont les clés sont déduites d'une phrase). L'utilisateur ne connaît pas les clés d'authentification qui sont la propriété du fournisseur de service. Une carte à puce par exemple, difficile à cloner, réalise après renseignement d'un code PIN les calculs d'authentification.

L'*infrastructure d'authentification*. La norme 802.1x recommande l'usage de serveur RADIUS. L'authentification peut être conduite par un serveur situé dans le domaine visité ou à l'extérieur de ce dernier. De manière analogue à PGP (*Pretty Good Privacy*), cette architecture établit un cercle de confiance, grâce auquel un message d'authentification est relayé par plusieurs serveurs, liés les uns aux autres par des associations de sécurité.

La *sécurité radio.* Elle assure la confidentialité, l'intégrité et la signature des paquets. Ces services sont assurés par des protocoles tels que WEP ou TKIP ou CCMP normalisés par le comité IEEE 802. Ils utilisent des clés cryptographiques (chiffrement, signature trames), déduites d'une clé maître, au terme de la procédure d'authentification.

Le *filtrage des paquets*. La fiabilité de cette opération repose sur la signature des paquets. Grâce à ce mécanisme, les trames qui pénètrent dans le système de distribution sont sûres (pas de risque de *spoofing*), les systèmes de filtrages (point d'accès ou portail) gèrent les privilèges des paquets IP (destruction des paquets illicites) et par exemple peuvent réaliser et facturer des services de QoS (qualité de service).

L'*accès à des services distants* (*roaming*) que nous désignons de façon générique sous l'appellation services VPN (*Virtual Private Network*). Par exemple, on mettra en œuvre des liens sécurisés (interdomaine) à l'aide des protocoles IPSec ou SSL.

Conclusion

Dans cet article, nous avons présenté les architectures de sécurité qui sont en cours de déploiement ou de définition pour les réseaux 802.11. Compte tenu de l'engouement du marché sur l'IP sans fil, il est probable que ces technologies deviennent des standards incontournables et jouent un rôle prépondérant dans l'informatique enfouie, qui ne pourra se développer sans normes de sécurité éprouvées.

Bibliographie

Arbaugh W., Shankar N., Wan J.Y.C., « Your 802.11 Wireless Network has No Clothes », Department of Computer Science, University of Maryland, College Park, March 2001, http://www.cs.umd.edu/~waa/wireless.pdf

Borisov N., GoldBerg I., Wagner D., « Intercepting Mobile Communications: The Insecurity of 802.11 », *Proceeding of the Eleventh Annual International Conference on Mobile Computing And Network*, July 16-21, 2001, p. 180.

Fluhrer S., Mantin I., Shamir A., « Weakness in the key scheduling algorithm of RC4 », *8th Annual Workshop on Selected Areas in Cryptography*, August 2001.

IEEE Std 802.11, « Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications », 1999.

IEEE Std 802.1X, « Standards for Local and Metropolitan Area Networks: Port Based Access Control », June 14, 2001.

IEEE Std 802.11i/D5.0, « Draft Supplement to standard for Telecommunications and Information Exchange, Between Systems LAN/MAN Specific Requirements Part 11 : Wireless Medium Access Control (MAC) and physical layer (PHY) specifications : Specification for Enhanced Security », August 2003.

Mishra A., Arbaugh W., « An Initial Security Analysis of the IEEE 802.1X standard ». February 2002.

Urien P., Pujolle G., « Architecture sécurisée par cartes à puces, pour des réseaux sans fil sures et économiquement viables », *GRES'2003*, Fortaleza Brésil, février 2003 (a).

Urien P., Loutrel M., « The EAP Smartcard, a tamper resistant device dedicated to 802.11 wireless networks, ASWN 2003 », *Third workshop on Applications and Services in Wireless Networks*, Berne Suisse Juillet 2003 (b).