Authentification dans les réseaux sans fil

Sébastien Gambs

sgambs@irisa.fr

19 octobre 2015

Réseaux sans fil

WEP, WPA et WPA2

RFID et réseaux de capteurs
- Sécurité et protection de la vie privée dans les RFID
- Réseaux de capteurs

Réseaux sans fil

Réseaux sans fil

Réseau sans fil : réseau informatique où la connection entre les postes et les différents systèmes se fait par ondes radio.

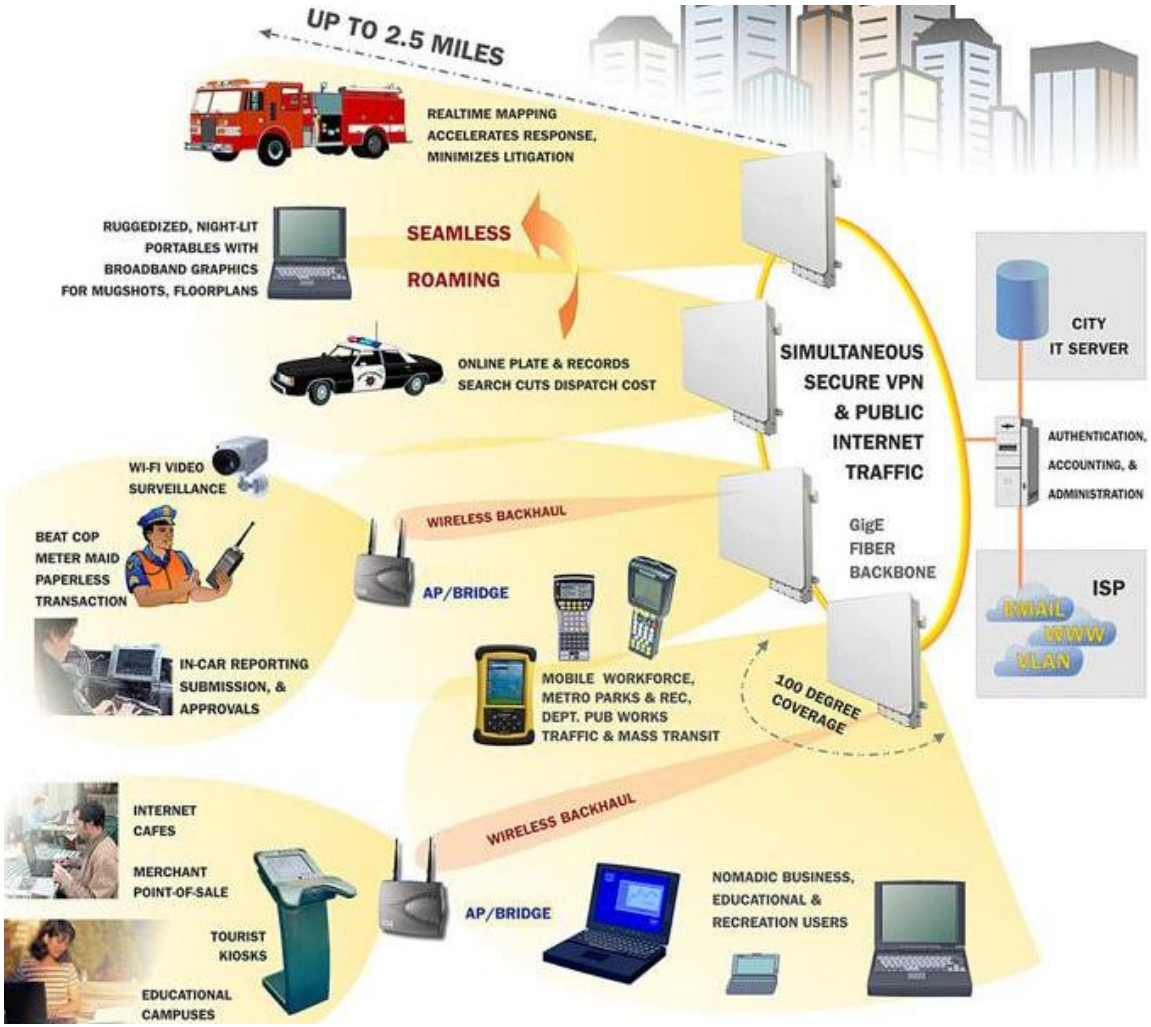
Types de réseaux sans fil :

- WiMAX pour des transmissions hertziennes haut-débit sur des distances allant jusqu'à plusieurs dizaines de kilomètres (comme les réseaux urbains),
- Wi-Fi pour des distances moyennes (par exemple un campus),
- Bluetooth pour des connections radio courte distance entre des appareils électroniques proches (imprimantes, ordinateurs, manettes de jeu vidéo, . . .).

Besoins principaux de sécurité :

- Authentification de l'utilisateur pour empêcher un accès non-autorisé aux ressources du réseau.
- Protection de la confidentialité et de l'intégrité des données transmises.

Exemples de réseaux sans fil



Dangers spécifiques aux réseaux sans fil

- Pas besoin pour un attaquant de compromettre physiquement du matériel pour intercepter les communications ...
- il peut simplement se placer à proximité et "écouter" (*attaque passive*).
- Il est facile aussi pour lui d'injecter de faux messages (*attaque active*).
- Remarque : certaines attaques qui étaient simplement théoriques dans les réseaux filaires deviennent réalisables en pratique dans les réseaux sans fil.
- Offre une porte d'accès supplémentaire pour pénétrer un réseau qui est plus difficile à contrôler que des postes fixes (ex : infection d'un poste car son antivirus n'est pas à jour).
- Difficultés supplémentaires dans les réseaux ad-hoc : pas d'accès centralisé par un point d'accès et donc risque potentiel de communication à travers un noeud malveillant

Wi-Fi

- Wi-Fi : standard IEEE 802.11 pour la communication radio dans les réseaux locaux sans-fil.
- Mis en place par la Wi-Fi alliance, un consortium à but non-lucratif regroupant plus de 260 compagnies tel que Cisco ou Motorola.
- Utilisé en pratique comme synonyme pour représenter le concept de communication dans les réseaux sans-fil entre une borne Wi-Fi offrant un accès Internet et des appareils tels que des ordinateurs, des téléphones portables ou encore des imprimantes.
- Portée du réseau : quelques pièces à plusieurs kilomètres carré.
- Exemples : aéroport, ville ou campus universitaire.

Wi-Fi : principales caractéristiques

- Permet de déployer des réseaux sans fil dans des endroits difficiles d'accès mais ...
- couverture limitée : portée typique d'un routeur Wi-Fi entre 32m à l'intérieur et 95m à l'extérieur.
- Consommation énergétique plus gourmande que pour le Bluetooth.
- Mobilité limitée d'un utilisateur à travers le réseau de part la portée maximale.
- Exception : le mode "itinérance" (*roaming* en anglais) qui permet de sauter d'un point d'accès à un autre en toute transparence.

Modes de connexion

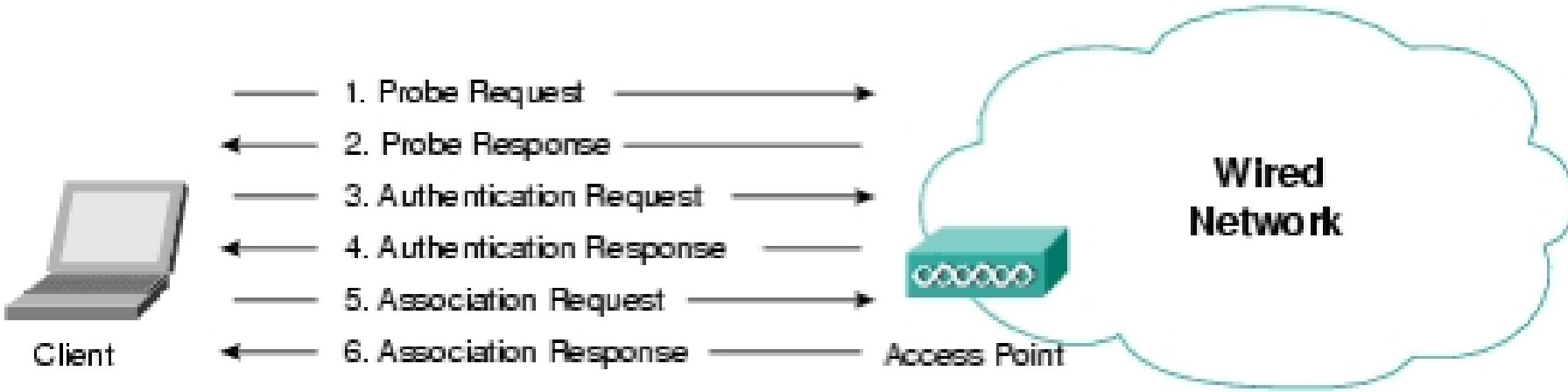
- Mode infrastructure : connexion entre un appareil équipé d'une carte Wi-Fi et un ou plusieurs points d'accès.
- Demande à ce que la zone soit couverte régulièrement par des bornes.
- Impossibilité d'étendre le réseau à moins de rajouter de nouvelles bornes.
- Exemples : accès Internet dans un aéroport ou un centre commercial.
- Mode "ad-hoc" : réseau local formé entre plusieurs machines équippés de carte Wi-Fi.
- Idéal pour l'échange de données rapide entre plusieurs machines proches physiquement.
- Exemples : réseaux intervéhiculaires ou réseaux de capteurs.

Schéma classique de connexion

1. Le client diffuse une requête pour sonder les réseaux présents dans le voisinage.
2. Les points d'accès présents dans la zone répondent.
3. Le client décide quel point d'accès utilisé et envoie une demande d'authentification.
4. Le point d'accès renvoie une réponse pour l'authentification.
5. Une fois l'authentification réussie, le client envoie une demande d'association avec le point d'accès.
6. Le point d'accès répond à cette demande d'association.
7. Le client peut maintenant utiliser le point d'accès pour accéder à Internet si toutes les étapes précédentes ont réussies.

Illustration du schéma de connexion

Figure 1 802.11 Client Authentication Process



WEP, WPA et WPA2

WEP

- WEP (*Wired Equivalent Privacy*) : créé en 1999 pour assurer la confidentialité et l'intégrité dans les réseaux sans fil de type Wi-Fi.
- Suppose que le client et le serveur possède une clé secrète partagée.
- La découverte de nombreuses faiblesses à partir de 2001 lui ont valu le surnom de *Weak Encryption Protocol*.
- Remplacé depuis 2003 par WPA (*Wi-Fi Protected Access*) et depuis 2004 par WPA2.
- Malgré cela reste encore souvent implémenté (par exemple dans certaines *boxes*).

Fonctionnement de WEP

- Confidentialité : assuré par le protocole de chiffrement à flot RC4 (utilisé aussi dans SSL).
- Contrôle d'intégrité : assuré par une somme de contrôle de type CRC-32.
- Deux longueurs de clés possibles :
  - WEP 64 : 40 bits de clés concaténé à un vecteur d'initialisation de 24 bits.
  - A été inventé au moment où les lois du gouvernement américain interdisaient d'utiliser des clés de taille trop longue.
  - WEP 128 : 104 bits de clés concaténé à un vecteur d'initialisation de 24 bits.
- Exemple de clé WEP sur 128 bits (écrit en hexadécimal) : 5d40223f3e7a4b556c25576f4c.

Résumé : chiffrement et intégrité sous WEP

Algorithme d'envoi (client) :

- Soit m le message et $CRC(m)$ le haché CRC-32 du message et $p =< m, CRC(m) >$.
- Générer un vecteur d'initialisation aléatoire v et calculer $RC4(v, k)$ pour k la clé partagée.
- Calculer $c = p \oplus RC4(v, k)$.
- Le client envoie c et v au serveur.

Algorithme de réception (serveur) :

- Générer le flux de bits aléatoire $RC4(v, k)$.
- Calculer $p = c \oplus RC4(v, k) = c \oplus RC4(v, k) \oplus RC4(v, k)$.
- Vérification de l'intégrité du message en utilisant $CRC(m)$.
- Si ce n'est pas le cas rejet du message, sinon celui-ci est accepté.

RC4 (*Rivest Cipher 4*)

- Chiffrement à flux inventé en 1987 par Ronald Rivest de RSA Security.
- Originellement l'algorithme était resté secret mais une version du code a été publiée anonymement en 1994.

Thank you Bob Anderson

- *To*: cypherpunks@toad.com
- *Subject*: Thank you Bob Anderson
- *From*: nobody@jpunix.com
- *Date*: Fri, 9 Sep 1994 22:11:49 -0500
- *Complaints-To*: postmaster@jpunix.com
- *Remailed-By*: remailer@jpunix.com
- *Sender*: owner-cypherpunks@toad.com

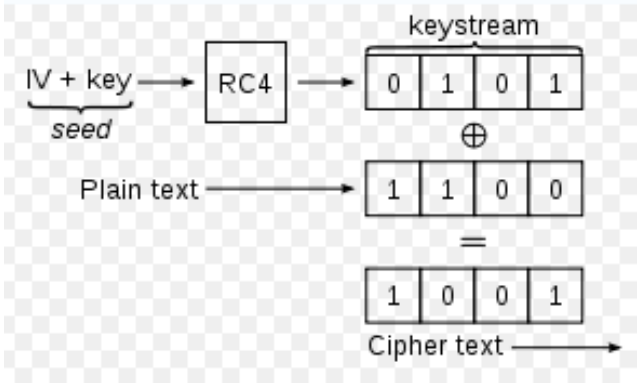
```
SUBJECT:  RC4 Source Code

I've tested this.  It is compatible with the RC4 object module
that comes in the various RSA toolkits.
```

- Combine un générateur de bits pseudo-aléatoires avec un chiffrement du type *masque jetable*.

Fonctionnement de RC4

- Chiffrement : OU-exclusif bit par bit entre le message et la chaîne de bits pseudo-aléatoires générée.



- Déchiffrement : même principe.
- Le générateur pseudo-aléatoire se base sur :
  - une permutation secrète de tous les 256 octets possibles.
  - deux pointeurs de 8 bits qui servent d'indexes dans un tableau.
- Permutation initiale dépend de la clé secrète (entre 40 et 256 bits).
- La permutation est mise à jour pour chaque nouveau bloc.

Clés faibles et biais du flux

- Problème : certaines attaques ont démontraient que RC4 était loin de se comporter comme un générateur pseudo-aléatoire parfait.
- Attaque de Roos et Wagner 95 :
  - certaines clés sont dites “faibles”,
  - la connaissance des trois premiers octets d'une clé faible permet de dériver la valeur du troisième octet si on observe le flux chiffré et qu'on connaît la valeur correspondante du texte clair.
- Biais de Jenkins 96 : il existe une corrélation importante entre certains bits du flux de clé.

Faiblesse de l'utilisation de RC4 sous WEP

- Problème : RC4 n'utilise pas un vecteur d'initialisation séparée en plus de la clé secrète (autrement dit pas de *salage*).
- Implication : le même message encrypté deux fois avec la même clé produira le même chiffré (*pas de sécurité sémantique*).
- Solution 1 : générer une nouvelle clé en faisant un hachage de la clé secrète concaténée avec le vecteur d'initialisation.
- Solution 2 : concaténer la clé secrète avec le vecteur (moins sécuritaire que 1.).
- Hypothèse : le vecteur est supposé publique.
- RC4 (sous WEP) se contente de la solution 2 en utilisant les 3 premiers octets de la clé comme vecteur d'initialisation (possibilité de l'attaque de Roos et Wagner).

Attaque FMS

- Attaque de Fluhrer, Mantin et Shamir (2001) : pour certaines clés *faibles*, les premiers bits générés ne sont vraiment pseudo-aléatoires.
- Conséquence : il est possible de faire des statistiques sur ces premiers bits pour apprendre de l'information sur la clé secrète.
- L'attaque demande l'accès à un grand nombre de messages chiffrés (relativement facile à obtenir dans un réseau sans fil).
- Attaque utilisé en pratique pour casser WEP.
- Contre-mesure possible : jeter les 768 premiers octets du flux (non implémenté sous WEP).
- Autres attaques : Korek 04, Klein 06, Pyshkin, Tews et Weinnmann 07, Vaudenay et Vuagnoux 07, Beck et Tews 09, Sepherhad, Vaudenay et Vuagnoux 10, ...

Inversion de bit

- Certains cryptosystèmes sont vulnérables à un changement de contenu du message envoyé, même s'il reste impossible pour l'attaquant de le lire en clair.
- Inversion de bit : possibilité d'inverser un bit particulier du contenu du message, même sans pouvoir le déchiffrer.
- Exemple : masque jetable.
- Peut-être détecté par l'utilisation d'un MAC.

CRC-32

- CRC-32 (*Cyclic Redundancy Check*) : fonction de hachage de 32 bits se comportant comme une code détecteur d'erreur (sert pour contrôler l'intégrité du message).
- Peut être implémenté très facilement dans le matériel.
- Permet de détecter une erreur non-malveillante ayant eut lieu sur le canal de communication mais ne protège pas contre les erreurs intentionnelles.
- En particulier, à partir d'un message et de son CRC correspondant, il est possible de fabriquer un autre message ayant le même CRC.
- Autrement dit, convient pour détecter du bruit généré par l'environnement mais pas par un attaquant actif.
- Approche plus sécuritaire : utiliser un code d'authentification de messages.

Authentification dans WEP

Méthodes principales :

- Authentification ouverte : le point d'accès accepte n'importe quelle requête d'authentification.
- Authentification avec clé partagée : chaque client possède une clé WEP statique connue par le point d'accès.

Autres méthodes possibles :

- Par adresse MAC (*Media Access Control*) pour le client et
- par SSID (*Service Set Identifier*) pour le point d'accès.

Authentification ouverte

- Le point d'accès accepte n'importe quelle requête d'authentification.
- Correspond à une forme de non-authentification.
- Idéal pour offrir un accès libre à Internet par exemple.
- N'empêche pas que les communications puissent être chiffrées par exemple VPN.
- Conséquence : sans la clé correspondante les messages chiffrés par le client ne pourront pas être déchiffrés par le point d'accès (forme de contrôle d'accès).
- Exemple : chiffrement par WEP.

Authentification par clé partagée

Chaque client a une clé WEP statique.

Protocole d'authentification :

1. Le client envoie une demande d'authentification au point d'accès avec qui il partage sa clé WEP.
2. Le point d'accès répond avec un challenge aléatoire envoyé en clair.
3. Le client utilise sa clé WEP local pour encrypter ce challenge et renvoie le message chiffré au point d'accès.
4. Le point d'accès déchiffre le message et considère le client comme valide si le texte correspond au challenge aléatoire envoyé.

Vulnérabilité de l'authentification par clé partagée

- Un attaquant peut écouter passivement les échanges entre le client et le point d'accès.
- Ceci inclut le challenge aléatoire et le même challenge encrypté avec la clé WEP du client.
- Comme la méthode de chiffrement utilisée (RC4) utilise un OU-exclusif entre le flux de clé et le message, il est facile de retrouver ce flux en faisant un OU-exclusif entre le texte clair et le message chiffré.
- Conséquence : possibilité d'attaque de l'homme au milieu.

Exemple d'attaque

- Un texte clair connu est envoyé à un client d'un réseau sans fil (par exemple par courriel).
- L'attaquant "renifle" le réseau en attendant le message chiffré correspondant généré par le client.
- À partir de ce message, il peut dériver le flux de clé correspondant et le faire croître pour chiffrer d'autres messages.

Adresse MAC

- Adresse MAC (*Media Access Control*) : identifiant physique unique d'une machine.
- Codée sur 6 octets et représentée en générale sous forme héxadécimale.
- Exemple : 5E:FF:56:A2:AF:15.
- Stockée en général au niveau de la carte réseau ou d'une interface réseau.
- Filtrage par adresse MAC possible pour donner ou refuser l'accès à un réseau pour certaines machines.
- Exemples de techniques : *liste noire* ou *liste blanche*.
- Difficulté pratique : demande un enregistrement préalable des machines.
- Usurpation d'adresse MAC est en général plus difficile à faire que l'usurpation d'adresse IP mais pas impossible.

SSID

- SSID (*Service Set IDentifier)* : nom qui identifie un réseau sans fil dans la norme Wi-Fi (codé jusquà 32 octets).
- C'est le SSID qui est diffusé par le point d'accès suite à une demande d'un client.
- En mode infrastructure il identifie un point d'accès et en mode ad-hoc une connexion.
- Plusieurs points d'accès peuvent partager le même SSID s'ils appartiennent au même réseau.
- De plus, un seul point d'accès physique peut parfois diffuser plusieurs SSID (*points d'accès virtuels*) s'il offre l'accès à plusieurs réseaux offrants des niveaux de sécurité différents.
- Exemples: IRISA-prive, IRISA-invite et INRIA.

Cacher son SSID

- Un réseau peut se protéger en refusant de donner son SSID suite à une demande de présence d'un client.
- Le réseau apparaît alors comme *non-nommé*.
- Le client est obligé de connaître à l'avance le nom du réseau et de fournir ce nom pour pouvoir y accéder.
- Protection partielle : un attaquant pourrait simplement écouter passivement les communications et apprendre le nom du réseau lorsqu'un client se connecte (le SSID est transmis en clair au début de la connexion).
- Autre méthode (active) : annoncer au client que la connexion a eut un problème et lui demander de se reconnecter (et donc de révéler le SSID du réseau).

WPA et WPA2

- WPA (*Wi-Fi Protected Access*) : protocole d'authentification développé par la Wi-Fi Alliance pour remédier aux faiblesses de WEP et servir d'intermédiaire avant WPA2.
- Conçu pour fonctionner avec le même matériel que WEP mais avec un logiciel mis à jour.
- Utilise RC4 avec une clé de 128 bits + 48 bits pour le vecteur d'initialisation.
- Implémente le protocole TKIP pour contrer certaines faiblesses rencontrées par WEP.
- WPA2 : protocole d'authentification de WPA et actuellement implémentée dans la norme Wi-Fi.
- Utilise CCMP (*Counter-Mode/CBC-Mac protocol*), un chiffrement par blocs du type AES pour assurer la confidentialité et l'intégrité des données.

TKIP

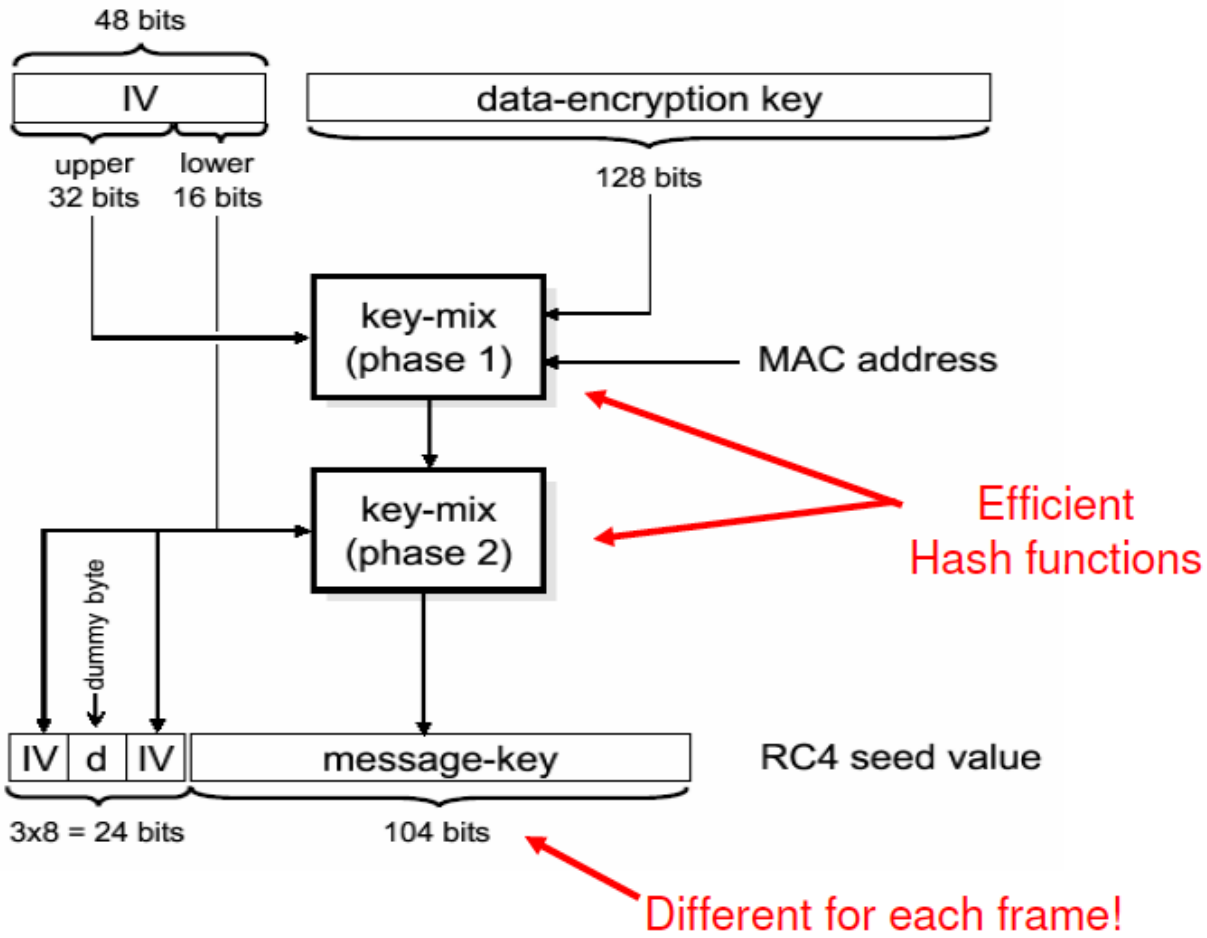
TKIP (*Temporal Key Integrity Protocol*) : protocole de sécurité qui intègre des mécanismes additionnels pour contrer les problèmes rencontrés par WEP en pratique.

- Fonction de mélange de clé : combine à la fois une clé secrète temporelle dérivée de la clé secrète racine, un vecteur d'initialisation et l'adresse MAC de transmission avant de passer le résultat obtenu à RC4.
- WEP se contentait de concaténer le vecteur d'initialisation avec la clé.
- Mécanisme de compteur pour séquence : chaque paquet envoyé contient un compteur.
- Les paquets qui ne sont pas recus dans le bon ordre sont rejetés.
- Michael : CAM utilisé pour la vérification de l'intégrité des messages (sur 64 bits).

TKIP (suite)

- Utilise RC4 comme méthode de chiffrement.
- Possède un mécanisme de mise à jour régulière de la clé de chiffrement.
- Chaque paquet envoyé est encrypté avec une clé de chiffrement qui est unique.

Illustration du mélange de clés



Chiffrement d'une trame avec TKIP

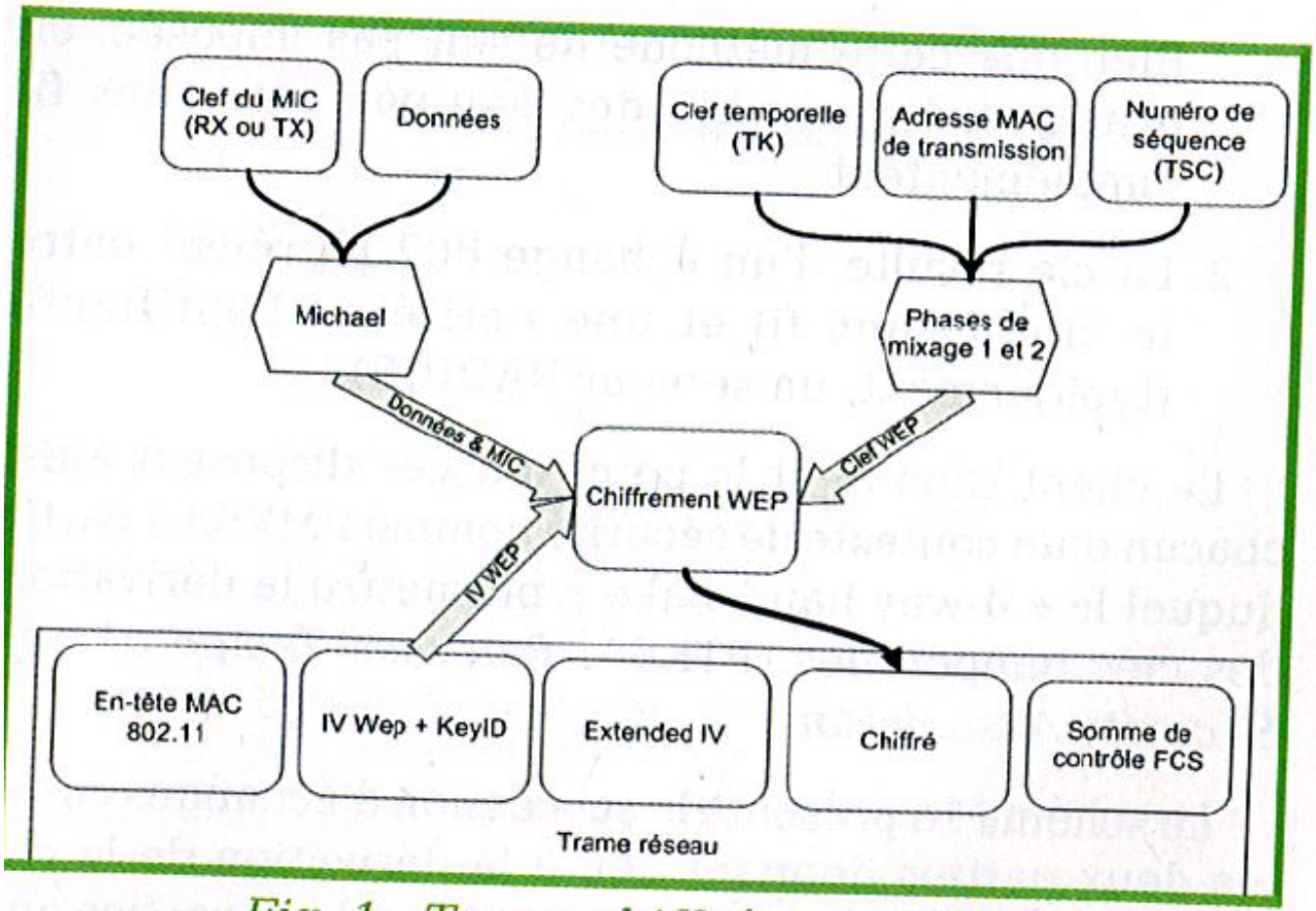


Fig. 1 : Trame chiffrée avec TKIP

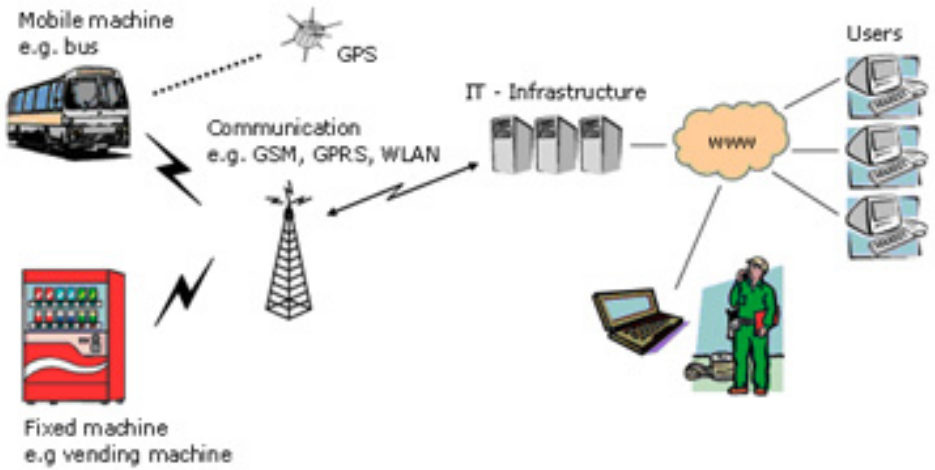
Aircrack-ng

- Aircrack-ng : ensemble d'outils de surveillance pour les réseaux sans fil qui peut aussi être utiliser pour casser les clés WEP et le mode "pre-shared key" dans WPA.
- A définitivement démontrer l'insécurité pratique de WEP.
- Permet de retrouver une clé WEP en générant activement des messages encryptés avec des vecteurs d'initialisation particuliers ce qui permet d'apprendre des bits d'information sur la clé.
- Nécessite entre 40000 et 1 million de vecteurs d'initialisation pour briser une clé WEP de 128 bits.

RFID et réseaux de capteurs

Applications MtoM

MtoM[1]: paradigme général pour l'interaction et la communication entre les machines.

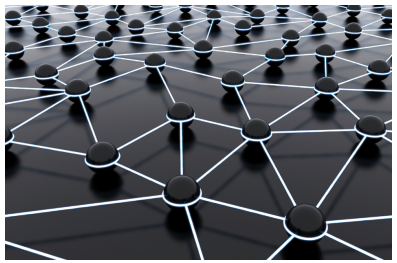


Exemples d'applications MtoM: système de transport, système de surveillance pour la santé, gestion d'une flotte de véhicules, réseau de senseurs, automatisation de la maison.

[1] Machine-to-Machine mais aussi parfois appelé Machine-to-Man, Machine-to-Mobile,...

Défis au niveau sécurité

- Machines avec des capacités de calcul et de mémoire limitées.
  $\Rightarrow$ pas nécessairement possible d'utiliser l'arsenal complet de la cryptographie
- Réseau non-structuré avec une topologie globale inconnue.
  $\Rightarrow$ Comment être sûr qu'on peut avoir confiance dans ses voisins (plus difficile encore si le réseau est dynamique et si sa topologie évolue au fur et à mesure du temps)?



- Potentiellement des millions de nodes dans le réseau.

Question fondamentale: comment assurer la confidentialité, l'authenticité, l'intégrité et la disponibilité dans ce contexte?

Défi au niveau de la protection de la vie privée

- Une machine peut appartenir à une personne en particulier et révéler beaucoup d'information personnelle la concernant.
  $\Rightarrow$ bris de vie privée
- Très intrusif si l'appareil est si petit ou si discret que la personne n'a même pas conscience de sa présence.
  Exemple: RFID dans un pull-over.

Systèmes RFID

RFID (Radio-Frequency IDentification): petite puce équippée d'une antenne.

Caractéristiques principales:

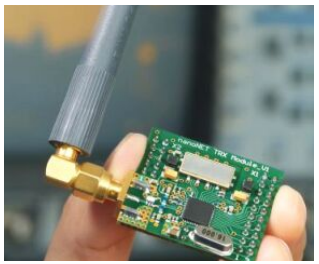
- Très petite taille.
- Capacités énergétiques, de calcul et de communcation limitées.

Exemples d'applications: carte de proximité, transpondeur pour paiement automatique au péage, jeton de paiement, tags RFID pour les animaux, appareils "intelligents" ...

Types de RFID

- Passif: pas de source d'énergie, émet seulement quand activé, portée limitée, petit et peu coûteux.

- Pas ou capacité limitée pour faire de la cryptographie (par exemple seulement des fonctions de hachages et cryptosystèmes symmétriques).
- Semi-passif: batterie intégrée, émet quand interrogé.
- Actif: batterie intégrée, peut initier la communication, longue portée, plus coûteux.



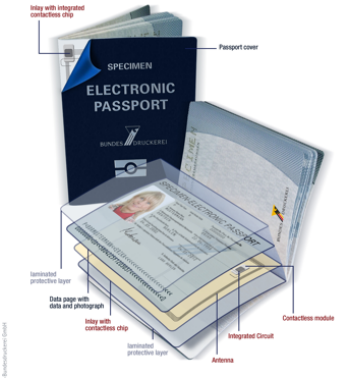
Compromis entre puissance de calcul et portée de transmission

Modèles d'adversaire pour les RFID

- Minimaliste: l'adversaire peut seulement entrer en contact un nombre fini de fois avec le RFID pour le scanner.
- Modèle de détection: l'adversaire veut cloner l'étiquette RFID sans être détecté.
- Pleinement cryptographique: modèle de sécurité habituellement considéré en cryptographie.
- L'étiquette est supposé avoir accès à toutes les primitives cryptographiques traditionnelles tel qu'un générateur de nombres (pseudo)-aléatoires.
- L'adversaire peut être passif (tel qu'un espion) ou actif (par exemple en faisant des requêtes à l'étiquette ou en générant de faux messages).
- Tous les modèles d'adversaires ne sont pas comparables et reflètent différentes situations de la vie réelle.

Traçage

- Intrusion: une étiquette RFID peut être scanné sans le consentement explicite de son utilisateur (et parfois même sans qu'il en ait conscience).



- Chaque RFID comporte en général un identifiant unique (+ potentiellement d'autre information).
- Si l'étiquette est relié à un individu particulier
  $\Rightarrow$ bris de vie privée s'il y a un système global de surveillance
- Menace plus important si possiblement combiné avec de l'information auxiliaire.

Illustration du traçage

Exemple: si une personne achète un objet équippé avec un RFID en utilisant sa carte de crédit (par exemple un pull-over)
$\Rightarrow$ possibilité de relier l'identité de la personne avec le numéro de l'étiquette
$\Rightarrow$ traçage possible à l'intérieur d'un réseau de lecteurs RFID
$\Rightarrow$ possibilité de suivre les mouvements du propriétaire

Supposons que l'objet soit transmis à une autre personne
$\Rightarrow$ il pourrait avoir été offert indiquant ainsi une relation sociale
$\Rightarrow$ possibilité de suivre les mouvements de la connaissance

Implanter une puce RFID sur un humain (1/2)

Implanter une puce RFID sur un humain (2/2)

BBC NEWS

Watch One-Minute World News

News Front Page
Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
Science & Environment
Technology
Entertainment
Also in the news
Video and Audio
Programmes
Have Your Say
In Pictures
Country Profiles
Special Reports
RELATED BBC SITES
SPORT
WEATHER
ON THIS DAY
EDITORS' BLOG

Last Updated: Wednesday, 29 September, 2004, 08:17 GMT 09:17 UK

E-mail this to a friend Printable version

Barcelona clubbers get chipped

BBC Science producer Simon Morton goes clubbing in Barcelona with a microchip implanted in his arm to pay for drinks.

Having the chip inserted was a breeze

Imagine having a glass capsule measuring 1.3mm by 1mm, about the size of a large grain of rice injected under your skin.

Implanting microchips that emit a Radio Frequency Identification (RFID) into animals has been common practice in many countries around the world, with some looking to make it a legal requirement for domestic pet owners.

The idea of having my very own microchip implanted in my body appealed. I have always been an early adopter, so why not.

Last week I headed for the bright lights of the Catalan city of Barcelona to enter the exclusive VIP Baja Beach Club.

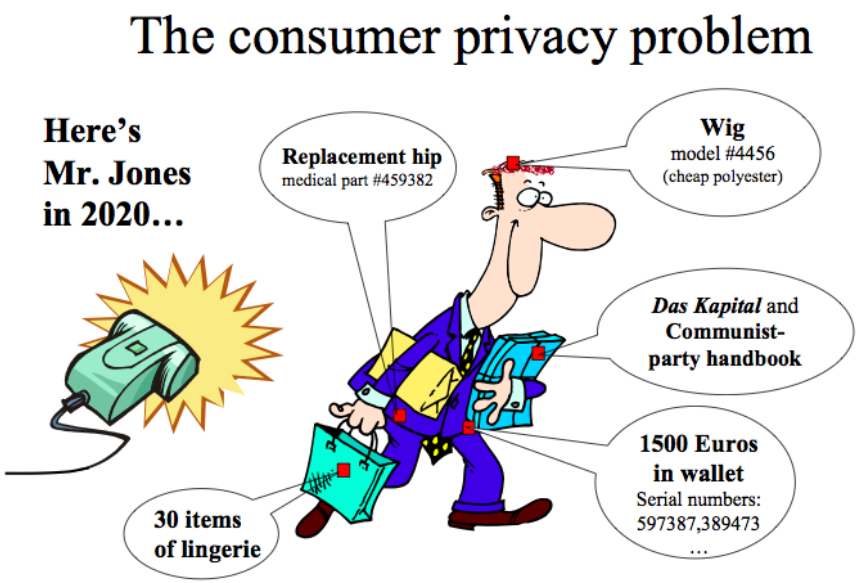
The night club offers its VIP clients the opportunity to have a syringe-injected microchip implanted in their upper arms that not only gives them special access to VIP lounges, but also acts as a debit account from which they can pay for drinks.

This sort of thing is handy for a beach club where bikinis and board shorts are the uniform and carrying a wallet or purse is really not practical.

Inventaire clandestin

Inventaire clandestin:

- Un scanning actif de l'utilisateur peut aussi révéler de l'information à propos des objets qu'il porte, et donc indirectement à son propos.
- Exemples: vêtements, accessoires, médicaments, cartes, ...



Approche par le renommage

Idée principale: changer l'identifiant du RFID au fur et à mesure du temps pour empêcher la possibilité de faire un traçage.

Techniques possibles:

- Permettre au possesseur d'une étiquette RFID de changer l'identifiant lui-même avec l'équipement adéquat.
- Rotation dans une collection de pseudonymes.
- Rafraîchir la clé (ou l'identifiant) au fur à mesure du temps.

Quelque techniques pour protéger la vie privée

- Codes de terminaison: commande protégée par un PIN qui force le RFID à commettre un suicide.
- L'étiquette est désactivée et ne répond plus aux lecteurs.
- Exemple: l'étiquette sur le pull que vous avez acheté est désactivé quand vous quittez la boutique.
- Bloqueur d'étiquette sélectif: brouille la communication entre l'étiquette et le lecteur à moins que le lecteur montre une autorisation valide.
- Prévient les lecteurs pirates de se faire passer pour des vrais lecteurs.
- Confiance basée sur la distance: utilise le ratio signal-bruit pour estimer si l'étiquette/lecteur est valide.

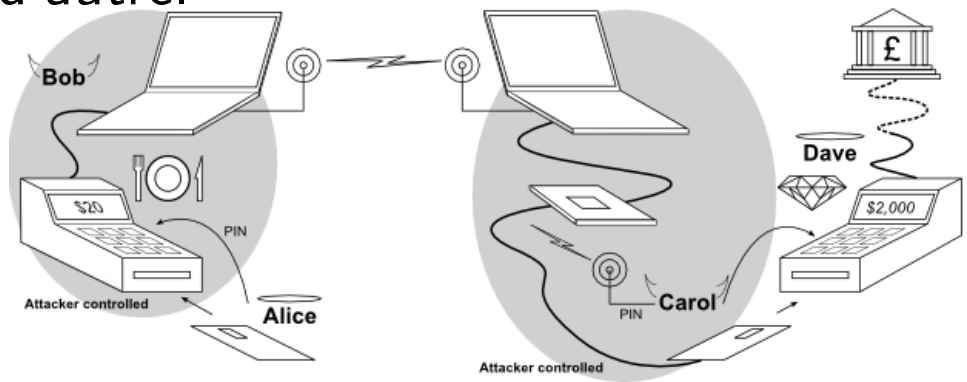
Exemple de bloqueurs d'étiquette des RSA laboratory

Comportement du signal comme information identifiante

- Mauvaises nouvelles pour la protection de la vie privée : le standard implémenté dans le RFID et même les défauts dans le comportement du signal peut être utilisé comme information identifiante.
- Bonnes nouvelles pour la sécurité : peuvent être utilisées pour l'authentification d'appareils sous la forme d'empreintes.
- Parade possible : un bloqueur d'étiquette sélectif peut agir comme un relai entre l'étiquette et le lecteur et randomiser le comportement de communication durant ce processus (par exemple en introduisant un délai avant de répondre).

Attaque par relai

- Possible si la portée du RFID est trop importante.
- Idée principale : relayer le signal entre l'étiquette et le lecteur.
- Exemple : faire payer vos achats au supermarché par quelqu'un d'autre.



- Difficile à empêcher à moins de prendre la notion de distance en compte.
- Contre-mesure possible : protocole délimiteur de distance (*distance-bounding* en anglais).

Communication sécurisée en exploitant différents portées de communication

But : communication sécurisée entre le lecteur et l'étiquette.
Difficulté : un adversaire peut espionner la communication entre le lecteur et l'étiquette (mais pas entre l'étiquette et le lecteur dû à la différence de puissance dans le signal).
Idée principale : exploiter la différence de portée de communication entre lecteur-à-étiquette et étiquette-à-lecteur.

Protocole du type masque jetable:

1. L'étiquette envoie une chaîne de bits aléatoire r au lecteur
2. Le lecteur calcule $c = m \oplus r$ et l'envoie à l'étiquette
3. L'étiquette calcule $c \oplus r = m \oplus r \oplus r$ afin de retrouver m

Authentification

- Authentification: comment assurer à un lecteur valide l'authenticité de l'étiquette scannée (autrement dit comment éviter les étiquettes contrefaites).
- Difficile à prévenir pour des RFID simples tel que les étiquettes passives.
- En principe, il est toujours possible d'interroger une étiquette, d'enregistrer la communication (tel que l'identifiant) et de le répliquer autant de fois que désiré.
- Solution partielle: signature digitale sur les données.
- Idée principale: les données sur la puce sont signées par une autorité de certification (CA).
- N'importe qui peut vérifier la signature avec la clé publique de vérification.
- Prévient la contrefaçon mais pas le clonage.

Contrôle d'accès par fonction de hachage

- L'identité d'une étiquette id_tag correspond au haché d'une clé secrète k, c'est-à-dire $id_tag = h(k)$.
- Le lecteur connaît (id_tag, k) alors que l'étiquette ne stocke que id_tag.
- Protocole de contrôle d'accès :
  1. Le lecteur envoie une demande d'identification à l'étiquette.
  2. L'étiquette envoie son identité id_tag au lecteur.
  3. Le lecteur répond en envoyant k.
  4. L'étiquette vérifie si $h(k) = id_tag$.
  5. Si c'est le cas le lecteur est authentifié, sinon le protocole avorte.
- Avantage : peut être utilisé avec des RFID implémentant simplement une fonction de hachage.
- Inconvénient : la réponse de l'étiquette est déterministe ce qui permet des attaques par rejeu.

Authentification via un protocole de type défi-réponse

Format général:

1. Le lecteur envoie un défi (par exemple une chaîne aléatoire de bits r) à l'étiquette
2. L'étiquette envoie sa réponse au lecteur
3. Le lecteur vérifie la réponse au défi et si correct, considère l'étiquette comme valide.

Un autre round de communication peut être ajouté pour s'assurer de la validité du lecteur (*authentification mutuelle*).

Première instance du protocole de type défi-réponse

- Chaque étiquette a une identité T_i et un secret k_i qu'il partage avec le système contrôlant les lecteurs valides.
- Parfois k_i peut-être considéré comme *l'identité de l'étiquette*.
- h est une fonction de hachage résistante au collision qui transforme une chaîne de bits de taille arbitraire vers une chaîne de taille finie.
- Protocole d'authentification de base:
  1. L'étiquette envoie son identité T_i au lecteur
  2. Le lecteur génère un défi aléatoire r_i et l'envoie à l'étiquette
  3. L'étiquette envoie la réponse $h(r_i \| k_i)$ au lecteur
  4. Le lecteur vérifie que $h(r_i \| k_i)$ est valide et reconnait l'étiquette comme authentique si c'est le cas
- Problème pour la protection de la vie privée: l'étiquette a diffusé son identité en clair.

Deuxième instance du protocole de type défi-réponse

- f est un cryptosystème symmétrique (par exemple AES) qui prend une clé k_i et un message m et produit $c = f(k_i, m)$ la version chiffrée du message.
- f^{-1} prend un texte chiffré c et une clé k_i et décrypte $m = f^{-1}(k_i, c)$
- Deuxième protocole d'authentification:
  1. Le lecteur génère un défi aléatoire r et l'envoie à l'étiquette
  2. L'étiquette l'encrypte avec sa clé $c = f(k_i, r)$ et l'envoie au lecteur
  3. Le lecteur essaye de déchiffrer c avec toutes les clés qu'il possède jusqu'à qu'il trouve la clé k_i tel que $r = f^{-1}(k_i, c)$
- Problème d'efficacité: terriblement lent si l'espace des clés (le nombre d'étiquettes RFID) est grand.
- Solution possible: faire une recherche du type arbre binaire sur l'identifiant en utilisant plusieurs rounds (un pour chaque bit

Authentification avec des étiquettes actives

- Les étiquettes RFID actives peuvent faire des opérations cryptographiques tel que le chiffrement symmétrique et des protocoles de type défi-réponse pour l'authentification.
- Authentification forte possible par de la communication à double sens entre l'étiquette et le lecteur.
- La cryptographie à clé publique n'est pas encore vraiment implémentée dans la plupart des étiquettes actives.

Réseaux de capteurs sans fil

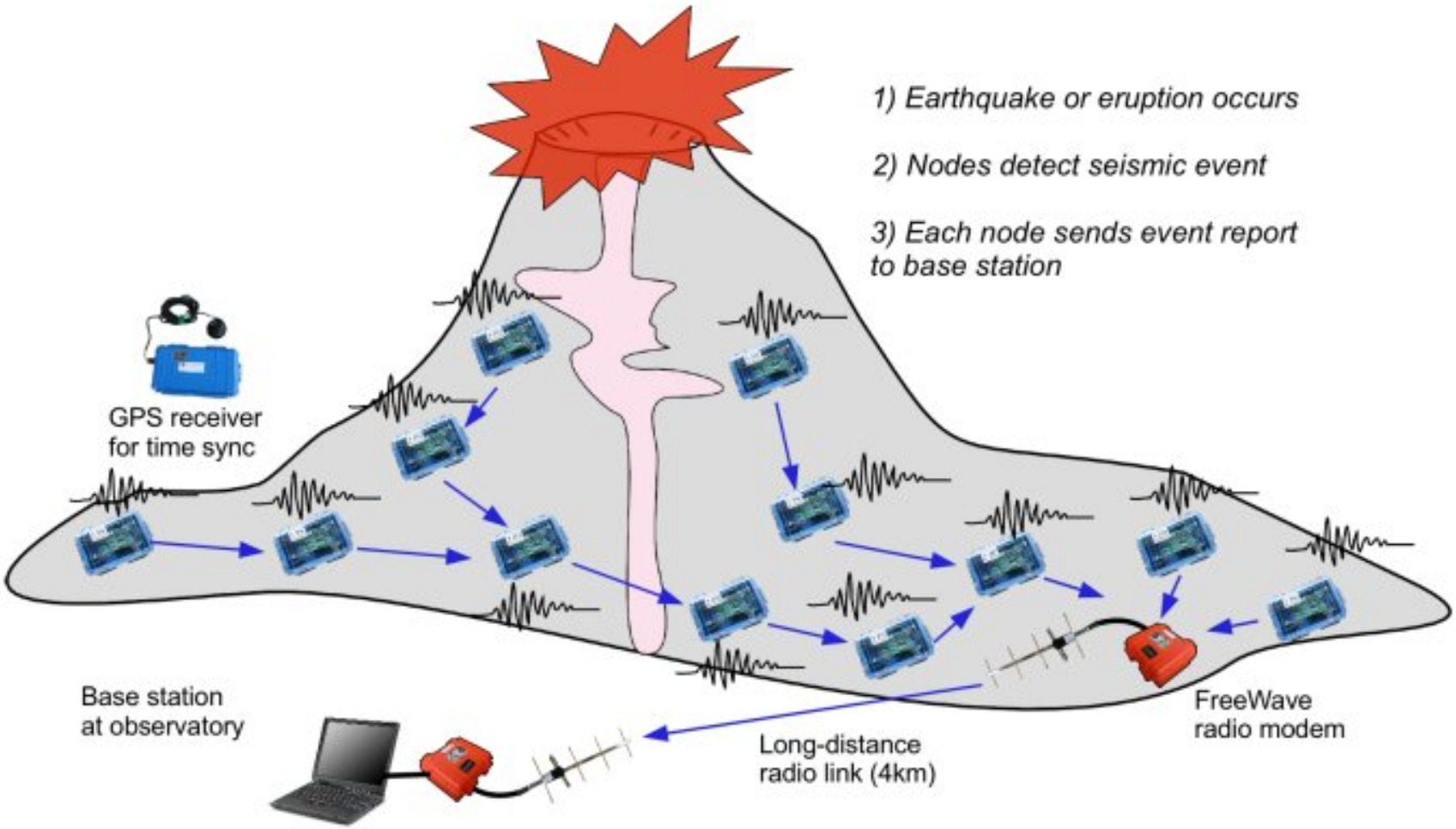
Réseaux de capteurs sans fil : réseau sans fil composé d'un grand nombre de capteurs qui peut collecter et transmettre des données à propos de l'environnement vers (un) ou plusieurs points (appelés collecteurs).

Caractéristiques principales:

- Chaque capteur peut scanner localement son environnement.
- Capacité limitée de calcul et de portée de communication.
- Possiblement une topologie dynamique du réseau.

Exemples d'utilisation: surveillance de l'environnement, système de détection d'intrusion pour la maison, surveillance des infrastructures critiques . . .

Illustration d'un réseau de capteurs



Contraintes de sécurité

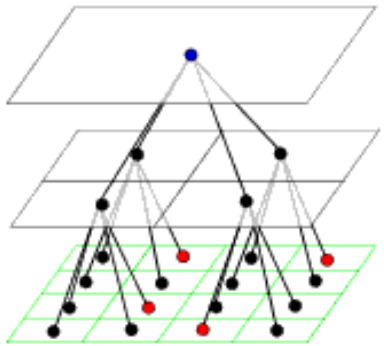
- Depend de la criticité de l'application.
- Exemple : sécuriser la surveillance d'infrastructures critiques (tel qu'une usine nucléaire ou un avion) a un niveau de criticité plus élevé que la plupart des autres applications.
- Défis principaux : assurer l'integrité et l'authenticité des données dans le réseau.
- La confidentialité est aussi important pour les applications médicales ou militaires.
- Contrainte en terme d'énergie : comment créer des protocoles sécuritaires qui minimisent la consommation d'énergie?
- Contrainte en terme de ressources calculatoire : pas de possibilité d'utiliser la cryptographie à clé publique due aux ressources limitées.

Modification volontaire de l'environnement

- Difficulté supplémentaire: un adversaire peut modifier l'environnement.
- Exemple : Mettre un briquet sous un détecteur de fumée.
- Peut être détecté par des tests de plausibilité qui vérifie la cohérence des mesures effectuées.

Aggrégation de données

- La compression ou l'aggrégation d'information réduit la consommation d'énergie.
- Exemple : réseau de n capteurs pour mesurer la température organisée sous la forme d'un arbre.



Si interessé dans une moyenne de températures, il est possible d'aggréger les n messages des noeuds intermédiaires en un seul message.

- Plus difficile si les messages sont chiffrés.

Sécuriser les données aggrégées

Première solution naive:

- Même clé de groupe pour chaque noeud.
- Utilisation d'un cryptosystème symmétrique (par exemple AES) pour sécuriser la communication entre les noeuds.
- Inconvénient : un seul noeud corrompu amène à un bris total de confidentialité.

Seconde solution :

- Une clé par lien entre noeuds.
- Inconvénients : une compromission près d'un collecteur conduit à une importante fuite d'information sur l'aggrégration + coûteux d'établir une clé avec chaque noeud voisin.

Utilisation d'un système de chiffrement homomorphique

- Chiffrement additif homomorphique : permet d'ajouter deux messages chiffrés.
- Chaque noeud dans le réseau partage une clé différente avec le collecteur.
- Quand il recoit un message chiffré d'autres noeuds, le noeud ajoute sa propre information au message en utilisant le chiffrement homomorphique en utilisant sa clé et passe le résultat au prochain noeud.
- Comme le collecteur connait toutes les clés il peut décrypter le résultat final.
- Problème : assure la confidentialité mais pas nécessairement l'intégrité.

Architecture de clés pour les réseaux de capteurs

Protocole probabiliste de Eschenauer et Gligor (2002).

Phase de pré-déploiement :

- Avant le déploiement, l'administrateur du réseau génère I nombres aléatoires indexés entre 1 et I.
- Chaque noeud est configuré avec m clés choisis au hasard parmi les I nombres générés à l'étape suivante.

Phase de communication :

- Quand deux noeuds veulent communiquer, ils échangent leurs indices de clés.
- Ils génèrent un secret à partir des clés qu'ils ont en commun (en utilisant une fonction de hachage tel que SHA1 par exemple).

Si m et I sont bien choisis, la probabilité qu'un autre noeud connaisse toutes les clés qu'ils ont en commun est faible.

Corruption ou introduction de noeuds

- Les capteurs sont généralement peu coûteux et sans protection matérielle particulière.
- Peuvent être facilement corrompus par un adversaire dans un environnement non-protégé.
- Des faux noeuds peuvent être introduits dans le réseau pour le perturber.
- Désavantage : un adversaire qui peut corrompre les noeuds petit à petit a accès à de plus en plus de clés.
- Besoin de rafraîchir régulièrement les clés.

C'est la fin !

Merci pour votre attention.
Questions?