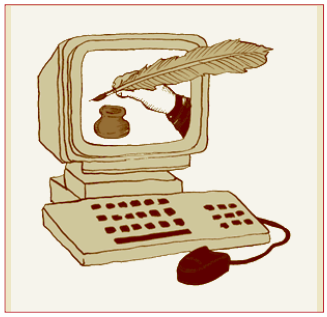
SÉCURITÉ INFORMATIQUE

numéro 40 juin 2002

SÉCURITÉ DES SYSTÈMES D'INFORMATION

Prudence est mère de sécurité



éditorial

Il en va des systèmes d'information comme d'un grand magasin parisien bien connu : pas une heure ne s'écoule sans qu'il ne s'y passe quelque chose. Le slogan est largement vérifié par la statistique lorsqu'il s'agit d'actes de malveillance, lorsqu'un virus en chasse un autre, lorsqu'un « spam » avec usurpation d'adresse électronique vole quelques précieuses heures de travail à nos administrateurs de réseau ou encore lorsque sont installés portes dérobées dépourvues de tout caractère romanesque ainsi que fichiers aussi illégaux que consommateurs de bande passante. Il est vérifié également, sur un mode plus positif heureusement, par les arrivées de produits nouveaux et de technologies innovantes.

Ainsi, les réseaux sans fil font-ils actuellement leur entrée en fanfare. Chaque fabriquant nous en vante les mérites : une plus grande souplesse d'organisation, une liberté supérieure pour l'utilisateur et une facilité accrue de reconfiguration des infrastructures réseau pour l'administrateur système. Les apports évidents de cette nouvelle technologie associés à son faible coût d'accès permettent d'augurer sans prendre trop de risque, qu'avant longtemps le sans fil sera partout.

Pourtant, il faut mettre en garde : les réseaux sans fil ne permettent d'assurer d'une manière certaine ni l'authentification des utilisateurs, ni la confidentialité et l'intégrité des données, ni la disponibilité des services. Bref, cette technologie reste très fragile. Allons-nous voir se généraliser cette situation ubuesque où les utilisateurs de réseaux locaux traditionnels se font imposer de lourdes procédures de sécurité tandis que n'importe qui, avec un ordinateur portable équipé de la carte idoine, peut tranquillement, de sa place de parking, capturer le trafic, modifier les données ou rentrer dans le réseau avec les droits qu'il veut.

Ce numéro est un peu plus technique qu'à l'ordinaire – raison oblige ! Les deux articles qui en constituent le corps, l'un d'un universitaire, l'autre d'un industriel, donnent deux points de vue complémentaires… et convergents sur la faiblesse des protocoles mis en œuvre. Des pistes sont ouvertes qui nous promettent des solutions plus satisfaisantes… pour demain bien sûr. Mais pour aujourd'hui ?

Aujourd'hui, il convient pour les instances de décision de bien analyser et d'apprécier les enjeux, de savoir éventuellement résister au caractère séduisant d'une technologie nouvelle en n'assimilant pas « émergence de celle-ci sur le marché » avec « perception d'un besoin aussi nouveau qu'impérieux ». Laissons aujourd'hui devenir demain, laissons aux techniciens le temps de mettre au point les solutions sécurité et adaptons, s'il y a lieu, l'architecture de nos réseaux à l'accueil de la nouvelle technologie.

suite page 6

Réseaux locaux sans fil : aussi dangereux que séduisants

Les réseaux locaux sans fil sont mûrs, abordables et se multiplient mais ils posent des problèmes de sécurité d'autant plus sérieux qu'ils sont censés avoir des mécanismes de chiffrement et d'authentification qui, outre qu'ils ne sont pas toujours activés, se révèlent vulnérables.

Principe d'un réseau local sans fil

Un réseau local sans fil, souvent appelé WLAN (Wireless LAN) dans la littérature, ou encore Réseau Local Radioélectrique (RLR), permet de remplacer une ou plusieurs liaisons matérielles de transmission de données par des ondes radio-électriques.
Il faut pour cela résoudre un certain nombre de problèmes : choix des fréquences utilisées, de la puissance d'émission, de la bande passante envisagée et, donc, du type de modulation et du spectre, régir le partage et donc l'accès à la liaison par plusieurs équipements, prendre en compte les interférences éventuelles, la réglementation, etc.
Si plusieurs solutions techniques ont vu (ou vont voir) le jour (*cf.* encadré page 2 : « Les principales technologies de réseaux sans fil »), le standard dominant aujourd'hui est le 802.11b de l'IEEE avec sa version labélisée Wi-Fi (1). Il offre une portée d'une centaine de mètres et un débit théorique de 11Mb/s. Même si le débit pratique ne dépasse guère la moitié de ce chiffre, c'est largement suffisant pour des clients « légers » qui voient ce type de réseau comme un réseau ethernet.

Réglementation

Les équipements 802.11b utilisent la bande des 2,4GHz (applications scientifiques, industrielles et médicales). En France l'utilisation en est libre à l'intérieur de bâtiments privés, est soumise à demande auprès de l'ART pour utilisation à l'extérieur sur un domaine privé, et est interdite sur le domaine public (2).

Coûts, disponibilité

Les équipements 802.11b sont disponibles sous de nombreuses marques (le nombre effectif de fabricants est bien plus faible) comme Lucent/Orinoco, Apple, D-Link, SMC, Aironet/Cisco, 3Com, Intel…

suite page 2

CNRS CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

suite de la page 1

Plusieurs configurations de mise en œuvre sont possibles suivant l'utilisation envisagée, celle rencontrée le plus souvent en environnement professionnel est celle dite «infrastructure» où les équipements communiquent *via* un ou plusieurs points d'accès qui se comportent en pont ethernet.

Le coût d'un point d'accès pouvant accueillir plusieurs dizaines d'utilisateurs est de l'ordre de 330 à 800 euros HT et celui d'un adaptateur Wi-Fi au format PCI ou PCMCIA est de l'ordre de 150 à 230 euros HT. Il existe même des cartes Wi-Fi au format CF particulièrement adapté aux PDAs et on trouve maintenant des portables intégrant un adaptateur 802.11b et son antenne en standard.

Outre Windows, la plupart des adaptateurs Wi-Fi sont supportés sous Linux et une partie sous PocketPC.

Domaine d'utilisation des RLR

- remplacement à moindre frais du câblage de tout ou partie d'un bâtiment (un point d'accès partagé plus un adaptateur peuvent coûter moins cher que d'installer une prise, surtout dans un bâtiment difficile) ;
- raccordement rapide d'équipements sans les démarches et les délais d'extensions d'un réseau existant ;
- offrir l'accès au réseau de l'entreprise aux équipements nomades (portables, PDAs...) qui, par nature, n'aiment pas les fils ;
- montage d'un réseau pour des manifestations temporaires (salons, démonstrations...) ;
- bornes d'accès dans des lieux publics (aéroports, gares...).

Un des gros avantages de la technologie Wi-Fi est sa facilité de déploiement : il suffit d'une prise de courant et d'un accès réseau. Les valeurs par défaut des paramètres de configuration permettent souvent un fonctionnement immédiat (mais non sécurisé).
Si les RLRs sont de plus en plus attractifs dans un contexte professionnel, la baisse des coûts en favorise la dissémination dans le grand public, aidée par le choix de quelques grands constructeurs comme Apple avec son AirPort2 (maintenant compatible Wi-Fi). Certaines études prévoient d'ailleurs une baisse des coûts de la technologie 802.11b de moitié au cours de 2002. On peut déjà trouver des points d'accès à 170 euros TTC (1 100 francs), des adaptateurs USB, des ponts câble/xDSL-802.11b... De quoi partager un accès ADSL ou câble en tout confort sans se ruiner !

Les problèmes

Absence de maîtrise du support

Comme toute émission radio, celle des RLR se propage dans un volume centré sur l'antenne d'émission et peut donc être captée par tout autre récepteur et par une antenne appropriés placés dans ce volume. Concrètement, tout autre adaptateur 802.11b, placé à portée d'un RLR, peut potentiellement révéler les données échangées, voire donner accès à celui-ci si des précautions ne sont pas prises.

La portée dépasse plus ou moins largement le bâtiment dans lequel se trouve l'antenne d'émission : même si un RLR Wi-Fi est au centre d'un campus de plusieurs centaines de mètres de rayon, l'utilisation d'antennes directionnelles (disponibles dans le commerce ou à fabriquer soi-même) sur un équipement pirate, peut décupler sa zone de couverture, le rendant ainsi accessible depuis l'enceinte, le site du concurrent, la cité universitaire voisine...

Faiblesse du contrôle d'accès

Pour accéder à un réseau Wi-Fi, il est généralement (mais pas toujours) nécessaire de connaître son identifiant (le SSID), mais, outre qu'il peut être laissé à la valeur par défaut du constructeur, il est annoncé en permanence par les points d'accès (beacon) ce qui permet à certains clients d'offrir le choix des réseaux disponibles à l'utilisateur.
Un contrôle par adresse MAC est souvent offert sur les points d'accès mais, même s'il est mis en œuvre, il peut facilement être contourné car la plupart des adaptateurs permettent de modifier leur adresse...

Situation et conditions d'installation des RLRs dans l'infrastructure réseau

Les problèmes ci-dessus sont fortement aggravés par le fait que les points d'accès sont généralement installés à l'intérieur des périmètres protégés par les pare-feux et souvent installés à l'insu de l'administrateur réseau (et du RSSI)...

Les attaques

Ces particularités ont engendré un nouveau «sport» en vogue outre-Atlantique : le *war-driving*. Il suffit d'un portable avec un adaptateur Wi-Fi, éventuellement une antenne améliorée, un des logiciels spécialisés disponibles sur l'Internet, éventuellement

suite page 3

Les principales technologies de réseaux sans fil

IEEE 802.11b
Normalisé en 1997, et promu également sous le label Wi-Fi de l'alliance WECA, il offre un débit théorique de 11 Mb/s pour une portée d'une centaine de mètres. Il utilise une bande de fréquence libre d'utilisation dans la plupart des pays autour de 2.4GHz en utilisant une modulation de type DSSS. Il émule un réseau ethernet et supporte donc le protocole IP sans problème mais n'offre pas de qualité de service. De nombreux produits 802.11b étant maintenant disponibles (et interopérables) et abordables, cette technologie est en plein essor et ne vise plus seulement les utilisateurs professionnels. Certains la verraient même se substituer, dans certaines conditions, à la téléphonie de 3e génération pour la transmission de données...
Des évolutions, offrant jusqu'à 54Mb/s, sont en cours de standardisation sous les références 802.11a (interdit en Europe) et 802.11g.

HomeRF
Né en 1998 à l'initiative du Home Radio Frequency Working Group rassemblant Compaq, HP, IBM, Intel et Microsoft, HomeRF, dérivé du standard 802.11, est orienté usage domestique. Paradoxalement, il offre une gestion de qualité de service et une meilleure sécurité que le WEP mais est concurrencé par Wi-Fi. Il permet de transporter des données et de la voix sur une liaison DECT. Peu de produits existent et, Intel et Microsoft s'étant ralliés à Wi-Fi, HomeRF semble condamné.

HiperLAN 1 et 2
Standard européen de l'ETSI initié en 1992, HiperLAN 1 offre un débit de 20Mb/s dans la bande des 5GHz contre 54Mb/s pour sa version 2. Utilisant la même couche physique que 802.11 (OFDM), il n'est néanmoins pas compatible avec lui car sa couche MAC se rapproche plus d'ATM que d'ethernet. Le principal défaut d'HiperLAN est d'être européen mais, si HiperLAN 1 n'a jamais vu le jour, des produits HiperLAN 2 sont attendus dans les prochains mois.

Bluetooth
Lancé en 1994 par Ericsson, il a vocation à permettre l'échange de données entre appareils numériques portables à courte distance (10 m), avec un débit théorique de 1Mb/s, sur la bande des 2.4GHz. Ses points forts sont sa faible consommation énergétique et le support de données synchrones comme la voix. Après bien des promesses les produits Bluetooth arrivent enfin sur le marché, mais à des prix pour l'instant nettement supérieurs à ce que ses promoteurs laissaient espérer. Une évolution est en préparation : Bluetooth 2, qui devrait offrir des débit de 2 à 10 Mb/s.

suite de la page 2

couplé à un GPS, à bord d'un véhicule se promenant aux abords des sites «intéressants» pour y repérer les RLRs. Une variante encore plus légère, à base de PDA, connaît un grand succès.

Nul doute que cette activité ne trouve quelques adeptes sur ou autour de nos campus…

Pour résumer : sans précautions spécifiques, l'installation d'un réseau 802.11b revient à offrir un accès public à son réseau interne !

La (fausse) réponse : Wired Equivalent Privacy (WEP)

WEP fait partie du standard 802.11, il est censé donner une réponse aux problèmes de sécurité inhérents aux RLRs :

- confidentialité : empêcher n'importe qui d'écouter les données circulant sur le RLR,
- contrôle d'accès : empêcher n'importe qui d'utiliser le RLR,
- intégrité des données : empêcher toute modification des données échangées.

Autrement dit, offrir le même niveau de sécurité qu'un réseau ethernet filaire. Pour cela, le WEP fait appel au mécanisme de chiffrement RC4 avec des clés de 40 ou 104 bits.

Mais…
Se pose le problème de la gestion des clés qui n'est pas traité par le WEP : généralement tous les utilisateurs partagent la même, qui est stockée en clair sur un équipement mobile (fichier ou adaptateur suivant les constructeurs), donc exposé, et, si un utilisateur la perd, il faut la remplacer par une autre sur tous les équipements. C'est donc un processus contraignant.

Pis : il a été montré que les choix effectués pour le WEP sont au mieux hasardeux, au pire vont à l'encontre des buts visés (3,4).

Conséquence : aucun n'est atteint ! Un attaquant peut en effet s'immiscer dans le réseau, falsifier des paquets et les déchiffrer sans même connaître la clé de chiffrement ! De toute façon celle-ci peut être découverte grâce à un logiciel comme AirSnort (7) rien qu'en écoutant passivement le trafic d'un RLR… !

En résumé : même en utilisant le WEP, les RLRs de type Wi-Fi n'offrent aucune garantie de confidentialité, de contrôle d'accès ni d'intégrité !

Solutions

Il n'existe malheureusement pas de solution simple pour sécuriser un RLR 802.11b. En attendant 802.11i (chiffrement AES et gestion de clés utilisateur) et 802.1x (authentification EAP et contrôle d'accès à base de certificats, promu par Cisco et Microsoft, dans lequel des failles ont déjà été découvertes (5)) qui demanderont des mises à jour, il faut mettre en œuvre des solutions éprouvées, mais plus ou moins lourdes comme les VPNs, IPSec, SSL/TLS, HTTPS (pas toujours exemptes de faiblesses et souvent incompatibles avec une gestion de qualité de service).

Il existe quelques extensions propriétaires ou anticipant les standards cités, mais qui ne sont envisageables que dans un environnement homogène.

Conclusion

Si la technologie Wi-Fi est le rêve des utilisateurs, elle peut être le cauchemar des administrateurs réseau du fait de ses caractéristiques intrinsèques, de sa facilité de déploiement «sauvage» et des promesses non tenues du WEP. Son utilisation doit se faire en connaissance de cause en appliquant un maximum de précautions comme celles ci-dessous.

Recommandations

- Avoir connaissance des RLRs déployés sur son site (au besoin utiliser les méthodes des war-drivers).
- Attention aux accès SNMP sur les points d'accès.
- Ne pas utiliser le SSID «anonyme» (ou vide), mais en choisir un non trivial et en empêcher la diffusion par les points d'accès (réseau fermé).
- Utiliser les dernières versions de *firmware* et de logiciels.
- Empêcher l'accès à l'interface d'administration des points d'accès *via* le RLR.
- Considérer ces réseaux comme le reste de l'Internet et y appliquer au moins les mêmes règles de sécurité (filtres, DMZ, firewalls, proxies, authentification, VPNs, SSL, IPSec, HTTPS…) que pour les accès extérieurs à votre réseau.

Sinon, en ayant conscience des limites de ces solutions :

- Utiliser le WEP, même s'il est imparfait, avec des clés non devinables (chiffres hexadécimaux) changées régulièrement et protéger les équipements les contenant.
- Utiliser les ACLs sur les points d'accès quand c'est possible.
- Utiliser éventuellement les solutions propriétaires si vous n'avez qu'un fournisseur.
- Faire de l'information pour empêcher les déploiements sauvages.

Christian Claveleira,
Ingénieur au Comité Réseaux des Universités,
Christian.Claveleira@cru.fr

Références

[1] Wireless Ethernet Compatibility Alliance (http://www.wirelessethernet.org/)
[2] ART. Cadre réglementaire et fréquences des réseaux locaux radioélectriques (http://www.art-telecom.com/dossiers/rlan/index-d.htm)
[3] Borisov, Goldberg, Wagner. Intercepting Mobile Communications: The Insecurity of 802.11 (http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf)
[4] Goldberg. An analysis of the Wired Equivalent Privacy protocol. Black Hat Briefings. (http://www.cypherpunks.ca/bh2001/)
[5] Mishra, Arbaugh. An Initial Security Analysis of the IEEE 802.1x Standard (http://www.cs.umd.edu/~waa/1x.pdf)
[6] The Unofficial 802.11 Security Web Page (http://www.drizzle.com/~aboba/IEEE/)
[7] AirSnort Homepage (http://airsnort.shmoo.com/)

Journées Techniques Réseaux

Les prochaines Journées Techniques Réseaux (JTR'2002), organisées par l'université de Limoges, le CRU et l'UREC, seront consacrées aux technologies de réseaux et d'interconnexions sans fil. Du 14 au 16 octobre 2002 à Limoges.
Objectifs : donner aux ingénieurs systèmes et réseaux qui réfléchissent à la mise en place de nouvelles architectures réseaux dans un environnement MAN, Campus, Institut ou Laboratoire, une expertise sur les technologies des réseaux sans fils.
Le programme et les inscriptions seront accessibles à :
http://jtr2002.unilim.fr/

Sécurité des réseaux sans fil

Interview de M. Pascal Urien (SchlumbergerSema)

Robert Longeon : *Monsieur Pascal Urien, vous travaillez à SchlumbergerSema dans la division «Smartcard Research Center». Vous vous intéressez depuis longtemps à la délicate question de l'authentification forte. Vos interventions à JRES (les journées réseaux organisées par le UREC et le CRU tous les deux ans) sont toujours très appréciées. Vous participerez aussi au séminaire vCars, organisé par le CNRS en partenariat avec l'INRIA en septembre prochain. Vous avez fait à InfoSec une intervention très remarquée sur la sécurité des réseaux sans fil. La technologie sur laquelle vous travaillez a été deux fois primée lors de salons internationaux (Meilleure innovation technologique cartes'2000, produit le plus innovant de l'année Advanced Awards 2001). Je vous remercie d'avoir accepté de répondre à mes questions. Tout d'abord, qu'y a t-il de nouveau du point de vue de la sécurité avec ces réseaux ?*

Pascal Urien : Jusqu'à présent les réseaux locaux traditionnels (par opposition à ceux «sans fil») ont été déployés sans protection particulière de leurs points d'accès. Typiquement ils sont organisés autour d'un arbre de HUBs (généralement fonctionnant en mode commutateur de paquets) auxquels sont reliées des stations de travail, à l'aide de prises RJ45 qui matérialisent les points d'accès au réseau (que la norme IEEE 802.1x nomme des ports d'accès). L'entrée d'un établissement étant contrôlée et réservée au personnel autorisé, les ports d'accès ne sont usuellement pas sécurisés, en particulier pour permettre la connexion des ordinateurs portables depuis divers emplacements.

Un réseau 802.11 (le réseau sans fil) est un ensemble de cellules de base (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 (*cf.* figure 1). L'ensemble de ces cellules (c'est-à-dire les APs) 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.

La taille des cellules de base, dont le rayon est voisin d'une centaine de mètres, permet un nouveau type d'attaque, dite attaque par le garage ((1) parking Lot attack). En l'absence de mesures de sécurité appropriées, un pirate possédant un ordinateur portable muni d'une carte IEEE 802.11b de coût inférieur à 150 euros se connecte au réseau intranet d'une entreprise ou d'un particulier, par exemple en stationnant son véhicule à proximité des locaux visés.

Conscient de ces contraintes la norme IEEE 802.11 (4) a introduit un protocole de sécurité (WEP), qui a pour objectif d'assurer les fonctions suivantes :

- Authentification d'un utilisateur.
- Confidentialité des données échangées sur les canaux radio.
- Garantie de l'intégrité des données.

Cependant cette spécification présente des failles importantes, et de nombreux logiciels disponibles sur le WEB permettent d'obtenir rapidement les clés RC4 de chiffrement et d'authentification (*cf.* encadré) ; en l'état actuel, les réseaux 802.11 offrent donc une sécurité quasi nulle (1,2,3).

R. L. : *Rentrons un peu plus dans les détails. Pouvez-vous nous décrire une trame WEP ?*

P. U. : Une trame 802.11 comporte les éléments suivants :

- un en-tête (MAC header) qui décrit la nature de la trame, les adresses des entités source et destination, et diverses informations ;
- un corps de trame (body) dont la longueur varie de 0 à 2312 octets ;
- un CRC (Cyclic Redundancy Code) de 4 octets assure le contrôle d'intégrité des données.

Un bit de l'en-tête MAC indique l'éventuel chiffrement du corps de trame et du CRC à l'aide du protocole WEP. La structure de la trame (figure 2, page 5) est alors la suivante :

- l'en-tête MAC,
- un champ IV (Init Vector) large de 3 octets,
- un octet, dont les six premiers bits sont à zéro et dont les deux derniers indiquent un index de clé (KeyID),
- une zone chiffrée par une clé RC4 de 64 bits déduite de la valeur IV et de l'indice KeyID. Ce bloc englobe le corps de trame et le CRC.

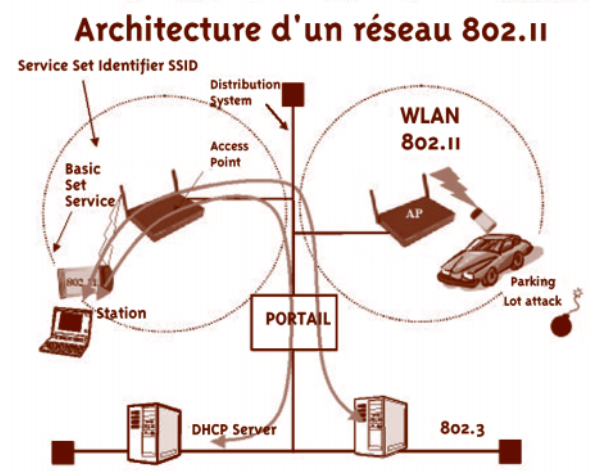


Figure 1

La clé de chiffrement RC4 d'une trame, large de 64 bits, est obtenue par la concaténation d'une partie secrète de 40 bits (une parmi quatre, dont l'indice KeyID est compris entre 0 et 3) et le vecteur IV (24 bits).

Il existe seulement deux puissance vingt-quatre (environ 16 millions) valeurs différentes du champ IV, soit encore deux puissance vingt-quatre keystreams distincts par secret partagé. Un attaquant peut facilement diffuser une trame dont il connaît le contenu en clair (courrier électronique, URL, etc.), puis déduire des trames chiffrées les différents keystreams générés par le protocole WEP. L'attaque de base ne consiste pas à une attaque force brute, visant à casser des clés RC4 de 64 bits, mais à enregistrer les 16 millions de keystreams qui réalisent l'authentification des utilisateurs et la confidentialité des informations échangées.

Remarquons également que conformément au paradoxe des anniversaires (dans un groupe de 23 personnes il y a 50 % de chance que deux dates d'anniversaire soient identiques), un même IV sera réutilisé au bout de 4823 trames avec une probabilité de 50 %.

suite page 5

Le protocole WEP utilise l'algorithme de chiffrement RC4

RC4 permet de chiffrer des données en mode flux octets (stream cipher) : à partir d'une clé de longueur comprise entre 8 et 2048 bits, on génère (à l'aide d'un pseudo random generator PRNG) une suite d'octets pseudo aléatoire nommée KeyStream. Cette série d'octets (Xsi) est utilisée pour chiffrer un message en clair (Mi) à l'aide d'un classique protocole de Vernam, réalisant un XOR (ou exclusif) entre Xsi et Mi (Ci = Xsi XOR Mi).

Il n'est pas recommandé d'utiliser plusieurs fois une clé RC4, parce que la connaissance d'un octet en clair (Mi) et chiffré (Ci) permet de déduire la valeur du KeyStream (Xsi) correspondant (Ci xor Mi = Xsi xor Mi xor Mi = Xsi).

suite de la page 4

R. L. : *La confidentialité des données ne peut donc pas être garantie. N'y a t-il pas aussi quelques faiblesses – pour utiliser un euphémisme – dans le processus d'authentification ?*

P. U. : Le processus d'authentification se déroule de la manière suivante. Un point d'accès (AP) émet périodiquement une trame balise (*beacon frame*). Une station qui désire rejoindre la cellule émet une demande d'association acquittée par le point d'accès. Une fois cette opération réalisée, la station s'authentifie auprès du réseau grâce à un scénario en quatre passes :

- La station transmet une requête d'authentification (Authentication Request).
- Le point d'accès produit un challenge (Authentication Challenge) de 128 octets en clair.
- La station encode ce nombre de 128 octets à l'aide d'une trame WEP (Authentication Response), associée à un IV 24 bits et un KeyID de 2 bits.
- Le point d'accès notifie l'échec ou la réussite de l'opération (Authentication Result).

La connaissance du message en clair (challenge de 128 octets) et du message chiffré permet de déduire les 128 premiers octets du keystream généré à partir du vecteur IV et du KeyID. Une conséquence immédiate est que l'on peut, par simple écoute, récupérer un triplet (IV, KeyID, keystream) réutilisable pour un autre processus d'authentification (3). Il est donc banal d'usurper une identité (Authentication Spoofing).

R. L. : *Pas de garantie dans la confidentialité et l'authentification. Peut-on au moins avoir confiance dans l'intégrité des messages ?*

P. U. : Une propriété remarquable des CRCs (3) est que le ou exclusif (octets à octets) de deux trames de même longueur est associé à un CRC obtenu par un ou exclusif des deux autres CRCs. A partir d'une trame en clair et de son CRC, il est donc possible de modifier une trame chiffrée tout en recalculant un CRC correct (Mi XOR Ksi XOR Mi' = Mi XOR Mi' XOR Ksi est associé au CRC chiffré CRCi XOR Ksi XOR CRCi' = CRCi XOR CRCi' XOR Ksi). Le protocole WEP n'assure donc pas l'intégrité des données.

Le successeur de WEP, WEP2 propose de mettre en œuvre des vecteurs IV de 128 bits, et des secrets partagés de 40, 104 ou 128 bits. Cependant la grande faiblesse de WEP provient de l'utilisation de clés RC4 fixes et donc de l'absence d'architecture d'authentification et de distribution de clés de session.

R. L. : *Une situation aussi intolérable doit susciter des réactions de la part des industriels. Vers quelle réponse semble aller aujourd'hui l'industrie ?*

P. U. : De manière générale, un système informatique est connecté à un réseau à travers un port d'accès qui peut utiliser un lien filaire (modem, prise RJ45) ou sans fil (interface radio…). L'insertion dans un réseau IP implique l'obtention d'une adresse IP et de divers paramètres (masque de réseau, serveur DNS, adresse de passerelle…) parfois obtenus au moyen du protocole DHCP, qui n'offre guère de moyens pour authentifier un client. En conséquence il est prudent d'authentifier un utilisateur avant l'attribution d'une adresse IP ; par exemple un internaute qui utilise le classique protocole PPP s'identifie auprès de son ISP à l'aide d'un login et d'un mot de passe, avant d'obtenir une adresse IP.

L'IEEE étudie à travers le groupe 802.1x (Port Based Network Access Control (5)) une architecture d'authentification applicable en mode filaire et sans fil. L'idée est d'interdire les services disponibles sur le réseau à un nœud (identifié par son adresse MAC 802) non authentifié. De manière logique, un client (supplicant system) est connecté au fournisseur de services *via* un port d'accès (par exemple le port d'un HUB ethernet). Le client utilise le protocole EAP (Extended Authentication Protocol - RFC 2284) pour être authentifié par son réseau d'accès ; puisque ce processus intervient avant l'attribution d'une adresse IP, EAP est transporté par des trames IEEE 802 (EAP encapsulation over LAN, en abrégé EAPOL dont le SNAP est égal à AA AA 03 00 00 00 88 8E) ou PPP (avec le numéro de protocole C227). EAP peut être perçu comme un protocole de type parapluie, il véhicule deux types de messages (requêtes et réponses) associés à différents types de schéma (type field) d'authentification tels que :

- MD5 challenge, production d'un digest MD5 à partir d'un nombre aléatoire et d'un secret partagé.

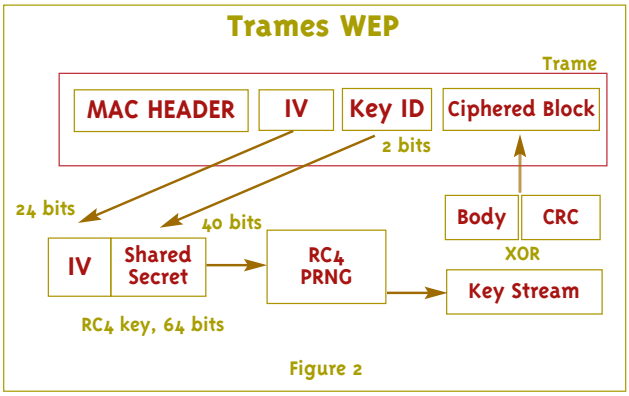


Figure 2

- Protocole d'authentification dit PPP EAP TLS (rfc 2716) basé sur SSL.
- IAKERB, adaptation des mécanismes d'authentification de Kerberos V5.
- EAP SIM, utilisation des cartes SIM (GSM 11.11).
- EAP AKA, mise en œuvre des cartes USIM (définies pour l'UMTS…).

Nous remarquerons également que le protocole EAP est intégré au système d'exploitation Windows XP.

Lorsqu'un nouveau client apparaît dans le réseau, il conduit une procédure d'authentification à l'aide du protocole EAP. Il est possible que le réseau visité soit incapable de vérifier l'identité de son hôte et d'établir le cas échéant ses droits. Dans ce cas, le système d'authentification local peut transférer les messages EAP vers un serveur d'authentification distant. IEEE 802.1X suggère d'utiliser le protocole RADIUS (RFC 2865) pour réaliser cette opération (EAP within RADIUS RFC 2869). RADIUS a été conçu outre-Atlantique pour permettre à un ISP, auquel un internaute n'est pas abonné, de vérifier son identité et ses droits auprès d'un autre ISP gérant son compte et ses droits. Il permet de transférer les procédures d'authentification entre ISPs et de répartir la rémunération du service entre plusieurs ISPs.

Une des contraintes du réseau sans fil 802.11 est de conduire une authentification répartie entre plusieurs points d'accès et une station. L'avantage d'une architecture 802.1X est d'être centralisée, ce qui facilite la gestion des comptes utilisateurs (et donc des droits) et renforce la sécurité par l'attribution de clés de sessions éphémères. Cependant ce standard présente encore des failles (6) de type Man In the Middle (MIM).

Une architecture proche, dite OWLAN (Operator Wireless LAN (7,8)), réalise le prolongement naturel, en mode sans fil, du réseau paquets GPRS d'un opérateur mobile. Cette extension se matérialise côté utilisateur sous la forme d'une carte 802.11b munie d'un lecteur de carte SIM. L'idée directrice est de permettre l'échange de données entre le réseau GPRS d'un opérateur et un réseau local muni de points d'accès sans fil. Un des avantages de cette approche réside dans l'utilisation de systèmes d'authentification (MSC/HLR) et de facturation (GPRS Charging Gateway) déjà déployés.

R. L. : *Vous travaillez plus particulièrement sur l'authentification des stations mobiles par carte SIM-IP. C'est cette technologie qui a été deux fois primée. Voulez-vous en décrire rapidement les principes ?*

P. U. : Un module SIM-IP est une carte à puce particulièrement adaptée aux services des réseaux IP de nouvelles générations qui pourront servir de support aux communications sans fil de 4e génération (802.11…). Ainsi que nous l'avons souligné précédemment, l'authentification de l'utilisateur est un prérequis pour le contrôle des accès, d'autres procédures d'identification peuvent également être nécessaires à la mise en œuvre de services offerts par différents opérateurs. En conséquence une carte SIM-IP doit embarquer plusieurs procédures d'authentifications relatives à différents environnements, par exemple :

- des fonctions à base d'empreinte (MD5 digest,…) et de secret partagé (Keyed-Hashing),

suite page 6

suite de la page 5

- des procédures de type Kerberos, utilisant une clé DES,
- des algorithmes importés des normes SIM ou USIM.

Le protocole EAP et les internet draft associés fournissent un cadre bien adapté pour la normalisation des procédures d'authentification. De surcroît, il semble indispensable de disposer d'une description standardisée des ressources embarquées afin d'une part de les identifier, et d'autre part de permettre leur mise en œuvre automatisée par des logiciels applicatifs. Parce que la syntaxe XML est devenue le standard incontournable de présentation de données, nous suggérons de décrire la structure d'un module SIM-IP à l'aide de documents XML, conformes à des DTDs normalisés.

Nous utilisons une technologie émergente de cartes à puce internet (9,10,11) permettant, grâce à une pile de communication distribuée entre carte et terminal, d'embarquer des applications client/serveur dans une puce ISO 7816. De manière synthétique, un module SIM-IP comporte les éléments suivants :

- des données, réalisant le profil d'un utilisateur relativement à un service et aux logiciels dédiés. Certaines informations sont détenues par le porteur de la carte, d'autres sont la propriété d'opérateurs (secrets partagés, clés RSA…) ;
- des procédures qui, par exemple, effectuent des algorithmes d'authentification à l'aide de clés cryptographiques ;
- des protocoles qui permettent de conduire des opérations diverses depuis le module SIM-IP (négociation de qualité de service…) sans une configuration préalable du terminal ;
- des agents (code java) utiles pour conduire des programmes nécessitant une puissance de calcul supérieure à celle disponible sur la carte.

R. L. : *Vous avez donc la solution aux problèmes que posent les réseaux sans fil…*

Cette approche fera l'objet d'études plus approfondies dans le cadre du projet MMQoS (www.mmqos.org Maîtrise de la Mobilité et de la Qualité de Service pour la 4e génération de réseaux mobiles) labellisé en 2001 par le comité RNRT (Réseau National de la Recherche en Télécommunications).

Références

[1] W. Arbaugh, N. Shankar, and Y. Wan, Your 802.11 «Wireless Network has No Clothes». http://www.cs.umd.edu/~waa/wireless.pdf

[2] N. Borisov, I. Goldberg, and D. Wagner, Intercepting Mobile Communications: The Insecurity of 802.11. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

[3] J. Walker, «Unsafe at any key size: An analysis of the WEP encapsulation», Tech Rep. 03628E, IEEE 802.11 committee, March 2000. http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip

[4] IEEE Draft P802.1X/D11, «Standard for Port based Network Access Control», Standards for Local and Metropolitan Area Networks, mars 2001.

[5] IEEE 802, Part 11 «Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications», juin 1997.

[6] Mishra, Arbaugh. «An Initial Security Analysis of the IEEE 802.1x Standard». http://www.cs.umd.edu/~waa/1x.pdf

[7] http://www.nokia.com/networks.

[8] J. Ala-Laurila, J. Mikkonen, J. Rinnemaa, «Wireless LAN Access Network Architecture for Mobile Operators», IEEE *Communications Magazine*, november 2001, pp. 82,89.

[9] Pascal Urien, «SIM-IP, Smartcard benefits for wireless applications». Application and Services in Wireless Networks ASW'2001, juillet 2001, *Hermès Sciences Publication*, ISBN 2-7462-0305-7.

[10] Pascal Urien, Hayder Saleh, Adel Tizraoui, «Carte à puce internet, état de l'art et perspectives». Actes du congrès JRES'2001, Quatrièmes Journées Réseaux 2001, pp. 353,364, Lyon 10-14 décembre 2001.

[11] http://www.1.slb.com/smartcards/infosec/isimplify.html

suite de l'éditorial de la page 1

De nombreux lecteurs se souviennent sans doute de l'arrivée des téléphones mobiles dans les foyers, il y a une dizaine d'années, ainsi que des mises en garde émises alors quant à des possibilités d'utilisation frauduleuse de cette nouvelle technologie. En général, la concrétisation du risque se traduisait par une facture téléphonique d'un montant désagréablement élevé. Quelques années plus tard, des causes similaires peuvent produire des effets de même nature avec des conséquences plus importantes, toutefois, dès lors que les cibles peuvent être les données présentes dans des laboratoires. Veillons donc à ne pas accroître la vulnérabilité de nos systèmes d'information par l'adoption d'une nouvelle technologie, prématurément ou sans disposer de garanties suffisantes.

A. Schwenck

SSHD et WINDOWS NT. Depuis l'ouverture récente de l'utilisation du protocole SSH, la plupart des machines Unix utilisent – ou vont bientôt utiliser – ce protocole en remplacement des R-Commandes. Les nombreuses fonctionnalités qu'offre SSH le justifient amplement : tunnel chiffré, authentification par machine ou par compte, compression, redirection de ports (TCP uniquement !), etc. Mais qu'en est-il dans le monde WINDOWS ?

Il existe plusieurs méthodes d'implémentations de clients SSH sous forme gratuite ou payante (sans obligatoirement avoir toutes les fonctionnalités) sous Windows :

– Porter OpenSSH (et OpenSSL) sur WINDOWS NT avec des compilateurs du marché.
– Porter OpenSSH (et OpenSSL) sur WINDOWS NT avec MinGW32.
– Utiliser une «surcouche» UWIN.
– Utiliser une «surcouche» CYGNUS (Cygwin).

L'article de Laurent Bardi expose comment implémenter ces différentes solutions.

Il n'y a malheureusement plus la place pour le publier dans ce numéro, mais vous pouvez le retrouver sur
http://www.cnrs.fr/Infosecu/Revue.html

Nous saluons l'arrivée d'un « nouveau confrère» : le magazine *MISC* (www.miscmag.com) dédié à la sécurité des systèmes informatiques, tant pour les plates-formes Mac ou Windows que pour les différents Unix. C'est une revue trimestrielle en vente dans les kiosques ou par abonnement. Les deux premiers numéros déjà sortis font, dès à présent, de cette revue une référence indispensable pour les administrateurs système. C'est aussi une source d'informations techniques d'une grande qualité pédagogique pour les néophytes éclairés qui veulent en savoir plus sur les problèmes de sécurité des systèmes.

SÉCURITÉ INFORMATIQUE
numéro 40 juin 2002
SÉCURITÉ DES SYSTÈMES D'INFORMATION

Sujets traités : tout ce qui concerne la sécurité informatique. Gratuit.
Périodicité : 5 numéros par an.
Lectorat : toutes les formations CNRS.

Responsable de la publication :
ROBERT LONGEON
Centre national de la recherche scientifique
Service du Fonctionnaire de Défense
c/o IDRIS - BP 167. 91403 Orsay Cedex
Tél. 01 69 35 84 87
Courriel : robert.longeon@cnrs-dir.fr
http://www.cnrs.fr/Infosecu

ISSN 1257-8819
Commission paritaire n° 3105 ADEP

Conseil et coordination : CNRS - DIST - Jacqueline Leclère • Conception et réalisation : La Souris 01 45 21 09 61