www.cesar-conference.fr

Sécurité des Applications Sans-Fil / Wireless Security

Sécurité des Applications Sans-Fil / Wireless Security

C&ESAR 2009

Computer & Electronics Security Applications Rendez-vous

24 > 26 Novembre 2009

Rennes - France

INRIA

orange Business Services

DGSIC

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE LA DÉFENSE

DGA

C&ESAR 2009

Computer & **E**lectronics
Security **A**pplications
Rendez-vous

24-25-26 novembre 2009
Rennes - France

http://www.cesar-conference.fr/

C&ESAR 2009 : Sécurité sans fil. . . ou sans filet ?

C'est avec un réel plaisir que nous vous présentons le programme de la seizième édition de la conférence C&ESAR (Computer & Electronics Security Applications Rendez-vous) organisée par le Centre d'Électronique de l'Armement (Ministère de la Défense) sur la Sécurité des Systèmes d'Information. L'édition 2009 est consacrée au vaste sujet de la sécurité des applications sans fil.

Nous nous sommes concentrés cette année sur l'impact que peuvent avoir les technologies de communication sans fil sur la sécurité des systèmes d'information, que ce soit en champ lointain (Wi-Fi, WiMAX, UMTS, Bluetooth,. . .), ou en champ proche (RFID, cartes sans contact). La frontière entre les deux tend en fait à s'estomper, avec la montée en puissance des RFID qui de simples étiquettes pourraient devenir les éléments d'un internet des objets, et le remplacement progressif des câbles informatiques par des micro-réseaux sans fil à courte portée. . . Quelles seront les implications de cette évolution ? La traditionnelle opposition entre la fonctionnalité et la sécurité va bien sûr trouver là matière à débat, en abondance, l'absence de confinement due au media utilisé ouvrant là des portes supplémentaires à l'attaquant éventuel.

L'appel à contribution a permis de sélectionner un premier lot de sujets, qui a ensuite été complété par un certain nombre de communications invitées, en fonction du périmètre envisagé par le comité de programme pour le thème de cette année. Nous souhaitons dès à présent remercier pour leur travail remarquable les membres du comité de programme ainsi que les experts sollicités, qui ont tous répondu présent à l'appel. C'est grâce à eux tous que le programme est si riche et complet.

Ce programme est organisé en demi-journées articulées chacune autour d'une thématique introduite par une keynote :

- Session 1 : « Réseaux sans fil (Wi-Fi, UMTS,. . .) », avec Laurent Butti (Orange Labs) ;
- Session 2 : « Réseaux auto-organisants (ad hoc,. . .), vie privée », avec Ana Cavalli (Management Telecom Sud Paris) ;
- Session 3 : « Réseaux de proximité (RFID, NFC,. . .), authentification », avec Gildas Avoine (Université de Louvain) ;
- Session 4 : « Réseaux de terrain (capteurs, robots, mobiles. . .) », avec Konrad Wrona (OTAN NC3A) ;
- Session 5 : « Écoute, vie privée, droit », avec Martin Vuagnoux (EPFL).

Il faut noter que la thématique « préservation de la vie privée » (*privacy*) apparaît dans plusieurs sessions, ce qui ne fait que traduire son caractère transversal : On retrouvera cette notion dans l'exposé de Gildas Avoine (UCL) avec une approche cryptologique, mais aussi dans la contribution de Marie Barel (Orange Consulting) sur les données personnelles, ainsi que dans la présentation de Daniel Le Métayer (INRIA) sur les interactions entre droit et informatique.

Le comité de programme a souhaité voir présentées les notions de preuves informatiques et de méthodes formelles : On les retrouvera dans l'exposé d'Ana Cavalli sur la vérification des protocoles, et à nouveau dans l'intervention de Daniel Le Métayer, ainsi que dans la contribution d'Éric Vétillard et Guillaume Dufay (Trusted Labs) sur la certification.

Enfin une attention particulière a été apportée à l'emploi opérationnel des technologies sans fil (réseaux ad hoc, réseaux de capteurs, etc. . . usage et interception), car si c'est là que leur apport est le plus intéressant, c'est aussi là que leurs vulnérabilités peuvent se révéler véritablement critiques.

Nous pensons que le programme ainsi construit brosse un bon panorama des divers aspects de la sécurité des applications sans fil (problèmes, et solutions, enfin jusqu'à un certain point sans cesse mouvant. . .), voire un peu au-delà. Nous espérons que les participants à cette conférence y trouveront un éclairage pertinent sur ce domaine en pleine évolution, et des réponses aux questions qu'ils peuvent se poser.

Nous souhaitons remercier à nouveau les contributeurs, que ce soit au travers des soumissions d'articles, des communications invitées ou des discours programmes (*keynotes*), les membres du comité de programme pour leurs évaluations et leur apport à la construction du programme définitif, ainsi que les membres du comité d'organisation qui font que cette conférence peut se dérouler dans les meilleures conditions. Et n'oublions par les divers sponsors (DGA, DGSIC, Orange) qui rendent possible ce rendez-vous annuel de la communauté SSI. . .

Bonne conférence C&ESAR 2009 à tous,
et au plaisir de vous rencontrer !

Yves Correc (DGA/CELAR), *Président du comité d'organisation.*
David Simplot-Ryl (INRIA Lille – Nord Europe), *Président du comité de programme.*

Comité d'Organisation

Pascal Chour	Services du Premier Ministre, SGDN/DCSSI
Yves Correc (Président)	Ministère de la Défense, DGA/CELAR
Olivier Heen (Directeur de la publication)	INRIA Bretagne Atlantique
Ludovic Mé	Supélec
Éric Wiatrowski	Orange Business Services

Comité de Programme

Daniel Augot	INRIA Saclay
Cédric Blancher	EADS
Abdelmadjid Boubdallah	UTC Compiègne
Claude Castellucia	INRIA Rhône Alpes
Yves Correc	DGA/CELAR
Frédéric Cuppens	Telecom Bretagne
Yves Deswarte	LAAS - CNRS
Caroline Fontaine	CNRS
Hervé Guyennet	LIFC
Olivier Heen	INRIA Bretagne Atlantique
Jean Leneutre	Telecom ParisTech
Pascale Minet	INRIA Rocquencourt
Nicolas Prigent	Thomson Research
Patrick Radja	EADS
Pierre Michel Ricordel	SGDN/DCSSI
Ahmed Serhrouchni	Telecom ParisTech
David Simplot-Ryl (président)	INRIA - LIFL
Franck Veysset	Orange Labs

Site officiel : `http://www.cesar-conference.fr/`

Partenaires

- DCSSI
- DGA
- DGSIC
- INRIA
- Orange Business Services
- Supélec

Table des matières

III

Première partie

État de l'art de la sécurité des réseaux radioélectriques 802.11

Laurent Butti

Orange Labs – Laboratoire Security and Trusted Transactions
38-40 Rue du Général Leclerc, 92794 Issy-les-Moulineaux Cedex 9 – France
firstname.lastname@orange-ftgroup.com

Cet exposé propose de décrire un état de l'art sur la sécurité des réseaux radioélectriques 802.11. Le sujet a largement été débattu dans de très nombreux articles ou conférences mais (à notre connaissance) aucun article ne semble présenter un historique complet des différentes vulnérabilités publiques.

Le principal objectif de cet exposé est d'offrir un contenu didactique sur les problématiques de sécurité des réseaux radioélectriques 802.11 afin que le lecteur puisse s'y référer. Le contenu de cet article est ambitieux tant les problématiques de sécurité ont été omniprésentes depuis l'apparition de cette technologie. Par conséquent, nous n'avons pas pour ambition de détailler complètement toutes les failles de sécurité, mais plutôt d'y faire référence en donnant la possibilité au lecteur d'approfondir ses connaissances à l'aide de références bibliographiques pertinentes.

À travers un historique, nous détaillerons les principales vulnérabilités auxquelles les réseaux radioélectriques 802.11 ont fait face au fil du temps. Nous verrons aussi comment les mesures correctives et préventives se sont mises en place (ou pas) selon les types d'architectures qui se sont déployées en milieu résidentiel, milieu entreprise ou milieu hotspot.

Le but final de l'article et de la présentation associée sera de décrire l'état actuel des risques associés aux réseaux radioélectriques 802.11 et de définir des recommandations d'utilisation et de déploiement.

Biographie

Laurent est expert senior en sécurité des réseaux à France Télécom Division R&D. Ses thèmes de recherche sont axées sur la sécurité des réseaux sans-fil (802.11, 802.16...) ainsi que les problématiques de lutte contre les codes malveillants (virus/vers/bots...). Il intervient régulièrement dans des conférences internationales en sécurité telles que le FIRST, BlackHat, ToorCon, ShmooCon...

Références

Laurent Butti, Julien Tinnés : Discovering and exploiting 802.11 wireless driver vulnerabilities. Journal in Computer Virology 4(1) : 25-37 (2008)

Laurent Butti, Julien Tinnés. Recherche de vulnérabilités dans les drivers 802.11 par techniques de fuzzing. Actes SSTIC 2007. http://actes.sstic.org/SSTIC07/WiFi_Fuzzing/SSTIC07-Butti_Tinnes-WiFi_Fuzzing.pdf

Étude de l'interception et du positionnement de trafic Wi-Fi dans un environnement hétérogène

Matteo Cypriani, Adrien Henriet, Philippe Canalda, François Spies

Laboratoire d'Informatique de l'Université de Franche-Comté
prénom.nom@univ-fcomte.fr
http://lifc.univ-fcomte.fr/

Résumé Dans le cadre d'une politique de sécurité dans les réseaux sans fils, il est intéressant de pouvoir identifier la position géographique d'une source de données, pour s'assurer de sa légitimé et de son utilisation du réseau. Dans cette optique, nous proposons ici un aperçu des possibilités de capture de trafic mises en relation avec un système de géolocalisation centralisé. Notre axe d'étude porte en particulier sur le matériel courant, librement accessible au plus grand nombre et à un faible cout.

1 Introduction

L'utilisation des communications sans fil a ouvert de nouveaux axes de recherche dans le domaine des réseaux informatiques. Le positionnement des terminaux sans fil en communication entre dans cette catégorie. Cette fonctionnalité ouvre plusieurs perspectives telles que l'informatique ubiquitaire, l'amélioration de la supervision du réseau et un meilleur suivi des utilisateurs. De plus, les réseaux sans fil remettent en cause des postulats bien établis, comme la sécurisation d'un réseau, l'identification des équipements ou l'efficacité du contrôle de congestion.

L'interception d'un trafic filaire devient de plus en plus difficile à réaliser grâce à la généralisation de la commutation des réseaux ; à l'inverse l'interception d'un trafic sans fil devient de plus en plus facile à réaliser même si les procédures à suivre se complexifient. En effet, quelques cartes Wi-Fi actuelles proposent des fonctionnalités étendues qui ne s'inscrivent plus dans la norme IEEE. La qualité de cette interception est variable en fonction des modèles. Ainsi, pour compléter une interception de trafic Wi-Fi, il est souhaitable de pouvoir lui associer une position géographique, pour une bonne gestion de l'infrastructure. L'objectif de cet article est de décrire un type d'application d'interception pouvant combiner le suivi des terminaux dans la couverture d'un réseau sans fil.

L'article est structuré en cinq sections principales. La section suivante décrit la solution utilisée pour effectuer les acquisitions de l'interception et du positionnement. La section 3 concerne l'état de l'art du domaine du positionnement en espace fermé s'appuyant sur la technologie Wi-Fi. Les sections 4 et 5 décrivent l'outil de positionnement OWLPS développé au laboratoire et une expérimentation menée grâce à lui. La dernière section retrace, en quelques périodes, l'historique de l'acquisition des données sur les couches physique et liaison des réseaux sans fil.

2 Analyse de données

2.1 Les données

Pour obtenir un positionnement, il est nécessaire d'avoir un ensemble de données exploitables. Que ce soit les puissances de réception, pour un positionnement de type OWLPS [1], ou le temps précis, comme utilisé par les systèmes GNSS, ces donnés doivent être accessibles. Or, les média de communication sans fil actuels (Wi-Fi, Bluetooth) sont centrés sur les données, et même si le matériel traite ces informations, ces dernières ne sont pas systématiquement remontées au système hôte. L'ensemble des normes de communication sans fil permettent d'assurer un service fiable dans la majorité des situations. Pour les constructeurs, et donc la mise en œuvre de la partie matérielle et logicielle, il existe de nombreuses libertés de réalisation. Certes, pour une communication simple, seules les données sont intéressantes, et les normes sont donc axées sur ces dernières, mais les puces pour les communications sans fil ont accès à de nombreuses informations qui pourraient être utiles pour des services annexes, voire pour améliorer l'existant. C'est pourquoi nous nous intéressons aux données complémentaires qui sont traitées par les puces, pour leur bon fonctionnement, mais qui ne font pas partie de la norme. On peut citer la puissance du signal, le bruit, les erreurs, les antennes utilisées, le temps de transmissions, la vitesse, la norme utilisée et les erreurs de communications.

2.2 802.11, les données de la couche MAC

La norme 802.11b/g est très complète, et propose une couche d'abstraction importante, avec de nombreuses options, souvent centrées sur les données. La couche MAC nous permet d'avoir des informations sur les participants aux communications, et sur les types de *trames* utilisées. Lors d'une capture sur le réseau, il est très simple d'extraire l'ensemble de ces données de manière rapide et fiable, dans le but d'une exploitation ultérieure.

2.3 *radiotap*, les données pilotes

Avec *radiotap* [2], devenu un standard de fait, il est possible d'accéder à beaucoup d'autres informations. Moyennant une configuration spécifique, il devient ainsi possible d'avoir un nouveau périphérique virtuel qui ajoute des informations à chaque paquet de données, sous la forme d'un en-tête *radiotap*. Ainsi, avec une simple capture et une analyse de ces nouveaux champs, il est possible d'extraire des informations intéressantes.

Actuellement, ce sont ces en-têtes *radiotap* qui sont le plus couramment utilisés et supportés. Il est assez intéressant de noter que la diversité des normes n'a pas facilité un support important de la part des divers constructeurs de matériel. C'est grâce à la restructuration actuelle, qui permet de se focaliser sur une seule extension souple et adaptable, *radiotap*, que l'on a accès de plus en plus facilement à ces données. Malgré tout, les informations retournées dépendent grandement de la puce étudiée.

Les données ainsi exploitables nous permettent de connaître l'antenne de réception, le bruit, l'atténuation du signal, le canal, le type de donnée, la qualité de réception, la vitesse de transmission et le temps.

La figure 1 présente un exemple de champs disponibles, exploitables avec *Wireshark* [3].

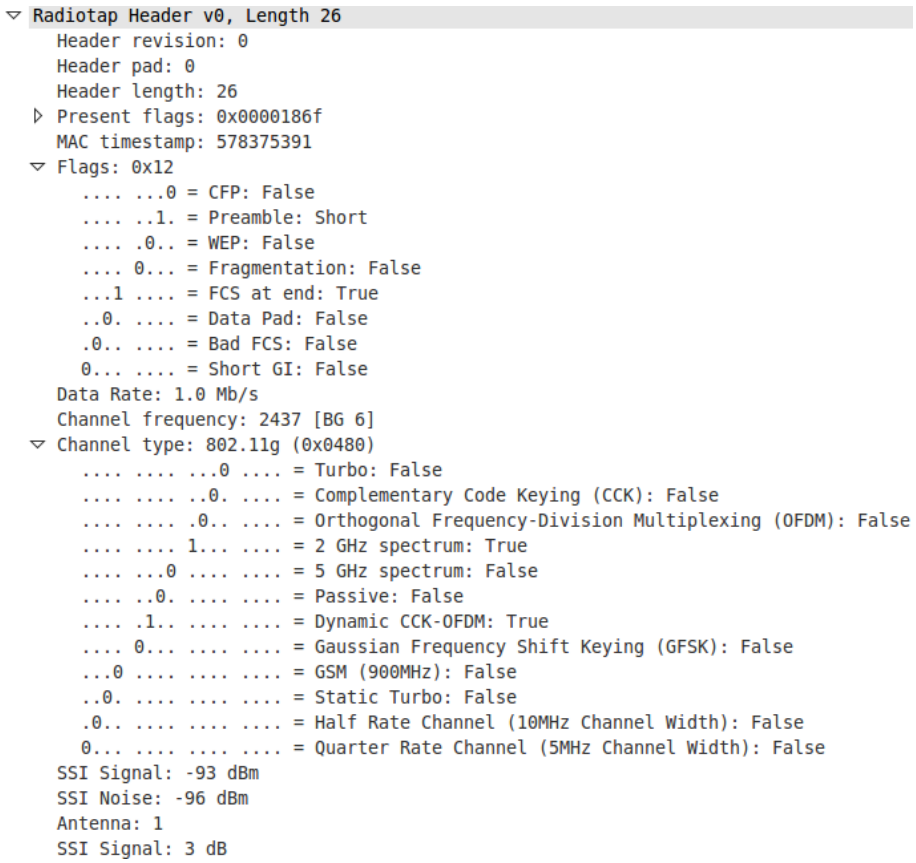


FIGURE 1: Capture d'écran du logiciel *Wireshark* [3] montrant l'en-tête *radiotap* d'un paquet intercepté.

2.4 Les pilotes, données supplémentaires

Au vu des possibilités diverses et hétéroclites offertes par les pilotes, un utilitaire permettant d'accéder aux paramètres des cartes Wi-Fi a vu jour sous Linux : *iwpriv* [4]. Cette commande permet d'interroger le pilote de la carte pour obtenir ses spécificités, aussi bien que de configurer de manière fine et spécifique ses paramètres. Avec les pilotes ouverts,

comme MadWiFi [5], nous avons encore accès à des paramètres de configuration supplémentaires.

Ainsi, il est possible d'accéder aux *trames* erronées et de demander au pilote logiciel de remonter ces dernières comme des *trames* valides. Il faudra ensuite, lors du traitement, différencier ces dernières grâce à une vérification du FCS [1]. L'intérêt de l'opération est d'obtenir plus d'information. En effet, même erroné, la majorité du paquet reste souvent correcte et les informations de l'en-tête *radiotap* sont alors exploitables (puissance du signal, canal, etc.), ce qui permet d'améliorer la précision de la localisation, même en cas de fortes interférences. En utilisant la notion de distance et d'historique, déterminer correctement l'adresse MAC, et donc le client émetteur, est donc très probable.

Les pilotes Wi-Fi sous Linux sont actuellement en pleine mutation, et entre ceux requérant un microcode propriétaire (bcm43xxx dans les bornes WRT54GL, ipw2100, ipw2200, ipw3945 centrino, prism54, rt61/73 et ZyDas), ceux n'ayant pas l'ensemble des fonctions intégrées (prism54 et Zydas sans WPA, ath5k sans mode Master, b43 très basique), le choix de la puce est primordial. L'utilisation de plusieurs types de cartes peut être intéressante pour les expérimentations, les tests de performances ou le monitoring, mais devient problématique pour le positionnement, cela étant du aux caractéristiques spécifiques et propres à chaque carte (puissance du signal, qualité du filtrage du bruit, puissance d'émission variable...).

3 État de l'art des systèmes de positionnement

Depuis près d'une dizaine d'années, les communautés scientifiques et industrielles portent un intérêt croissant à des travaux qui concernent le positionnement en utilisant le Wi-Fi. Bien sur, l'intérêt de se positionner n'est pas nouveau. Sans remonter aux premiers temps de la navigation et des découvertes de nouveaux territoires, le système de positionnement le plus conventionnel aujourd'hui est celui par satellites dénommé GNSS (GPS, Galiléo, GLONASS...). Dans un tel système, et cela reste vrai pour tous les autres systèmes faisant appel à un réseau sans fil, la précision est influencée par le type d'environnement (urbain, rural...), la densité de celui-ci (immeubles, largeur des rues), la précision de l'horloge du récepteur (besoin d'une horloge atomique pour une précision optimale), les corrections sur les erreurs (ionosphérique, troposphérique...), etc. Différents systèmes d'augmentation ont été créés pour réduire l'impact de ces facteurs sur la position. Seulement, lorsque le service de positionnement doit être rendu dans un milieu intérieur, il est rendu plus ardu (réflexion, réfraction, diffraction). Mais s'il existe des solutions nécessitant une intervention lourde sur l'infrastructure (réseaux de capteurs, détections infra-rouge et sonores...), nous assistons à la pénétration de solutions basées sur les signaux Wi-Fi. Il est désormais possible, et nécessaire, de combiner deux (voire trois) systèmes de positionnement pour garantir l'intégrité et la continuité des données et des services.

1. Le *Frame Check Sequence* permet de vérifier et corriger une trame.

Les réalisations basées sur les signaux Wi-Fi ont pour but d'améliorer la précision du positionnement en intérieur, mais pas ou plus seulement, et ensuite de proposer des services contextualisés enrichis. Ces travaux peuvent être classés en trois catégories. La première concerne les travaux basés sur la cartographie des puissances de signal tels que les systèmes RADAR [6], HORUS [7] et Ekahau [8]. Dans ces systèmes la précision est liée à la finesse du maillage de la cartographie. La deuxième catégorie est celle des systèmes fondés sur la multilatération utilisant la puissance du signal, et dont le positionnement repose sur le calcul des distances vers des points d'accès connus, tels que SNAP-WPS [9] et les travaux de Interlink Networks [10]. Dans ces systèmes la précision dépend des modèles de propagation utilisés. Pour affiner le choix de la position, on peut également tenir compte du parcours antérieur du mobile, éventuellement en tenant compte de la topologie du bâtiment pour estimer la distance entre deux points. La troisième catégorie est celle de l'hybridation qui emploie les deux, la cartographie du signal et le calcul de la position. L'inconvénient majeur du calcul de la position concerne le fait de devoir se baser sur des modèles approximatifs de la propagation des ondes. Plus la topologie est hétérogène, plus le résultat du calcul de la distance est éloigné de la réalité.

Les systèmes appartenant à ces trois catégories nécessitent la mesure du signal, soit sur le client mobile, soit sur les points d'accès. On oppose ainsi le système de géolocalisation supporté par une infrastructure à celui où le mobile, autonome, déduit sa position de ses observations de l'environnement, par exemple les systèmes mécaniques à gyroscopes et accéléromètres.

Dans tout système de géolocalisation supporté par une infrastructure à communication bidirectionnelle, il existe deux solutions de positionnement. La première est que le calcul de la position soit effectué par le mobile. Dans ce cas de figure, les éléments de l'infrastructure émettent des informations, que le mobile écoute et dont il se sert pour déduire sa position. Ces informations peuvent tout simplement être les balises Wi-Fi (*beacons*) émises par de simples points d'accès (AP), auquel cas il est très simple d'ajouter des AP pour affiner le calcul de la position (en prenant toutefois garde à éviter le brouillage mutuel des AP) ; la contrepartie est qu'il est nécessaire que le mobile dispose d'un logiciel dédié et d'une liste à jour des AP environnants avec leurs positions.

La seconde possibilité est que le mobile questionne l'infrastructure quant à sa position, et que ce soient les éléments de cette infrastructure qui effectuent le calcul de la position avant de la transmettre en réponse au mobile. Les avantages de cette solution sont multiples. Tout d'abord, le mobile n'a besoin que d'un petit programme lui permettant de contacter l'infrastructure pour lui demander le calcul de sa position. Mais le principal intérêt réside dans la souplesse dont dispose l'infrastructure pour effectuer le calcul. Puisque les « AP » écoutant les demandes de localisation n'ont pas à émettre eux-mêmes, ils peuvent être entièrement passifs et ainsi éviter toute surcharge du réseau [2] ; on peut donc les multiplier

2. Il ne s'agit donc pas, dans ce cas, de points d'accès au sens strict du terme, puisqu'étant passifs ils ne fournissent pas d'accès au réseau aux mobiles.

autant qu'on le souhaite sans influer sur la qualité de service du réseau sans fil. Les éléments de l'infrastructure peuvent également communiquer facilement, se coordonner, et on peut imaginer que grâce à ce support le système s'adapte aux évolutions de l'environnement. Cette seconde solution offre également la possibilité de traiter toute émission de la part d'un mobile comme une demande de localisation, afin de trouver la position des mobiles qui n'envoient pas de demande de localisation.

Technique [a]	**Carto** [b]	**Atnt** [c]	**Histo** [d]	**Topo** [e]	**Centré** [f]	**Déploiement** [g]
RADAR [6]	x				I	moyen / long [h]
RADAR + VL [11]	x		x		I	moyen / long [h]
Interlink Networks [10]		x			I	court [i]
FBCM [12]		x			M ou I	court [i]
FRBHM Basique [13]	x	x			M ou I	moyen [j]
FRBHM Discret [14]	x	x	x	x	M ou I	moyen [k]
FRBHM Continu [14]	x	x	x	x	M ou I	moyen [k]

a. Nom de publication de la technique ou de l'algorithme de géolocalisation.

b. Indique si la technique utilise ou pas une cartographie des puissances de signal.

c. Indique si la technique utilise ou pas un modèle d'atténuation du signal.

d. Indique si l'historique de parcours du mobile est pris en compte pour le calcul des positions suivantes.

e. Indique si la topologie de la zone de mesure est prise en compte pour calculer la distance entre deux points.

f. Indique si le système expérimental, tel que décrit par les auteurs de la technique, effectue les mesures et les calculs sur le mobile (« M ») ou sur l'infrastructure (« I »).

g. Indique si le déploiement du système est aisé et rapide, ou au contraire long et fastidieux.

h. Le temps de déploiement d'un système fondé uniquement sur la cartographie des puissances dépend du maillage de cette cartographie, dont dépendra la précision obtenue ; à cela s'ajoute, comme pour les autres systèmes, le déploiement des AP.

i. Le déploiement consiste seulement à placer les AP et à déterminer leurs coordonnées.

j. Le déploiement consiste en une cartographie des puissances minimaliste (comme pour RADAR dans le cas d'un maillage large) et au placement des AP avec enregistrement de leurs coordonnées (comme pour Interlink Networks et FBCM).

k. La description de la topologie du bâtiment allonge un peu le temps de déploiement par rapport au FRBHM Basique.

TABLE 1: Comparatif de techniques de géopositionnement basées sur le réseau Wi-Fi.

Le tableau 1 dresse un comparatif de plusieurs techniques de géopositionnement, fondées sur le réseau Wi-Fi, actuellement publiées dans les travaux de la communauté. Les colonnes *Cartographie* et *Atténuation* décrivent le cœur du fonctionnement du système expérimental, à savoir la façon dont est employée la puissance du signal : pour réaliser une cartographie, pour évaluer la distance en vue d'une multilatération, ou les deux. Les

deux colonnes suivantes, *Historique* et *Topologie*, précisent l'utilisation d'éventuelles données complémentaires permettant d'affiner la position calculée et l'estimation des distances. Enfin, les deux dernières colonnes, *Centré* et *Déploiement*, donnent des informations plus générales sur le système.

La précision du système RADAR [6], qui utilise une cartographie des puissances seule, est dépendante de la finesse du maillage de la cartographie des puissances réalisée lors du déploiement. Selon la précision souhaitée, il est donc possible de consacrer plus ou moins de temps au déploiement : un maillage d'un mètre est très long à réaliser, tandis qu'un maillage de quatre ou cinq mètres (qui correspond à environ un point par pièce dans un environnement de bureaux) est nettement moins fastidieux. Ce système RADAR apporte une première adaptation, selon la précision recherchée, le temps et les moyens dont on dispose, d'une technique dont le temps de déploiement est variable en offrant une précision plus ou moins bonne. La combinaison d'un tel système avec d'autres techniques (ne nécessitant pas de calibration) et d'autres algorithmes (tirant bénéfice d'un contexte : prédiction, topologie) constituerait une contribution remarquable. Le système RADAR a été étendu par des méthodes probabilistes permettant d'accroitre sa précision : Ekahau [8] considère la distribution de la puissance du signal selon une courbe gaussienne ; HORUS [15] utilise une représentation par histogrammes. Ces méthodes permettent d'obtenir une meilleure précision que l'usage de la moyenne des mesures de calibration de la cartographie.

D'autres techniques de géopositionnement fondées sur des réseaux sans fil (GSM, Wi-Fi) existent ; la façon de déterminer la position est généralement fondée sur un calcul de la distance par atténuation du signal ou par différentiel de temps ($TdoA$), ou sur les cellules du réseau (l'erreur est dans ce cas dépendante de la taille des cellules). Les travaux d'Interlink Networks [10] fonctionnent sur la base de la puissance du signal, en modifiant la formule de Friis [16]. Le principe est le même dans le cas du SNAP-WPS [9], qui établit une relation entre la puissance du signal et la distance entre l'émetteur et le récepteur ; dans le cas de ce système, la relation est obtenue par régression d'ordre 3 sur des données de calibration. D'autres systèmes utilisent des modes de fonctionnement complètement différents : capteurs infrarouges, ultrasons, gyroscopes et accéléromètres [17], etc.

Enfin, des travaux actuels s'emploient à faire collaborer le positionnement Wi-Fi et le positionnement par satellite, afin d'offrir une continuité de positionnement quel que soit l'endroit où se trouve le mobile, à l'intérieur comme à l'extérieur et une amélioration de l'intégrité.

4 Open Wireless Positioning System

Open Wireless Positioning System (OWLPS) [1] est un système de géolocalisation en intérieur, utilisant comme support le réseau sans fil IEEE 802.11 (Wi-Fi). Il met en œuvre plusieurs techniques de positionnement, toutes fondées sur l'analyse de la puissance des signaux Wi-Fi reçus.

4.1 Architecture

OWLPS est un système dit « centré infrastructure », car le calcul de la position des mobiles est effectué par les éléments de l'infrastructure et non par le mobile lui-même (comme c'est le cas pour un système tel que le GPS).

Cette infrastructure est essentiellement composée de points d'accès (AP) écoutant le réseau afin de repérer les informations susceptibles de permettre le positionnement d'un mobile, à savoir les demandes de localisation envoyées par ce dernier. Ces demandes sont ensuite transmises à un serveur de calcul, chargé de traiter l'information de manière à déterminer la position du mobile. Les AP ne communiquant pas entre eux, ils transmettent les demandes sans se soucier d'un quelconque ordre ; un serveur intermédiaire fait donc l'interface entre les AP et le serveur de calcul afin de présenter à ce dernier l'information de manière cohérente.

Sur le plan matériel, les mobiles peuvent être tout type d'appareil doté d'une interface Wi-Fi (ordinateur portable, téléphone cellulaire, PDA communicant, console de jeux portable…). Il en est de même pour les AP, à la différence que leur interface Wi-Fi doit supporter l'en-tête *radiotap*. Enfin, le serveur d'agrégation et le serveur de calcul peuvent être installés sur une machine plus ou moins puissante selon le nombre de mobiles [3] à tracer.

La figure 2 résume les quatre étapes de la résolution de la position d'un mobile.

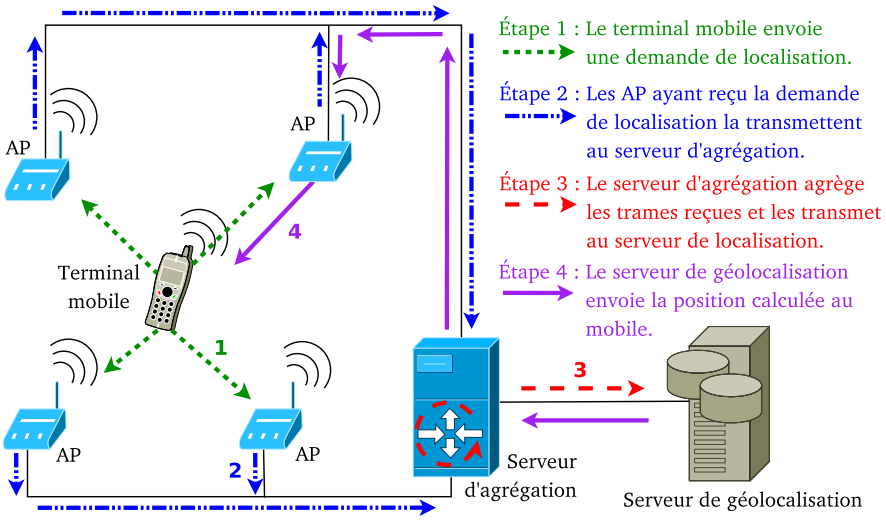


FIGURE 2: Fonctionnement en quatre étapes du système de géolocalisation centré infrastructure.

3. Lors de nos expérimentations, une simple machine de bureau assez ancienne a amplement suffi à supporter ces deux services pour un petit nombre de mobiles.

4.2 Caractéristiques

OWLPS implante plusieurs techniques de positionnement issues de la littérature (RADAR [6,11], formule d'Interlink Networks [10]) et de nos propres recherches (FBCM [12], FRBHM [13,14]). Pour cela, plusieurs caractéristiques ont du être mises en œuvre : cartographie des puissances du signal, modèles de propagation, prise en compte de la topologie du bâtiment et du parcours du mobile.

La topologie du bâtiment est décrite, lors de la configuration, comme un ensemble de zones homogènes (les pièces) reliées entre elles par des points de passage (les portes et autres ouvertures).

Afin de calibrer le système ou de réaliser une cartographie des puissances du signal, une phase hors ligne est nécessaire, pendant laquelle le mobile envoie, à des positions connues, des requêtes de calibration – qui ne sont autres que des demandes de localisation auxquelles nous ajoutons la position actuelle du mobile. Ces requêtes sont capturées par les AP de la même manière que les demandes de localisation, et les données agrégées sont enregistrées pour êtres utilisées par le serveur de calcul lors de la résolution de la position d'un mobile.

En plus du positionnement des mobiles à la demande, il est possible de considérer chaque paquet émis par ces derniers comme des demandes de localisation. Nous positionnons alors les mobiles de manière systématique, ce qui est intéressant dans le cadre d'une détection d'intrusion.

5 Expérimentations

Nous avons mené une expérimentation visant à positionner un trafic Wi-Fi à l'aide d'OWLPS, au sein d'un bâtiment hétérogène qui héberge notre laboratoire.

5.1 Matériel

Pour les expérimentations réalisées avec le système centré infrastructure, nous avons utilisé cinq mini-PC (processeur Intel Celeron M à 1,50 GHz, 512 Mo de SDRAM, carte Wi-Fi Intel BG2200 dotée d'une antenne de gain 5 dBi ; le système d'exploitation utilisé est Debian GNU/Linux Etch, la version du noyau Linux est 2.6.23.16), un point d'accès Wi-Fi (Linksys WRT54GL), un ordinateur portable (IBM Thinkpad R40, également doté d'une carte Wi-Fi Intel BG2200), et un ordinateur de bureau faisant office de serveur d'agrégation, et exploitant les mesures grâce au serveur de calcul (processeur AMD Athlon 2000+, 1 Go de SDRAM ; le système utilisé est Debian GNU/Linux Lenny).

5.2 Protocole expérimental

Les expérimentations se sont déroulées au rez-de-chaussée et au premier étage de l'aile ouest du bâtiment Numérica, où le LIFC possède ses locaux à Montbéliard. Cette aile

mesure 33,50m de long sur 10,30m de large, et comporte deux étages, ainsi qu'un sous-sol. Les dalles de béton et colonnes porteuses ont des épaisseurs variant entre 20cm et 80cm. La plupart des pièces sont des bureaux de 3,60m sur 5m dont les parois extérieures sont entièrement vitrées, alignées du côté ouest et desservies par un couloir faisant toute la longueur du bâtiment côté est ; chaque étage comporte une salle d'eau, des colonnes électriques et d'eau, et deux escaliers. Cet espace est occupé par une trentaine de personnes et est assez passant.

Les cinq mini-PC servant d'AP ont été disposés, deux au rez-de-chaussée (aux deux extrémités du bâtiment), et trois au premier étage (deux disposés dans la longueur, un peu plus resserrés qu'au rez-de-chaussée, et un à l'extérieur, dans une aile perpendiculaire au bâtiment), de manière à former une figure géométrique dans l'espace englobant la majorité des positions potentielles des mobiles.

Nous avons tout d'abord effectué une cartographie des puissances, avec un maillage d'un mètre (une mesure tous les mètres, dans quatre directions correspondant aux quatre points cardinaux), ce qui représente trois à quatre jours de travail (plus de 1200 mesures). Des mesures en mobilité ont ensuite été réalisées, traçant un déplacement sur les deux étages, en entrant dans plusieurs pièces, et ce à raison d'une mesure par seconde environ, soit un total de 86 points de mesure.

Nous avons pu comparer, pour chaque point de mesure, la position réelle, notée lors du déplacement, à la position calculée par les divers algorithmes, dans des conditions strictement identiques (environnement radio, calibration et cartographie des puissances) puisque le même jeu de mesures est utilisé. Nous avons fait varier le maillage de la cartographie des puissances, d'un mètre à quatre mètres (la distance approximative lorsque l'on ne conserve qu'une seule mesure par pièce, plus une mesure dans le couloir en face de chaque pièce).

5.3 Résultats

Maillage	Propag. [10]	Carto. [6]	Propag. calibré [12]	Carto. + propag. [13]	Carto. + histo. [11]	Carto. + propag. + histo. [14]	Carto. + propag. + histo. [14]
2m (113pts)	11,63	4,48	10,1	4,79	4,52	5,03	5,01
4m (35pts)	11,63	5,03	7	5,94	4,77	5,78	6,07

TABLE 2: Erreur moyenne (en mètres) du positionnement d'un terminal en mouvement. *(Propag. = modèle de propagation, Carto. = cartographie des puissances du signal, Histo. = historique des positions du mobile.)*

Les principaux résultats obtenus sont présentés dans le tableau 2. Les combinaisons algorithmes et techniques de positionnement offrant les meilleures précisions sont RADAR et RADAR avec Viterbi-like, qui illustrent respectivement la cartographie des puissances du

signal seule et combinée avec un historique des positions du mobile. On peut constater que le bénéfice tiré de la mémorisation du parcours antérieur du mobile grâce à un algorithme à la Viterbi n'améliore pas significativement la précision. La série des algorithmes et techniques combinant cartographie et modèle de propagation, et éventuellement un historique des positions du mobile (FRBHM) a une précision légèrement moins bonne, quoique comparable (l'erreur dépasse d'environ un mètre au maximum celle de RADAR) ; les résultats des FRBHM avec historique confirment le fait que l'algorithme à la Viterbi n'apporte pas de précision : dans la plupart des cas, le FRBHM sans historique est plus précis. Enfin, viennent les techniques n'utilisant que l'atténuation du signal (modèle de propagation non calibré ou calibré, respectivement Interlink Networks et FBCM) et la multilatération, qui souffrent d'une erreur beaucoup plus grande ; à noter que l'erreur de la première technique est fixe car elle ne dépend pas du maillage (puisqu'aucune calibration n'est utilisée), tandis que celle du FBCM varie, car il utilise les points de calibration pour modifier la formule d'atténuation du signal employée.

On peut constater que la précision des algorithmes fondés sur une cartographie des puissances ne varie que légèrement en fonction de la finesse du maillage. À noter qu'une étude plus poussée [18] a montré qu'un maillage plus fin (1m) n'offre pas les meilleurs résultats, et que tous les algorithmes et techniques révèlent leur meilleure précision avec un maillage de deux mètres.

À l'occasion d'évaluations complémentaires [1], nous avons observé le comportement des différentes techniques en faisant varier le nombre d'AP (de 3 à 5). Cela révèle une baisse générale de la précision lorsque l'on diminue le nombre d'AP, sauf pour l'algorithme FBCM.

Ces observations invitent à plusieurs éléments d'analyse. Tout d'abord, pour démontrer la pertinence d'une combinaison (algorithme et technique) telle que la mémorisation de l'historique et son adéquation à un environnement (topologie de bâtiment, exposition à la réflexion, réfraction, absorption en multi-chemin, interférences), il est nécessaire d'introduire un critère de précision topologique, puis de l'appliquer à différents types de bâtiments. Ensuite, il n'existe actuellement pas de modèle d'atténuation satisfaisant en environnement hétérogène et hostile (comme Numérica), alors que dans des espaces clos avec peu ou pas d'obstacles (cloisons, sols, plafonds) des modèles sont efficaces (un rebond sur le sol, rebond sol et plafond). Cela requiert d'évaluer d'autres approches (temps d'arrivée, déphasage). Enfin, la précision n'augmente pas de manière linéaire avec la densité du maillage ; nous pensons que cela peut être imputable à la pérégrination du mobile, les points de calibration, et la prise en compte de la topologie du bâtiment. Toutes ces analyses se doivent d'être validées afin d'aboutir à la compréhension des liens unissant telle approche avec tel environnement.

6 Histoire de l'art de l'acquisition Wi-Fi

6.1 (2000) – La période propriétaire

Initialement, les premiers matériels de communication Wi-Fi étaient composés d'un point d'accès constitué d'un système embarqué propriétaire et d'une carte réseau sans fil, associés à un pilote logiciel et un microcode (*firmware*) embarqué sur la carte. Les accès aux données de la couche physique et de la couche liaison n'étaient pas possibles. En effet, il n'y avait pas d'API pour obtenir des informations de bas niveau. Cependant, à l'aide des logiciels propriétaires livrés par les constructeurs tels que Aironet/Cisco ou Orinoco, l'obtention de statistiques générales concernant la couche physique était possible. Les pilotes de carte Wi-Fi n'existaient pas pour l'environnement UNIX. Il était seulement possible d'imaginer qu'un accès aux données de la couche physique serait disponible assez rapidement du côté des clients. De plus, la plupart des interfaces Wi-Fi en mode client ou station filtrent les paquets en retournant uniquement les paquets de données et en remplaçant l'en-tête 802.11 (Wi-Fi) par un en-tête 802.3 (Ethernet).

6.2 (2002) – La période du mode client libre

Les premiers pilotes libres sont apparus associés aux *chipsets* Prism et Orinoco. Malgré tout, le microcode de la carte Wi-Fi reste très protégé. L'accès aux données de la couche Wi-Fi est partiellement accessible. Cependant, la plupart des pilotes ne créent que des interfaces réseau de type Ethernet. À partir de ce moment là, les premiers travaux de recherche concernant le positionnement Wi-Fi voient le jour avec une fonction de positionnement intégrée dans les terminaux.

La suite logicielle *wireless-tools*, composée de *iwconfig*, *iwscan*, *iwspy* et *iwpriv*, permet d'obtenir des statistiques générales sur les données de la couche physique en interrogeant le pilote de la carte. *iwscan* et *iwspy* permettent selon le matériel d'obtenir l'atténuation moyenne des émissions Wi-Fi et *iwpriv* configure les paramètres de la carte.

Puis, la première solution permettant d'obtenir des informations détaillées par paquet est apparue sous la forme d'une insertion d'en-tête de type *AVS* ou *PRISM* devant l'en-tête de niveau 2. Cela a ouvert une nouvelle voie où les systèmes de positionnement allaient devenir plus réactifs et plus précis. La contre-partie concerne l'impossibilité de faire fonctionner un applicatif simultanément à cause de l'introduction de cet en-tête non prévu. De ce fait, le mode *monitoring*, qui est un mode complètement passif, a été de plus en plus utilisé. C'est ce mode qui permet en général d'intercepter l'intégralité du trafic Wi-Fi tout en conservant les en-têtes d'origine (802.11). Cependant, en fonction du modèle de carte, les informations sont plus ou moins bien renseignées.

6.3 (2003) – La période du mode point d'accès programmable

Les premières cartes Wi-Fi intégrant le mode *master* (appelé aussi *ap*) dans leur microcode apparaissent. Elles sont généralement associées au logiciel *hostap*. Les premiers

ordinateurs intégrant une carte Wi-Fi peuvent à présent servir de point d'accès. Toute la puissance du système d'exploitation GNU/Linux permet donc de transformer un ordinateur en point d'accès réseau programmable. La fonction de positionnement peut s'envisager depuis un élément d'infrastructure. Cette manière de positionner élargit le champ d'applications aux terminaux sans logiciel installé, c'est-à-dire qu'il devient possible de positionner tout type de terminal Wi-Fi qu'il soit intégré dans une architecture ou bien en situation tiers. Cependant, le cout de déploiement de chaque point d'accès est assez élevé. Le mode *monitor* permet également de recevoir le trafic, mais c'est un mode passif qui ne permet pas la double fonction : point d'accès et point de mesure.

Une grande avancée a été effectuée lors de l'apparition des en-têtes *radiotap* dans quelques pilotes. Une des premières intégrations a été effectuée dans le système NetBSD en 2001 (FreeBSD en 2003). Elle a été ensuite portée sous GNU/Linux en 2006. Cette bibliothèque fonctionne de manière stable principalement avec le *chipset* Intel des versions Centrino appelé initialement BG2200 et les *chipsets* Atheros.

6.4 (2004) – La période du point d'accès ouvert

La société Linksys, marque grand public de Cisco, met sur le marché en 2003 une borne Wi-Fi nommée WRT54G (*Wireless Router 54Mbps 802.11g*) intégrant un système GNU/-Linux embarqué. Cette borne Wi-Fi dispose d'un processeur de type MIPS. En 2004, les premières versions libres d'un système d'exploitation ouvert apparaissent. Les deux distributions les plus répandues sont DD-WRT et OpenWRT. À l'aide d'OpenWRT, il devient possible d'exécuter du code additionnel à partir d'une suite de cross-compilation. Cependant, l'utilisation de l'extension *radiotap* est difficile à mettre en place, car le microcode de la carte Wi-Fi reste protégé. La société Fon diffuse depuis la fin de l'année 2006 une borne Wi-Fi équipée d'un *chipset* Atheros dont le microcode est beaucoup plus ouvert. La bibliothèque *radiotap* s'intègre facilement et fonctionne de manière stable. Les valeurs indiquées dans les champs de l'en-tête *radiotap* sont correctes.

7 Travaux futurs et perspectives

OWLPS est une plate-forme expérimentale permettant l'évaluation de différentes techniques de géolocalisation dans un espace à trois dimensions ; ces techniques sont mises en situation identique, de manière à obtenir des résultats comparables. Les techniques mises en œuvre sont fondées sur une cartographie des puissances, des modèles d'atténuation de la puissance du signal, un historique dynamique des itinéraires des mobiles, et la topologie du bâtiment. Les plus précises offrent une précision d'environ 5 mètres dans un espace intérieur très hétérogène, en requérant une calibration limitée à un peu plus d'un point de référence par pièce, pour une densité de 5 AP pour 600 mÂš sur deux étages.

Un tel système est approprié au calcul de la position de mobiles situés à l'extérieur des bâtiments, avec un couplage éventuel avec d'autres systèmes de positionnement [19,20], tels

que le GPS ou le positionnement par GSM. Il est de plus possible de détecter les intrusions et de calculer la position [21], dans la zone couverte, de mobiles non autorisés, et ce en écoutant tout le trafic réseau, chaque paquet capturé par les AP représentant alors une demande implicite de positionnement (alors que les demandes de localisation émises par les mobiles autorisés, comme dans le cadre de nos expérimentations, sont des demandes explicites).

Le système OWLPS a encore besoin d'un peu de travail afin d'être aisément utilisable, notamment au niveau du serveur de calcul de la position, qui est encore à un stade expérimental. Mais le gros des développements futurs portera sur l'ajout de fonctionnalités.

Le principal axe des recherches futures est l'auto-calibration du système. Il a en effet été observé que l'environnement intérieur des bâtiments, en plus d'être très hétérogène, évolue beaucoup. En fonction de l'heure de la journée par exemple, le nombre de personnes évolue ; des meubles peuvent être déplacés, de l'eau circuler dans les canalisations ou pas... Autant de facteurs influant sur le comportement du signal. Les éléments de l'infrastructure pourraient donc échanger périodiquement des informations de signalisation, qui serviraient de base pour corriger le paramétrage du système. Ainsi, si la fréquentation de la zone couverte augmente subitement, le signal se trouvera plus atténué, et les distances seront surestimées ; les éléments de l'infrastructure, en échangeant des messages, pourraient se rendre compte du changement, et appliquer une correction sur leurs estimations.

Ce principe pourrait également être appliqué dans le cadre d'une infrastructure mobile. Si les AP sont amenés à se déplacer ou à être déplacés régulièrement, il serait intéressant que l'infrastructure recalcule la position de l'AP déplacé (position absolue calculée grâce à des points fixes connus, ou relative aux autres AP).

Nous avons également en vue la problématique de la continuité des services dépendants du contexte [14,22], en intérieur comme en extérieur. Pour cela, de nombreux verrous sont à lever. Tout d'abord, la contextualisation des applications nécessite un géopositionnement dans des environnements divers (extérieurs et intérieurs). Ensuite, un service riche contextuel nécessite de la communication multiple (réseaux d'infrastructure mais aussi *ad hoc*, sur différents supports). En outre, il faut proposer des mécanismes permettant de mettre en œuvre une continuité (prédiction de mobilité, systèmes de cache avec pré-chargement, handover, etc.).

8 Conclusion

Le système de positionnement intérieur OWLPS, que nous développons, fonctionne actuellement à l'aide de requêtes explicites provenant du terminal. C'est l'infrastructure qui calcule la position des terminaux actifs dans l'environnement. Le positionnement implicite, c'est-à-dire sans l'envoi de requêtes du terminal, est la prochaine étape d'intégration. Pour que les points d'accès Wi-Fi puissent être déployés simplement, il sera nécessaire qu'ils puissent tous détecter automatiquement les variations de puissance, qui peuvent provenir

de plusieurs facteurs tels que la présence d'une foule ou des transformations dans la structure du bâtiment. Enfin, concernant l'acquisition qui est actuellement traitée isolément pour chaque points d'accès, une approche de données fusionnées permettra de suivre plus efficacement les utilisateurs dans leurs déplacements.

Remerciements

Ce travail est le fruit d'un projet financé par l'ANR, la Région Franche-Comté, la Communauté d'Agglomération du Pays de Montbéliard, et le Pôle Véhicule du Futur.

Références

1. Cypriani, M., Lassabe, F., Zirari, S., Canalda, P., Spies, F. : Open Wireless Positioning System. Technical Report RT2008-02, LIFC – Laboratoire d'Informatique de l'Université de Franche-Comté (December 2008)
2. radiotap : Site officiel `http://www.radiotap.org/`.
3. Wireshark : Site officiel `http://www.wireshark.org/`.
4. Wireless Tools for Linux : Site officiel `http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html`.
5. MadWiFi : Site officiel `http://www.madwifi-project.org/`.
6. Bahl, P., Padmanabhan, V.N. : RADAR : An in-building RF-based user location and tracking system. In : INFOCOM (2). (2000) 775–784
7. Youssef, M., Agrawala, A., Shankar, A., Noh, S. : A probabilistic clustering-based indoor location determination system, UM Computer Science Department ; CS-TR-4350 (2002)
8. Roos, R., Myllymäki, P., Tirri, H., Misikangas, P., Sievänen, J. : A Probabilistic Approach to WLAN User Location Estimation. International Journal of Wireless Information Networks **9**(3) (July 2002) 155–164
9. Wang, Y., Jia, X., Lee, H. : An indoors wireless positioning system based on wireless local area network infrastructure. In : 6th Int. Symp. on Satellite Navigation Technology Including Mobile Positioning & Location Services. Number paper 54, Melbourne (July 2003)
10. Interlink Networks, Inc. : A practical approach to identifying and tracking unauthorized 802.11 cards and access points. Technical report (2002)
11. Bahl, P., Balachandran, A., Padmanabhan, V. : Enhancements to the radar user location and tracking system. Technical report, Microsoft Research (2000)
12. Lassabe, F., Baala, O., Canalda, P., Chatonnay, P., Spies, F. : A Friis-based calibrated model for Wi-Fi terminals positioning. In : Proceedings of IEEE Int. Symp. on a World of Wireless, Mobile and Multimedia Networks, Taormina, Italy (June 2005) 382–387
13. Lassabe, F., Charlet, D., Canalda, P., Chatonnay, P., Spies, F. : Refining Wi-Fi indoor positionning renders pertinent deploying location-based multimedia guide. In : Procs of IEEE 20th Int. Conf. on Advanced Information Networking and Applications. Volume 2., Vienna, Austria (April 2006) 126–130
14. Lassabe, F. : Géolocalisation et prédiction dans les réseaux Wi-Fi en intérieur. PhD thesis, École doctorale SPIM (2009)
15. Youssef, M.A., Agrawala, A., Shankar, A.U., Noh, S.H. : A probabilistic clustering-based indoor location determination system. Tech. Report CS-TR-4350, University of Maryland (March 2002)

16. Blake, L. : Radar Range-Performance Analysis. Artech House Radar Library (December 1986)
17. Moix, S., Steiner, C., Ladetto, Q., Merminod, B. : Capteurs et analyse de signaux pour la navigation pédestre. MPG (August 2002) pp. 512–516
18. Cypriani, M., Lassabe, F., Canalda, P., Zirari, S., Spies, F. : Open wireless positioning system : un système de géopositionnement par wi-fi en intérieur. In Caminada, A., ed. : JDIR'09, 10èmes Journées Doctorales en Informatique et Réseaux, Belfort, France (February 2009) 73–78
19. Zirari, S., Canalda, P., Spies, F. : Geometric and signal strength dilution of precision (DoP) Wi-Fi. Int. Journal of Computer Science Issues **3** (August 2009) 35–44
20. Zirari, S., Canalda, P., Spies, F. : Modelling and emulation of an extended GDOP for hybrid and combined positioning system. In : ENC-GNSS'09, European Navigation Conference - Global Navigation Satellite Systems, Naples, Italy (May 2009) 6 pages, CD-ROM publication.
21. Cypriani, M., Canalda, P., Spies, F. : Problématiques de sécurité dans un système de géolocalisation implicite. In : Colloque Francophone sur l'Ingénierie des Protocoles, Strasbourg (October 2009) 2 pages, Poster session.
22. Zirari, S., Canalda, P., Spies, F. : Critère de dilution de précision pour un positionnement en intérieur et en extérieur. In : Colloque Francophone sur l'Ingénierie des Protocoles, Strasbourg (October 2009) 2 pages, Poster session.

Attaques Wi-Fi - WPA

Cédric Blancher

EADS
cedric.blancher@eads.net

Après quatre ans comme consultant en sécurité des systèmes d'information, Cédric Blancher a rejoint le laboratoire de recherche en sécurité informatique tout juste créé chez EADS Innovation Works. D'abord ingénieur-chercheur, avec des travaux focalisés sur la sécurité des réseaux de données et les honeypots, puis responsable du laboratoire pendant trois ans, il intervient aujourd'hui à l'échelle du groupe en tant que Senior Expert. Rédacteur pour MISC et Linux Magazine, membre du groupe Rstack et du chapitre français du Honeynet Project, intervenant en mastère à la faculté de Limoges et à l'ESIEA, conférencier et serial blogger à ses heures, il participe également à la promotion et au développement du logiciel libre en SSI, particulièrement dans les pays en voie de développement, via un programme de l'organisation Internationale de la Francophonie.

Sécurité UMTS

Henri Gilbert

Orange Labs
henri.gilbert@orange-ftgroup.com

Henri Gilbert received the engineer degrees of Ecole Polytechnique and Telecom Paris, and a PhD in Computer Science from University Paris XI. He has been working at France Telecom since 1984. He took part in the specification of the radio subsystem architecture and protocols of the GSM mobile communications system. He has been doing research in cryptology since 1990, was responsible for the security research activities of France Telecom until 2006, and is currently fellow expert in cryptology at Orange Labs. His main current areas of interest are the design and cryptanalysis of symmetric ciphers, authentication schemes, and software/content protection algorithms. He designed cryptologic algorithms used in various systems operated by Orange, participated in numerous standardisation committees and national or European research projects (RNRT, ANR, Eurescom, IST), and is a member of the European group of experts in charge of specifying security algorithms for telecommunication systems (ETSI/SAGE). He is the (co-)author of numerous international publications and patents, and has served on more than 20 international program/lecture committees.

Démonstration relative aux dangers des réseaux de type Wi-Fi

Christophe Rault

Centre d'électronique de l'armement BP 57419 la Roche Marguerite 35174 BRUZ-CEDEX
christophe.rault@dga.defense.gouv.fr

Le scénario joué dans cette démonstration fait intervenir une machine cible équipée de Wi-Fi. L'utilisateur de cette machine se connecte à Internet dans le cadre professionnel, via l'architecture de l'entreprise ou via des architectures privées (hôtel, gare, HotSpot), ou bien dans le cadre privé via sa Box préférée. Pour la majorité des configurations constatées, cette machine peut de façon transparente se raccorder automatiquement à un point d'accès Wi-Fi, du type HotSpot par exemple. Ce point d'accès peut être légitime, ou illégitime (FakeAp), c'est-à-dire mis en place de façon opportuniste par un attaquant. Cet attaquant crée donc un HotSpot afin que la machine de la victime se connecte à son piège. La machine cible se connecte alors sur ce point d'accès, et son propriétaire va accéder aux services habituels. L'attaque montrée ici est du type « Man in The Middle » (MiTM). Elle va permettre l'écoute des flux aussi bien que l'intrusion sur la machine cible. La démonstration réalisée illustre les étapes de ce scénario.

Mots clés : Wi-Fi, menace, sans fil, attaque.

Deuxième partie

Vérification de protocoles dans les réseaux ad hoc

Professeur Ana Cavalli

INSTITUT TELECOM/ TELECOM SudParis 9 rue Charles Fourier, 91011 Évry Cedex

Résumé Dans cet exposé, nous présentons des techniques de vérification, basées sur le test et le monitorage, et leur application à la vérification des propriétés des protocoles de routage pour les réseaux ad hoc. Les techniques de test actif vérifient la conformité d'une implantation donnée à son spécification. L'implantation sous test est exécutée avec des valeurs d'entrée spécifiques et les sorties observées sont évaluées par rapport à la spécification. Les techniques de monitorage, consistent à examiner de façon passive le comportement d'entrée/sortie d'une implantation sans pour autant imposer les entrées. La force majeure du monitorage est sa capacité à être utilisé sur un réseau en cours de fonctionnement. Ces nouvelles techniques devront permettre l'automatisation de la supervision d'un système, ainsi que le développement des moyens de prévention des problèmes rencontrés. En outre, l'application de ces méthodes suppose une révision des modèles classiques d'architecture afin d'atténuer les difficultés liées aux manques de contrôle et d'accessibilité. Une démarche de combinaison de la technique de monitorage avec l'injection de fautes pour étudier le comportement d'un système en présence d'événements redoutés est également présenté. Il s'agit de tester si un système réagit correctement en présence de fautes. Ces différentes techniques sont illustrées sur un cas d'étude du domaine des réseaux ad hoc : les protocoles de routage, et en particulier le protocole OLSR. Nous montrons comment il est possible d'adapter ces techniques pour la validation des propriétés de sécurité et la détection d'intrusion.

Mots clés : vérification, test de conformité, monitorage, méthodes de génération de test, réseaux ad hoc, protocoles de routage, propriétés de sécurité.

Références

1. Ana Cavalli, Stephane Maag and Edgardo Montes de Oca, A Passive Conformance Testing Approach for a Manet Routing Protocol, The 24th Annual ACM Symposium on Applied Computing SAC'09, March 9-12 2009, Hawaii, USA.

2. Anderson Morais, Eliane Martins, Ana Cavalli, Willy Jimenez, Security Protocol Testing Using Attack Trees, IEEE/IFIP International Symposium on Trusted Computing and Communications (TrustCom-09), August 29-31, 2009, Vancouver, Canada.

3. Cesar Andres, Stephane Maag, Ana Cavalli, Mercedes G. Merayo, Manuel Nunez, Analysis of the OLSR Protocol by using formal passive testing, APSEC 2009, December 2009, Penang, Malaysia.

4. Wissam Mallouli, Bachar Wehbi, Ana R. Cavalli, Distributed Monitoring in Ad Hoc Networks : Conformance and Security Checking, The 7th International Conference on AD-HOC Networks & Wireless (ADHOC-Now 2008), September 10-12, Sophia Antipolis, France.

5. Bachar Wehbi, Anis Laouiti, Ana R. Cavalli, Efficient Time Synchronization Mechanism for Wireless Multi Hop Networks, The 19th annual IEEE International Symposium

on Personal, Indoor and Mobile Radio Communications (PIMRC 2008), September 15-18, Cannes, France.

6. Stéphane Maag, Cyril Grepet, Ana R. Cavalli, A Formal Validation Methodology for MANET Routing Protocols Based on Nodes' Self Similarity, Computer Communications Journal 31(4) : 827-841, 2008.

7. J. M. Orset and A. Cavalli, A Security Model for OLSR Manet Protocol, Workshop on Future Mobile and Ubiquitous Information Technologies (FMUIT), May 2006, Nara, Japan.

8. D. Lee, D. Cheng, R. Hao, R. E. Miller, J. Wu and X. Yin, ŞNetwork Protocol System Monitoring - a Formal Approach with Passive TestingŤ, IEEE/ACM Trans. On Networking, April 2006.

9. J.-M. Orset, B. Alcalde and A. Cavalli, An EFSM-Based Intrusion Detection System for Ad Hoc Networks, ATVA 05, Taipei, Taiwan, October 2005.

10. Emmanuel Bayse, Ana R. Cavalli, Manuel Núñez, Fatiha Zaïdi : A passive testing approach based on invariants : application to the WAP, Computer Networks 48(2) : 235-245 (2005).

11. B. Alcalde, A. Cavalli, D. Chen, D. Khuu, and D. Lee, ŞPassive Testing on EFSM by Variable Determination and Backward CheckingŤ, Proc. FORTE/PSTV, 2004.

12. D. Lee and M. Yannakakis, ŞPrinciples and Methods of Testing Finite State Machines - A SurveyŤ, Proceedings of The IEEE, Vol. 84, No. 8, August 1996, pp. 1090-1123.

13. A. Cavalli, D. Lee, C. Rinderknecht and F. Zaidi, ŞHIT-OR-JUMP : an Algorithm for Embedded Testing with Applications to IN ServicesŤ, Proc. FORTE/PSTV, 1999.

Survivability Of Mobile Ad Hoc Networks In Military Applications

Cédric Adjih[1] , Pascale Minet[1], Paul Muhlethaler[1] and Thierry Plesse[2]

[1] INRIA, Rocquencourt, 78153 Le Chesnay Cedex, France
cedric.adjih@inria.fr, pascale.minet@inria.fr, paul.muhlethaler@inria.fr
[2] DGA/CELAR, BP 7419, 35174 Bruz Cedex, France
thierry.plesse@dga.defense.gouv.fr

Abstract Mobile ad hoc networks (MANETs) are autonomous, self-organized and adaptive networks supporting mobility. Their ability to adapt themselves to dynamic, random and rapidly changing multihop topologies is given by a multihop routing protocol. Survivability of these networks can be compromised by potential attacks against routing. In this paper, we focus on the OLSR routing protocol, standardized by IETF. We first list and classify these potential attacks and then show how to secure the OLSR routing against them. This solution has been implemented on a real platform of 18 nodes communicating over a 802.11b network, using either IPv4 or IPv6.

Keywords : MANET, routing protocol, security, OLSR.

1 MANETs for military tactical networks

1.1 Needs of military applications

The arrival of new military concepts like NEC (Network Enabled Capability), NOC (Network Centric Operation), and NCW (Network Centric Warfare) has increased dramatically the need of network survivability.

Tactical networks have to face potential survivability troubles due to the tactical environment. Links and nodes may be degraded or even out of order, destroyed or simply jammed, at any moment.

Survivability means protecting military information. It includes the assurance that this information can continue to be used in a battle environment for as long as needed. That means the ability to restore some of the damaged parts of networks to maintain an operational status and to integrate fragmented parts into a surviving and enduring network.

Today, for instance, some nodes are essential and service is degraded or stopped when they become inoperative, like master node in legacy tactical radio networks. The ability to restore is partly addressed by some of the network management functions.

Reconfiguration is made easier by use of a common internetworking solution with a flat architecture, meaning that any router can potentially replace a defective one, within the limits of the physical interface compatibility and the hardware performances.

Automatic reconfiguration and meshed topology are critical items to provide enhanced availability of tactical networks. If intermediate nodes are destroyed or become otherwise unavailable, there is still a chance that the data can be sent via alternate paths.

1.2 Potentialities of mobile ad hoc networks

Mobile ad hoc networks, MANETs, have a lot of potentialities that make them good candidates for military application support. For instance, as they do not require any preexisting infrastructure to communicate, they are well adapted for rescue applications when the existing infrastructure is partially or totally damaged. They can also offer internet access to poorly covered areas. Another big advantage of MANETs is that they are decentralized. A centralized control would mean a single point of failure and a bottleneck on both the central entity and the links with this entity. This decentralized control makes MANETs more robust.

The main reason of the success of mobile ad hoc networks lies in their support of node mobility. Any node in a MANET can move, the routing protocol should allow it to communicate with any other node, possibly moving too, in the network. The last very interesting characteristic of MANETs is they are self adaptive and self organizing. MANETs aim at operating in a highly changing environment :

- radio propagation is versatile ;
- topology changes because of the arrival/departure of nodes, moving obstacles, ... New links are created, other ones are broken ;
- node mobility increases the frequency of link creation/breakage ;
- traffic distribution is time and space varying. This is partially due to node mobility.

1.3 Protocols for mobile ad hoc networks

Protocols operating over mobile ad hoc networks should be designed in order to preserve the inherent potentialities of these networks. An example of such protocols is the routing protocol in charge of building a route to any destination in the network. We have shown in [Adjih 2005a] that the OLSR routing protocol adapts to topology changes and supports mobility, always providing the shortest path to the destination. Additional modules must also be present in order to provide the self-organizing potentiality of these networks. For instance, auto-configuration allows a node to join the network at any time, an address being automatically allocated to the joining node. In order to protect the network against potential attacks, routing should be secured. We will focus in this paper on the module in charge of securing the routing protocol against potential attacks.

2 The OLSR routing protocol

As radio coverage is usually limited, multihop routing is generally needed. The IETF MANET (Mobile Ad-hoc NETwork) working group aims at standardizing dynamic routing in ad-hoc networks. All the routing protocols proposed in the MANET group address the problem of unicast routing, while taking into account the features of wireless, multihop, mobile ad-hoc networks. Such protocols can be divided into two classes : proactive and reactive, depending on the route establishment mechanism that is used.

With reactive protocols, a node discovers routes on-demand and maintains only active ones. Thus, a route is discovered whenever a source node needs to communicate with a destination node for which a route is not available. This discovery mechanism is based on pure flooding in the network. The main reactive protocol is AODV [Perkins 2003].

OLSR (Optimized Link State Routing) [Adjih 2003a] is a proactive routing protocol that is now an RFC. It provides the advantage of having routes immediately available in each node for all destinations in the network. Periodic control packets are in charge of monitoring the network topology. This class of protocol is particularly well suited for applications where all nodes can use the topology knowledge discovered by the routing protocol. Moreover, proactive routing protocols can be used without modification in the network protocol stack.

2.1 OLSR presentation

OLSR is an optimization of a pure link state routing protocol. It is based on the concept of multipoint relays, denoted MPRs. First, using multipoint relays reduces the size of the control messages :

- rather than declaring all links, a node declares only the set of links with its neighbors that are its multipoint relays.
- only the multipoint relays of the sender node forward control messages. This technique significantly reduces the number of retransmissions of broadcast control messages [Qayyum 2002].

The two main OLSR functionalities, Neighbor Sensing and Topology Discovery, are now detailed.

Neighbor Sensing Each node must detect the neighbor nodes with which it has a direct link. For this, each node periodically broadcasts HELLO messages, containing the list of neighbors known to the node and their link status. The link status can be either :

- symmetric : if communication is possible in both directions,
- asymmetric : if communication is only possible in one direction,
- multipoint relay : if the link is symmetric and the sender of the HELLO message has selected this node as multipoint relay,
- or lost : if the link has been lost.

The HELLO messages are received by all one-hop neighbors, but are not forwarded. They are broadcast once per refreshing period. The default period value is 2 seconds. Thus, HELLO messages enable each node to discover its one-hop neighbors, as well as its two-hop neighbors. This neighborhood and two-hop neighborhood information has an associated holding time, after which it is no longer valid. On the basis of this information, each node independently selects its own set of multipoint relays among its one-hop neighbors in such a way the multipoint relays cover (in terms of radio range) all two-hop neighbors (see [Qayyum 2002] for an algorithm example). Figure 1 illustrates the multipoint relays of node m.

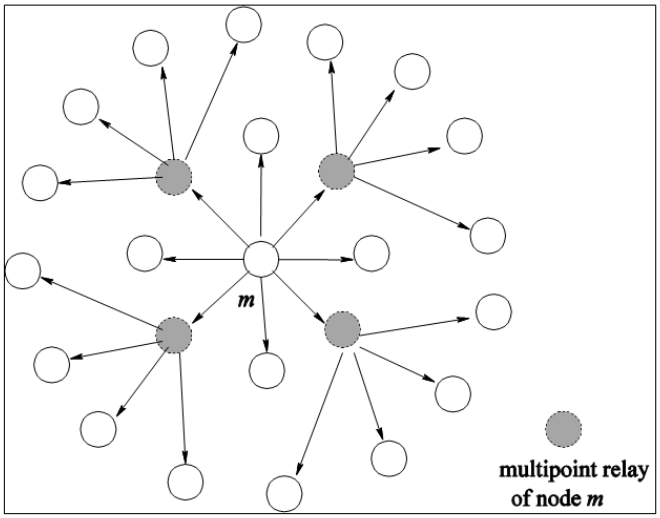


FIGURE 1: Multipoint relays of node m

The multipoint relay set is computed whenever a change in the one-hop or two-hop neighborhood is detected.

Topology Discovery Each node of the network maintains topological information about the network obtained by means of TC, Topology Control, messages. Each node selected as multipoint relay, broadcasts a TC message periodically. The default period value is 5 seconds. The TC message declares the nodes having selected the message originator as multipoint relay. The TC messages are flooded to all nodes in the network and take advantage of MPRs to reduce the number of retransmissions. Thus, a node is reachable either directly or via its MPRs. This topological information collected in each node has also an associated holding time, after which it is no longer valid.

The neighbor information and the topology information are refreshed periodically, and they enable each node to compute the routes to all known destinations. These routes are computed with Dijkstra's shortest path algorithm. Hence, they are optimal as concerns the number of hops. The routing table is computed whenever there is a change in neighborhood or topology information.

2.2 OLSR platform

CELAR (French MoD / DGA) works on the concept of ad-hoc networks. These studies interest military programs like "Soldier of the Future", and could be fully integrated in RHD project (High Data Bit Rate Radio), for Navy and Land tactical networks. The objective of

the MANET/OLSR CELAR tesbed is to evaluate and demonstrate the potential benefits of MANET advances in military tactical applications.

The CELAR MANET/OLSR platform, illustrated in Figure 2, is a real network using 802.11b radio technology (Wi-Fi) consisting of 18 MANET/OLSR nodes (10 routers, 4 VAIO laptops, 4 iPAQ PDAs). These nodes implement OLSR routing. This wireless network allows the communications between :

- the different floors of a building including a central tower : see routers R02 to R08 on figure 2 ;
- a shelter : see router R09 on figure 2 ;
- pedestrians with laptops or PDAs moving outside ;
- vehicles : see embedded routers R01 and R10 on figure 2.

This platform was built at the end of December 2002. It has been improved since its installation. It now supports both IPv4 and IPv6. OLSR routing has been secured against potential attacks. A Quality of Service support has been added [Nguyen 2006]. This network is now interconnected with an OSPF network.

3 SECURED OLSR ROUTING

A significant issue in the ad-hoc network domain is that of the integrity of the network itself. OLSR allows, according to its specification, any node to participate in the network - the assumption being that all nodes are behaving well and welcome. If that assumption fails - then the network may be subject to malicious nodes, and the integrity of the network fails. An orthogonal security issue is that of maintaining confidentiality and integrity of the data being exchanged between communications endpoints in the network. This issue has already received lot of attention for wired networks and we will not be considered it in the following. We will first study the attacks that can be launched against the integrity of OLSR networks. We will, then, study how these attacks can be countered.

3.1 Attacks against OLSR routing

Considering the OLSR specifications, it is simple to classify the potential attacks in two different kinds, see [Adjih 2003b] and [Adjih 2005b]. The first kind consists in incorrect message generations i.e. an attacker node is not sending control messages compliant with OLSR specification [3]. The second kind consists in incorrect traffic relaying i.e. the attacker node is not properly relaying the packets. These packets can be control packets or data packets.

OLSR employs, basically, two different kinds of control traffic : HELLO messages and TC messages. An attacker node may affect the network connectivity through incorrect generation of HELLO and TC messages. In general, we observe that with respect to control

3. We will not consider jamming attacks where a node generates massive amounts of interfering radio transmissions, which will prevent legitimate traffic to be received in the network. This vulnerability cannot be dealt with at the routing protocol level (if at all).

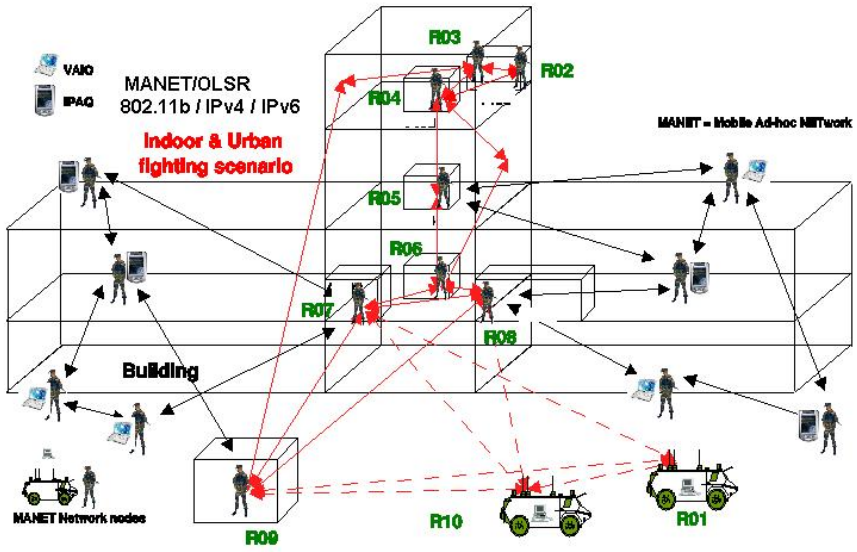


FIGURE 2: CELAR MANET/OLSR platform

traffic generation, a node may misbehave in two different ways : through generating control traffic "pretending" to be another node (i.e. Identity Spoofing) or through advertising incorrect information (links) in the control messages (i.e. Link Spoofing).

In terms of HELLO messages, Identity Spoofing implies that a node sends HELLO messages, pretending to have the identity of another node. E.g. node X sends HELLO messages, with the originator address set to that of node A, as illustrated in the figure 3 below. This may result in the network containing conflicting routes to node A. Specifically, node X will choose MPRs from among its neighbors, signaling this selection pretending to have the identity of node A. The MPRs will, subsequently, advertise that they can provide "last hop" to node A in their TC messages. Conflicting routes to node A, with possible loops, may result from this.

Similarly, Link Spoofing implies that a node sends HELLO messages, signaling an incorrect set of neighbors. This may take either of two forms : if the set is incomplete, i.e. a

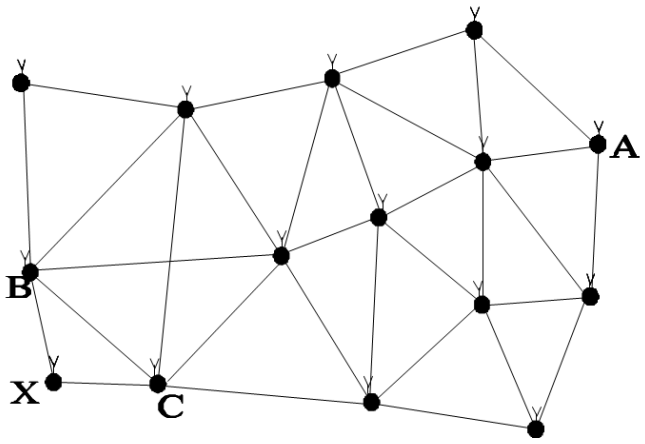


FIGURE 3: Identity Spoofing in HELLO control messages

node "ignores" some neighbors, the network may be without connectivity to these "ignored" neighbors.

Alternatively, an intruder advertising a neighbor-relationship to non-present nodes may cause inaccurate MPR selection with the result that some nodes may not be reachable in the network. In figure 4 below, X pretends to be a neighbor of node B. Thus D can choose as MPR set nodes X and E (smallest MPR set with this two-hop neighborhood). TC messages from F will not be delivered to B. Should X operate correctly, D would have to choose as MPR set nodes X, C and E and the TC flooding will work correctly.

As for HELLO messages, Identity Spoofing with respect to TC messages implies that a node sends TC messages, pretending to have the identity of another node. Effectively, this implies Link Spoofing since a node assuming the identity of another node effectively advertises incorrect links to the network. Similarly, Link Spoofing implies that a node sends TC messages, advertising an incorrect set of links. This may take either of two forms : if the set is incomplete, i.e. a node "ignores" links to some nodes in its MPR selector set, the network may be without connectivity to these "ignored" neighbors - as well as to neighbors which are reachable only through the "ignored" neighbors. A node may also include non-

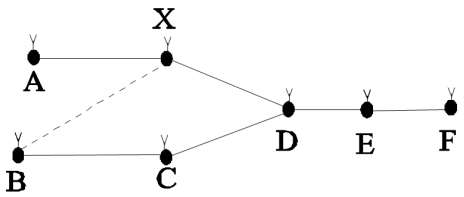


FIGURE 4: Wrong information about a node neighborhood may cause inaccurate MPR selection and uncomplete flooding

existing links (i.e. links to non-neighbor nodes) in a TC message. Link spoofing in TC messages may yield routing loops and conflicting routes in the network.

An intruder node can reuse already generated messages in the network. Generated messages within an average timescale (more than a few seconds) can be replayed by an attacker, these obsolete control messages will probably contain inaccurate topology information. Another possible attack is when a control traffic from one region of the network is recorded and within, a small timescale (less than a few seconds), replayed in a different region. This may, for example, happen when two nodes collaborate on an attack, one recording traffic in its proximity and tunneling it to the other node, which replays the traffic. We have an incorrect messages generation by relay. This attack is often called wormhole attack. In a protocol where links are discovered by testing reception, this will result in extraneous link creation (basically, a link between the two "attacking" nodes), see figure 5. This may also break the MPR flooding because of the rule which mandates that a TC message already received from a node which is not an MPR must not be relayed. In figure 6, node B will not relay the TC message from node F since intruder X has artificially relayed this TC message to B.

Nodes in a MANET relay two types of traffic : routing protocol control traffic and data traffic. A node may misbehave through failing to forward either type of traffic correctly.

If TC messages (or routing protocol control messages in general) are not properly relayed, connectivity loss may result. In networks where no redundancy exists (e.g. in a "strip" network), connectivity loss will surely result, while other topologies may provide redundant connectivity. Similarly if a node does not forward data packets (e.g. if intra-node forwarding is impaired), loss of connectivity may result. Even a node correctly generating, processing and forwarding control traffic as required, may act in a malicious way through not forwar-

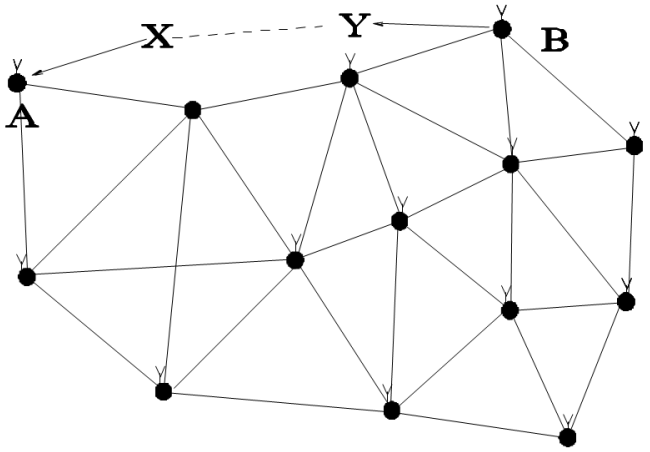


FIGURE 5: Intruders X and Y are creating an artificial connectivity between nodes A and B

ding data traffic. The node thereby breaks connectivity in the network (data traffic cannot get through) however this connectivity loss is not detected by the routing protocol (control traffic is correctly relayed).

3.2 Secured OLSR

To prevent malicious nodes from injecting incorrect information into the network or to incorrectly relay packets, a signature is generated by the originator of each OLSR control message and transmitted with the control message. Public-key as well as symmetric shared-secret key systems can be employed. We will call a cryptographic capable node, a node which has received valid keys [4] and which can sign and verify messages. In addition, a time-stamp is associated with each signature, in order to estimate the message freshness. Upon receiving the control message, a node can determine if the message originates from a cryptographic capable node, and if the message integrity is preserved. The time-stamp allows verifying if the packet is fresh and is not a replay. This security first proposed in [Adjih 2003b] actually relies on two functions a signing function and a time-stamping function.

In the figure 7, it is shown how to build a secured control message. Your first find the usual control message and then there is a security information part which contains the

4. For instance from a certification entity

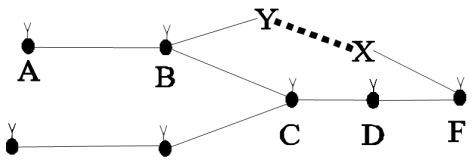


FIGURE 6: Intruders X and Y are creating an artificial connectivity between nodes F and B, this breaks the MPR flooding in B

signature and the timestamp of the control message. The control message and its security information are sent in a same packet. Signature in the security information field of the control message is used by a receiving node to authenticate the corresponding OLSR control message : every control message without a matching corresponding signature is rejected. Depending on the properties of the signature method, different levels of authentication and resilience to attacks can be provided, see [6]. For instance, the highest level of authentication can be provided by using individual asymmetric keys, as the messages advertised as generated from every non-compromised node are uniquely accepted when they indeed originate from this node. Weaker (but less complex or less computationally intensive) systems can be imagined, e.g. employing a shared secret-key system among cryptographic capable nodes.

Notice, that for the computation of the signature, the TTL and Hop-Count fields of the TC or HELLO message are considered as set to 0 (zero) since these fields are modified while the message is in transit and, thus, would otherwise interfere with verification of the message by the receiving node.

There are many ways to generate time-stamps. The easiest way is to use a physical clock. The drawback of this approach is that it requires a precise clock or a synchronization algorithm. Another way is to use logical time-stamps. In such a case, an exchange protocol is required. A precise description of these mechanisms are beyond the scope of this paper and further information can be found in [Adjih 2005b] and [Adjih 2006].

It can be shown that the secure architecture proposed above with a signing and a time-stamping mechanism allows countering most of the attacks when the attacker nodes are not cryptographic capable nodes. Actually this security architecture allows preventing that such attacker nodes be part of the network. When attacker nodes are cryptographic capable

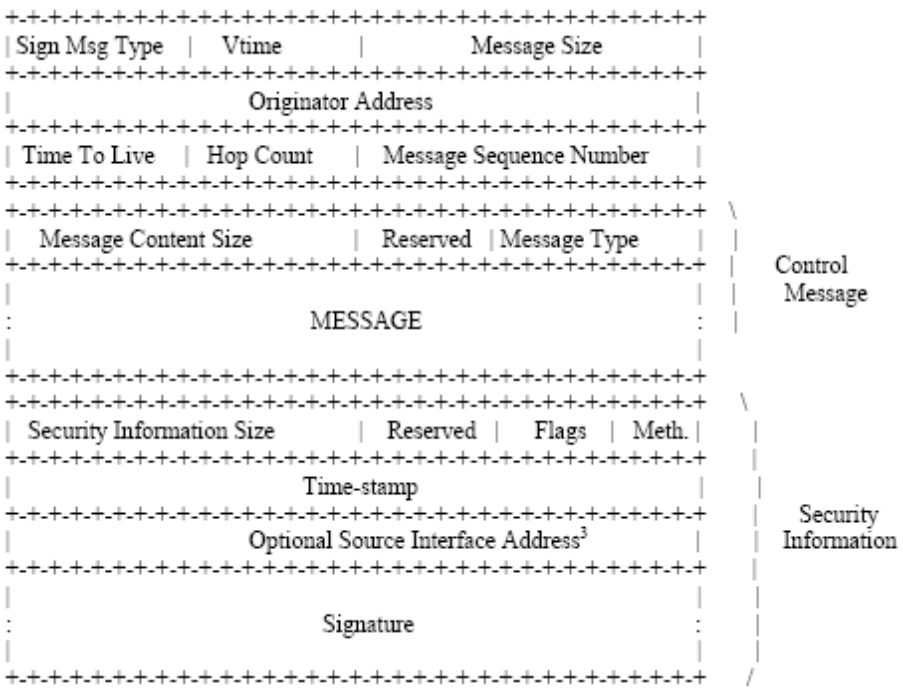


FIGURE 7: A secured OLSR control message

nodes, we say that we have compromised nodes in the network. More advanced techniques are then required to counter attacks with compromised nodes, a few of them are described in [Adjih 2005b], [Raffo 2004] and [Raffo 2005].

4 Conclusion

Mobile ad hoc networks exhibit qualities required by military applications. Protocols operating over MANETs should preserve these qualities. Among them, the routing protocol is of prime importance to allow communication between any two nodes in the network. The OLSR routing protocol inherits the robustness of the OSPF protocol, the most widely used IGP protocol. However, potential attacks against OLSR can endanger the network integrity. After having established a classification of these attacks, we have presented a solution to secure OLSR. This solution, implemented on a real platform, contributes to the survivability of MANETs.

References

[Adjih 2003a] Adjih C., Clausen T., Jacquet P., Laouiti A., Minet P., Muhlethaler P., Qayyum A. and Viennot L., Optimized Link State Routing Protocol, IETF, RFC 3626, October 2003.

[Adjih 2003b] Adjih C., Clausen T., Jacquet P., Laouiti A., Muhlethaler P. and Raffo D., Securing the OLSR Protocol, Proceedings of the 2nd IFIP Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2003), Mahdia, Tunisia, June 2003.

[Adjih 2005a] Adjih C., Minet P., Plesse T., Laouiti A., Muhlethaler P., Jacquet P., Lecomte J., Experiments with OLSR routing in a MANET, Information Systems Technology NATO Symposium, Rome, Italy, April 2005.

[Adjih 2005b] Adjih C., Clausen T., Jacquet P., Laouiti A., Muhlethaler P. and Raffo D., OLSR security, theoretical study deliverable 1 for CELAR also published as : Securing the OLSR Routing Protocol With or Without Compromised Nodes in the Network, INRIA RR-5494, February 2005.

[Adjih 2005c] Adjih C., Muhlethaler P. and Raffo D., Attacks Against OLSR : Distributed Key Management for Security, 2nd OLSR Interop / Workshop, Palaiseau, France, July 2005.

[Adjih 2006] Adjih C., Laouiti A., Muhlethaler P. and Raffo D., OLSR security, detailed implementation deliverable 2 for CELAR. Also to be published as INRIA Research Report, 2006.

[Nguyen 2006] Nguyen D. Q., Minet P., QoS support and OLSR routing in a mobile ad hoc network, ICN'2006, Mauritius, April 2006.

[Perkins 2003] Perkins C., Belding-Royer E., Das S., Ad hoc on Demand Distance Vector (AODV) Routing, IETF, RFC 3561, July 2003.

[Qayyum 2002] Qayyum A., Laouiti A. and Viennot L., 2002, HICSS : Hawai Intern. Conf. on System sciences, Hawai, USA, January 2002.

[Raffo 2004] Raffo D., Adjih C., Clausen T., Muhlethaler P., An Advanced Signature System for OLSR, Proceedings of the 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04), October 2004.

[Raffo 2005] Raffo D., Adjih C., Clausen T., Muhlethaler P., Securing OLSR Using Node Locations, Proceedings of 2005 European Wireless (EW 2005)", pp 437–443", Nicosia, Cyprus, April 2005.

A secure approach for tactical MANETS

Jérôme Lebegue[1], Christophe Bidan[1], Thierry Plesse[2]

[1] SUPELEC, RENNES Avenue de la Boulaie F-35511 Cesson-Sévigné, FRANCE E-mail : jerome.lebegue,christophe.bidan@supelec.fr
[2] CELAR BP 7419 F-35174 Bruz cedex, FRANCE E-mail : thierry.plesse@dga.defense.gouv.fr

1 Introduction

In battlefield or emergency situations the engaged forces are generally divided in *units* or *predefined groups*, each unit having to accomplish one (or more) specific task(s). Each unit has to be functionally autonomous and as much as possible does not rely on other units to accomplish its task. In particular, a given unit cannot require the presence of other unit ; otherwise its absence should be a drastic disadvantage for the unit task. Moreover battlefield and emergency are also situations where the need to deploy network quickly and without existing architecture is important. In these situations communication is vital and we cannot rely on existing infrastructure (because there is none or the infrastructure is no longer operational). MANETs (*Mobile Ad hoc NETworks*) are perfect candidates for these situations. Indeed they are built as wireless, self-organizing networks allowing interconnection of mobile nodes by the mean of specific routing protocols.

In this paper we discuss the impact of predefined groups in tactical MANETs. Then we show how, by taking advantage of the existence of such predefined groups, we can achieve a better intra-unit communication as well as provide a more robust inter-unit routing. Finally, we address the security issues of the tactical MANETs.

2 Impact of predefined groups in MANETS

The organization in units has significant consequences for the use of MANETs. First of all, this implies that each node of the MANET belongs to a specific predefined group (defined by its owner unit). Moreover, since each unit has to be functionally autonomous, the nodes of the same predefined group have as much as possible to rely on themselves to ensure their ability to communicate. Thus, the nodes of the same predefined group have (at least ideally) to build their own MANET, independently of other nodes within radio range that do not belong to their predefined group. However, since the members of a given unit may be physically scattered on the field (for any reasons), some of the nodes of the predefined group may be without radio range, and it may be impossible to build a specific MANET for that predefined group. Nevertheless, it is very important that the members of a scattered unit are able to communicate so as to eventually adapt the unit task to this situation. So, the nodes of such members have to rely on nodes that do not belong to the

same predefined group to communicate. To summarize, the two following properties have to be ensured :

- As much as possible, the nodes of a same predefined group have to rely on themselves to ensure their ability to communicate ; and
- When the nodes of a given predefined group are scattered, the ad hoc routing protocol has to automatically and transparently maintain their ability to communicate.

Notice that, since the nodes of a predefined group collaborate to accomplish the same specific task, we can assume that they are likely moving together. Thus, we consider the situation where the members of a predefined group are scattered on the field as an exception.

3 How MANETS can benefit from predefined groups

Our objective is to enhance the routing protocol to take advantage of the predefined groups. Our approach is based on the notions of *compact group* and *scattered group* (see 1). Considering a node X, its compact group is the set of nodes that belong to its predefined group and with which it can build an autonomous sub-MANET. So, a predefined group is defined as a unique compact group when it is not scattered (let us recall that this is the usual form of a predefined group), and as a set of compact groups otherwise. This notion of compact groups directly results from the first property defined in the previous section. Indeed, the nodes of a compact group belong to the same predefined group and only rely on themselves to communicate. The *scattered group* of the node X is a table that allows to retrieve, for each scattered node, its compact group it belongs to. Notice that if the nodes X and Y belong to the same compact group, they have the same scattered group.

Consequently, these notions allow us to define the entire MANET as a *meta-MANET* in which (meta-)nodes are *compact groups*. In order to ensure the consistency of the (meta-) node information, we consider in the following that the nodes of the same compact group share/exchange their information related to the meta-MANET. Before showing how intra-unit communication and inter-unit routing benefit from this meta-view, we explain how we automatically and transparently maintain the ability of scattered nodes to communicate.

3.1 Communication between scattered nodes

Any node having a neighbor node that does not belong to its predefined group can act as a gateway for its compact group. Considering the meta-MANET, such nodes define meta-interfaces of the meta-node they belong to. Thus, using an ad hoc routing protocol at the meta-MANET level allows maintaining a routing table, called the *scattering table*, that specifies the route to reach any distant meta-node.

By definition, scattered nodes belong to distinct meta-nodes. Using the scattering table, meta-nodes of the same predefined group can then exchange their meta-information, and especially the information related to their membership. As we consider that nodes of the same compact group exchange their meta-node information, each node can automatically

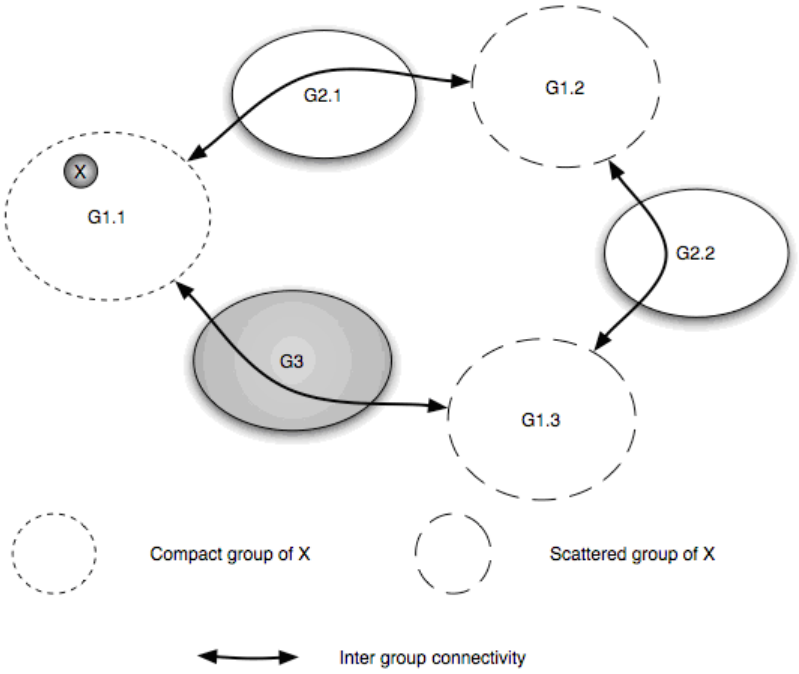


FIGURE 1: Compact and scattered groups of the node X.

and transparently update its scattered group, and maintain its scattering table. Each node is then able to communicate with any scattered node of its predefined group.

Notice that a meta-node can have different meta-interfaces. Thus, the scattering table has to deal with the following possibilities :

- A given meta-interface have multiple routes to reach the same distant meta-node (see 2) ;
- Multiple meta-interfaces can be used to reach the same distant meta-node (see 3) ;

By construction, the ad hoc routing protocol allows to deal with the first case. The latter case will allow us to enhance the inter-unit routing as we show later.

3.2 Benefits to intra-unit communication

By definition, the nodes of a compact group belong to the same predefined group and form an autonomous sub-MANET. The benefits from this are :

- The compact group is built with only *trusted* nodes (members of the same unit are very likely to act for the sake of the unit),
- The nodes of the compact group have only to take into account the topology changes that impact the compact group itself. Since the nodes of the compact group likely

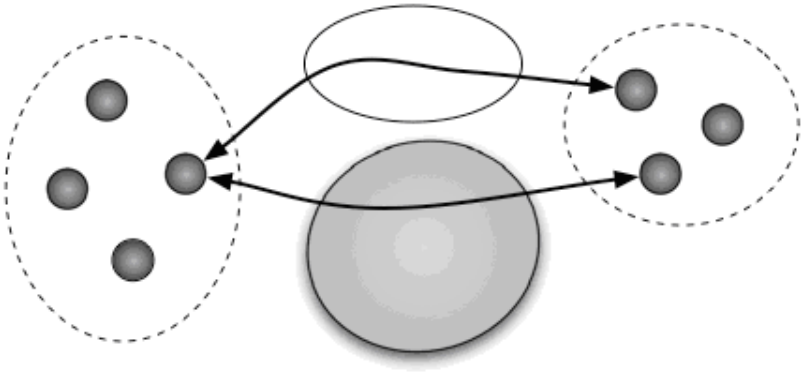


FIGURE 2: Meta-interface with multiple route.

move together, these topology changes are limited. So we have a more stable sub-MANET with respect to the routing protocol.
– Since the compact group only considers a subset of nodes of the entire MANET, the routing packets as well as the routing tables are smaller than the ones we will obtain considering the entire MANET.

These benefits are not completely lost when the predefined group is scattered on the field. Indeed each compact group of the predefined group has these benefits. But they also have to rely on neighbor compact groups to maintain the ability to communicate. At this point the meta-network view brings significant advantages, mainly in term of robustness to mobility.

3.3 Benefits to inter-group routing

By using the meta-network view when routing between compact groups we do not have to know the routing done inside the compact groups. Indeed, each node maintains its scattering table that corresponds to its vision of the meta-network in which it evolves. This scattering table specifies the next hop (i.e., the next compact group) to reach the distant compact group.

The meta-network view brings significant advantages :
– We do not have to care about the way nodes communicate in their compact group ;
– We do not have to care about inside group mobility ; and
– Group mobility is likely to be slower than node mobility and so meta-network topology changes do not occur as often.

With this scattering table, a node does not have to know the specific route through other compact groups. It does not even need to know the next hop in term of node, because it can use any suitable nodes (i.e., any node defining a meta-interface) that belong to the

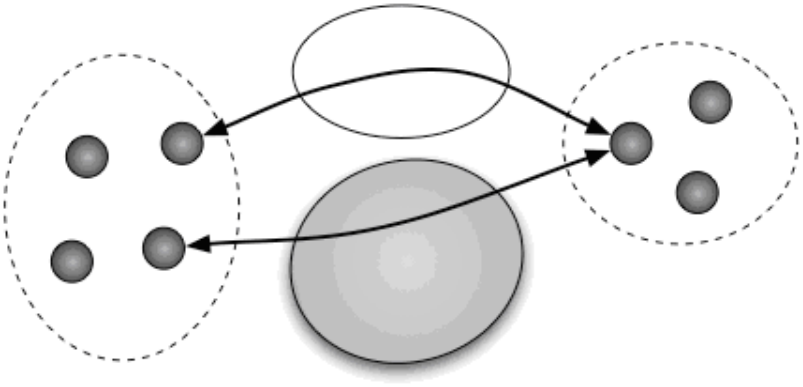


FIGURE 3: Multiple interface for the same meta-node.

next hop compact group. This guarantees that as long as the considered compact group has connectivity with the next hop compact group, messages will be routed.

4 Security issues

From the security point of view, the logical and organizational views that allow grouping the nodes define a *trust* relation between the nodes. Indeed, we can reasonably assume that a node trusts the nodes that belong to its predefined group. Conversely, trust relationship between nodes that do not belong to the same predefined group cannot be supposed.

Given this trust relation between nodes of the same predefined group, we can reformulate the previous requirements :

- As much as possible, the nodes with trust relationship have to rely on trusted nodes to communicate.
- When the nodes with trust relationship are scattered, they can try to maintain their ability to communicate thanks to nodes of *unknown trust*.

We discuss the security issues with respect to these requirements.

4.1 Security of the routing services

The previous requirements imply that nodes with trust relationship have to support the deployment of an autonomous and *secure* sub-MANET, and only rely on nodes of *unknown trust* to communicate with distant trusted nodes.

Basically, a secure MANET allows securing the routing protocol so as to protect against attackers that try to gain privileges by usurping the identity of other nodes. Thus, in a secure MANET, if we know a route between the nodes A and B, we are confident about

the intermediate nodes. On the other hand, we do not have the assurance that if A send a message to B, B will receive it, or even that if such a route exists, it will be discovered.

In a secure MANET of nodes with trust relationship, we can reasonably assume that the nodes will act properly with each others. Consequently, we can consider that all the routes are discovered and that any sent messages will be received. In other word, by deploying a secure MANET, nodes with trust relationship can communicate through trusted routes.

Conversely, according to the second requirements, scattered nodes with trust relationship have to rely on *uncertain nodes* to communicate. Consequently, we cannot assume anything about the routing protocol. Especially, we can not suppose that the routing protocol will allow to discover the routes between scattered nodes with trust relationship, and even if we have such a route, we cannot be confident about the intermediate nodes and so the message routing.

4.2 Security of the exchanges

Although we cannot be confident about the intermediate nodes, we have to ensure the security of the received messages, that is : if a node A receives a message from a node B it trusts, this message is confidential, fresh and authenticated. So we have to use cryptographic mechanisms that allow authenticating both the sender and the sending information, as well as ensuring the confidentiality and the freshness of the message.

Basically, the methods to achieve these goals are well known, and are based on integrating timestamp and computing MAC (*Message Authentication Code*). Notice that, in the context of the tactical MANETs, we can reasonably suppose the existence of an offline authority in charge of providing the cryptographic material (i.e., either the secret key or the public key certificate) to each node.

Nevertheless, in the tactical MANETs, the problem of captured nodes is crucial. More specifically, we have to provide a mechanism that allows to detect the captured / corrupted nodes, as well as to prevent the captured / corrupted node to access the future confidential exchanges. Basically, the detection of corrupted nodes consists in monitoring node misbehaviour using a watchdog mechanism and possibly a reputation system. To prevent the captured nodes to access the future confidential exchanges, the approach can be to use a group key agreement protocol that ensures the forward secrecy that is the old group key material does not allow computing the new group key material.

5 Conclusion

In this paper we briefly discuss the impact of the existence of predefined groups in tactical MANETs, in terms of both routing and security services. The interested readers can find more information on these issues in the referenced papers.

Bibliography

[1] Jérôme Lebègue, Christophe Bidan and Thierry Plesse. Security of predefined groups in MANETs, In proceedings of the 3-rd ACM International Workshop on QoS and Security for Wireless and Mobile Networks (Q2SWinet 2007), pp 164-167. Octobre 2007.

[2] Jérôme Lebègue, Christophe Bidan and Thierry Plesse. Taking advantage of predefined groups in tactical MANETs. In proceedings of the Military Communications and Information Systems Conference (CDROM). Septembre 2007.

[3] Jérôme Lebègue, Christophe Bidan and Thierry Plesse. An OLSR extension to deal with predefined groups. In proceedings of IST Mobile & Wireless Communications Summit (CDROM). Juillet 2007.

Quand la technologie se mêle de droit et vice versa

Daniel Le Métayer

INRIA Grenoble
daniel.lemetayer@inria.fr

L'interpénétration croissante des aspects juridiques et informatiques pose des questions complexes qui ne peuvent être abordées sérieusement qu'à travers une démarche de recherche véritablement pluridisciplinaire. L'objectif de l'action exploratoire LICIT lancée par l'INRIA en 2008 est de répondre à ce besoin en contribuant, en partenariat avec des chercheurs en droit, au développement de méthodes permettant une meilleure intégration des instruments informatiques et juridiques. Dans cette présentation, nous illustrons la démarche adoptée par LICIT à travers les questions des responsabilités juridiques et de la protection de la vie privée.

Biographie

Daniel Le Métayer est directeur de recherche au centre de recherche INRIA Grenoble - Rhône-Alpes et responsable de l'action exploratoire LICIT. Après six années passées dans la société Trusted Logic, spécialisée en sécurité des systèmes embarqués, il a rejoint en 2006 l'INRIA Grenoble Rhône-Alpes pour y lancer de nouvelles activités sur les interactions entre droit et nouvelles technologies.

Sécurité dans les systèmes RFID

Gildas Avoine

UCL Louvain-la-Neuve, Belgique
Information Security Group
http ://sites.uclouvain.be/security/

Résumé Il est aujourd'hui difficile de parler d'identification par radiofréquence (RFID) sans que ne viennent à l'esprit les termes de « sécurité de l'information » et de « protection des données personnelles ». Nous présentons ici les grandes familles de menaces auxquelles doit faire face la RFID, ainsi que leur impact dans notre vie de tous les jours.

1 L'évolution de la technologie RFID

Contrairement à ce que l'on pourrait croire, l'identification par radiofréquence (RFID) n'est pas une révolution technologique du vingt-et-unième siècle, mais de la première moitié du vingtième. Elle a cependant beaucoup évolué depuis lors et celle qui nous entoure aujourd'hui n'a plus grand-chose à voir avec la RFID de nos aïeux. Bien sûr, les principes physiques sur lesquels elle repose restent les mêmes, mais les progrès réalisés en électronique ont radicalement changé la donne : le prix d'un tag peut atteindre une quinzaine de centimes d'euros et sa taille est parfois inférieure à un grain de riz. Ces valeurs extrêmes ne doivent cependant pas cacher la réalité, car à chaque application correspond un tag qui lui est adapté : il est inutile d'utiliser un tag minuscule (et donc coûteux) pour une application qui ne le nécessite pas, et il est impossible d'utiliser un tag à 15 centimes d'euros pour une application qui requiert de la sécurité. Il existe donc une large gamme de tags avec des caractéristiques très variées, allant de la simple mémoire sans capacité de calcul, à la carte à puce sans contact capable d'utiliser de la cryptographie à clef publique.

Les tags RFID les plus courants sont « passifs », c'est-à-dire qu'ils ne possèdent pas de source d'énergie embarquée : ils obtiennent leur énergie à partir du champ électromagnétique émis par le lecteur. Cela signifie que les tags doivent être présents dans le champ du lecteur pour communiquer et éventuellement effectuer des calculs. Ils répondent donc à la sollicitation d'un lecteur mais n'initient pas eux-mêmes de communication. Ils ont une distance de communication pouvant aller de quelques centimètres à quelques mètres selon la technologie utilisée, c'est-à-dire substantiellement plus faible que les tags avec batterie, dits « actifs ». Ce sont ces tags passifs qui sont aujourd'hui sur le devant de la scène et il est même devenu usuel d'utiliser simplement le terme « RFID » pour désigner la RFID passive et de dire explicitement « RFID active » dans le cas contraire.

Les tags passifs les moins chers ne sont dotés que d'une mémoire contenant un identifiant unique. La communication entre le lecteur et le tag est alors très simple : sur sollicitation

du lecteur, le tag envoie son identifiant, comme le ferait tout simplement une personne à qui l'on demanderait son nom. La communication peut parfois bénéficier de mécanismes légèrement plus évolués : certains tags ne fourniront leur identifiant que si le lecteur envoie un mot de passe correct, convenu à l'avance, lors de la fabrication ou de l'initialisation du tag. Le déploiement des tags à très bas coût a été renforcé et même catapulté par la création d'un consortium aux États-Unis en 1999, l'Auto-ID Center [10], qui a pour but de standardiser et de promouvoir l'utilisation de la RFID dans les chaînes logistiques, en particulier dans la grande distribution.

Un autre exemple de tag, cette fois plus coûteux, est un tag qui possède des capacités de calcul importante, capable d'effectuer des opérations cryptographiques, qui permettent de sécuriser le système RFID considéré notamment en chiffrant la communication entre le lecteur et le tag. Ces tags possèdent également une mémoire pour stocker des données, généralement un ou deux kilo-octets, mais des valeurs bien supérieures peuvent être atteintes, comme c'est le cas avec les passeports biométriques. Ces derniers peuvent contenir plusieurs dizaines de kilo-octets de données. Un tag de ce type possède une distance de communication de l'ordre de quelques centimètres (ISO 14443) ou décimètres (ISO 15693).

2 Usurpation d'identité

S'il existe plusieurs types de tags, c'est bien parce qu'il existe aussi plusieurs types d'applications. Il faut principalement distinguer celles dont l'objectif est *l'identification* d'objets ou de sujets (remplacement des codes-barres, tatouage du bétail, etc.) de celles dont l'objectif est *l'authentification* de ces mêmes objets ou sujets (badge d'accès à un immeuble, clef de démarrage d'une voiture, abonnement aux transports publics, etc.).

L'identification n'a pas pour but de prouver l'identité d'une personne ou d'un objet, mais seulement d'annoncer une identité. Quiconque écoute la communication entre un lecteur et un tag est donc en mesure « d'entendre » cette identité mais il ne s'agit pas là d'un vol. En revanche, un protocole d'authentification doit assurer au lecteur qu'il communique réellement avec la personne ou l'objet prétendu.

Alors qu'il est possible de concevoir des protocoles d'authentification qui soient sûrs, il n'est pas rare de voir en pratique des attaques sur des systèmes d'authentification reposant sur la RFID, en particulier des systèmes de contrôle d'accès. Plusieurs raisons expliquent cela. Tout d'abord, de nombreuses firmes proposent des systèmes d'authentificaton qui cachent en fait seulement un protocole d'identification. Ensuite, les contraintes de la RFID, en particulier en termes de calcul, incite à utiliser des algorithmes cryptographiques « allégés » en termes de calcul, mais aussi malheureusement « allégés » en termes de sécurité. Deux exemples très médiatisés sont le module DST de Texas Instrument cassé en 2005 [1] et la puce NXP Mifare Classic vendue à plusieurs centaines de millions d'exemplaires – et toujours en vente – est totalement cassée depuis 2008 [5,6,13,4,7,3].

Notons enfin qu'une attaque générique à prendre très au sérieux permet également de déjouer n'importe quel protocole d'authentification existant, aussi solide soit-il. Cette

attaque, dite *par relais*, exploite le fait que les tags acceptent de répondre sans l'accord préalable de leur porteur. Elle implique deux complices reliés par un canal de communication suffisamment rapide (une communication radio par exemple) pour la transmission des données. L'un des complices est situé à proximité d'un lecteur RFID légitime – par exemple un distributeur de tickets de cinémas – alors que le second est situé à côté du tag RFID victime – par exemple un client qui attend patiemment son tour dans la file pour acheter un ticket. Cette technique permet en quelque sorte de créer une rallonge entre la victime et le distributeur : les deux attaquants relaient simplement les messages entre les deux parties, laissant croire à la victime qu'elle communique directement avec un distributeur légitime et vice-versa. Hancke [8] a réalisé un système d'attaque performant, en utilisant une communication radio entre les deux attaquants. Son système parvient à relayer le signal sur une distance de 50 mètres. Le coût du matériel ne dépasse cependant pas une centaine d'euros. Des expériences similaires ont été réalisées par Kasper, Carluccio et Paar [2] d'une part, et par Kfir et Wool [9] d'autre part. Se protéger des attaques par relais n'est pas une chose aisée car l'utilisation de la cryptographie seule ne permet pas de contrer ce type d'attaque de très bas niveau.

3 Fuite d'information

Alors que l'usurpation d'identité ne concerne que les tags qui ont pour objectif de réaliser de l'authentification, le problème de la fuite d'information concerne potentiellement tous les tags. Il se pose dès lors que les données envoyées par le tag révèlent de l'information sur l'objet ou la personne qui le porte.

Par exemple, un document d'identité ou une carte de paiement peut révéler des informations confidentielles. Une carte de transport public peut révéler les dates et lieux des derniers passages de son porteur. Plus préoccupant, les produits pharmaceutiques marqués électroniquement, comme préconisé par le Food & Drug Administration aux États-Unis, pourraient indirectement révéler les pathologies d'une personne, etc. Mais la fuite d'information n'est pas seulement le vol d'informations personnelles. Un problème rarement évoqué est l'espionnage industriel. Celui-ci peut prendre différentes formes. Au lieu de soulever la bâche d'un camion de la société concurrente, il est aujourd'hui plus facile de découvrir leur contenu en les scannant lorsqu'ils sortent de l'entrepôt ou lorsqu'ils sont stationnés sur les aires de repos. Nombre de cartons, palettes et containers sont en effet déjà marqués aujourd'hui avec des tags RFID.

La limite entre les attaques théoriques et les attaques pratiques est difficile à fixer car elle dépend principalement de la motivation de l'attaquant à réaliser son méfait. Prenons l'exemple d'une carte de transport public qui divulgue à qui le lui demande le nom de son porteur, ainsi que les trois derniers trajets de celui-ci. La probabilité que Monsieur Dupont, employé communale de Joinville-le-Pont, soit scanné à distance dans la rue par

un attaquant qui souhaite connaître son nom à des fins malicieuses est faible [1]. Le réel risque pour Monsieur Dupont vient plutôt de Madame Dupont elle-même. En effet, Madame Dupont n'a bien sûr aucun intérêt à lire l'identité de son mari sur la carte de transport, mais elle peut chercher à savoir si Monsieur Dupont est bien rentré directement de son travail sans faire un détour inexpliqué et inexplicable. La carte de Monsieur Dupont apportera cette réponse, que Monsieur Dupont ou non soit d'accord. Plutôt qu'il s'agisse de Madame Dupont, il peut s'agir de Monsieur Chef, supérieur hiérarchique de Monsieur Dupont, qui souhaite s'assurer que son subalterne dit la vérité lorsqu'il affirme qu'il est arrivé en retard en raison d'un problème sur la ligne 4 du métro.

4 Traçabilité malveillante

Le problème de la traçabilité malveillante est plus délicat à traiter. Quelle que soit l'information envoyée par le tag, elle peut potentiellement être utilisée pour le tracer dans l'espace ou dans le temps.

Pour ne pas permettre la traçabilité malveillante, le tag doit n'envoyer aux lecteurs que des réponses qui « semblent » être aléatoires sauf pour le lecteur autorisé. Cette technique n'est presque jamais employée car elle présente plusieurs inconvénients majeurs : (1) le tag doit avoir les capacités suffisantes pour utiliser de la cryptographie ; (2) pour pouvoir lire efficacement les données reçues, le lecteur doit connaître l'identité du tag (pour savoir quel secret utiliser), mais pour connaître l'identité du tag, il doit savoir lire les données reçues ; (3) pour pouvoir communiquer, le système RFID utilise un protocole d'évitement de collisions qui repose souvent sur le fait que chaque tag possède un identifiant d'évitement de collisions unique et fixe (UID) ; en conséquence, même si le protocole d'identification ou d'authentification évite la traçabilité malveillante, le protocole d'évitement de collisions peut permettre la traçabilité du tag et donc de son porteur. Le seul exemple que nous connaissons où le problème de la traçabilité malveillante est pris en compte de manière sécurisée est le passeport biométrique. En effet, dans le cas du passeport, le tag ne délivre des informations intelligibles qu'à partir du moment où le lecteur s'est correctement authentifié. En outre, l'identifiant d'évitement de collisions n'est pas fixe : il est généré aléatoirement chaque fois que le tag est sollicité par un lecteur.

5 Déni de service

Enfin, le piratage peut ne pas concerner un tag donné, mais un système donné en cherchant à déstabiliser son infrastructure. Cela peut être fait de manière inintéressée, au même titre qu'un pirate informatique défait un site web ou qu'un délinquant dessine des

1. Notons toutefois qu'un jour de manifestation où Monsieur Dupont brise des vitrines, les forces de l'ordre pourraient s'infiltrer dans la foule et scanner les identités des délinquants sans prendre le risque d'intervenir physiquement.

graffitis sur les murs, ou cela peut être le fruit d'un travail élaboré et prémédité. Ce dernier cas est tout à fait envisageable dans une situation de concurrence entre deux sociétés. Il pourrait être tentant de déstabiliser son concurrent en anéantissant le système RFID qui contrôle sa chaîne de production.

Les techniques qui permettent de faire cela sont diverses et variées et dépendent fortement de la technologie RFID utilisée. Cela peut aller du brouillage électromagnétique qui empêche la lecture des tags à leur destruction en utilisant des dispositifs extrêmement peu coûteux [11], en passant par l'exploitation de failles dans les lecteurs ou la diffusion de virus [12]. Alors que cette dernière menace semble peu réaliste à l'heure actuelle, l'exploitation de failles dans les lecteurs pour déstabiliser un système est quant à elle tout à fait réelle. Par exemple, une étude menée en 2006 sur la compatibilité des systèmes de vérification de passeports avec le document 9303 publié par l'Organisation de l'Aviation Civile Internationale, montre que les implémentations de ce standard souffrent généralement de nombreux problèmes, allant parfois jusqu'à la non-vérification des mesures de sécurité embarquées sur les passeports.

L'étude des dénis de service dans les systèmes RFID n'en est qu'à ses premiers balbutiements. Ce domaine profite d'une longue histoire et expérience dans le domaine plus général de l'informatique qui pourront être utilisées, à bon ou mauvais escient, dans le domaine plus restreint de la RFID.

6 Conclusion

Cette succincte présentation de la sécurité de la RFID a pour but de présenter et de clarifier les menaces qui pèsent aujourd'hui sur cette technologie. Sans aborder les aspects purement techniques, elle permet de distinguer ce qui est réalisable de ce qui ne l'est pas. Usurpation d'identité, fuite d'informations, traçabilité malveillante et déni de service sont autant de menaces qu'il faut considérer sérieusement. Certaines d'entre elles trouvent incontestablement leur parade dans l'usage de la cryptographie. D'autres sont plus délicates à traiter. Mais il est un point important qu'il faut garder à l'esprit : les techniques mises en œuvre pour sécuriser la RFID repose sur le postulat que les attaques proviendront d'un pirate extérieur au système. Une menace majeure, pourtant, concerne l'utilisation abusive voire frauduleuse des données par les personnes mêmes qui les recueillent licitement.

Références

1. Steve Bono, Matthew Green, Adam Stubblefield, Ari Juels, Avi Rubin, and Michael Szydlo. Security Analysis of a Cryptographically-Enabled RFID Device. In *USENIX Security Symposium*, pages 1–16, Baltimore, Maryland, USA, July-August 2005. USENIX.
2. Dario Carluccio, Timo Kasper, and Christof Paar. Implementation Details of a Multi Purpose ISO 14443 RFID-Tool. In *Workshop on RFID Security – RFIDSec'06*, Graz, Austria, July 2006. Ecrypt.

3. Nicolas T. Courtois. The Dark Side of Security by Obscurity and Cloning MiFare Classic Rail and Building Passes, Anywhere, Anytime. In *Workshop on RFID Security – RFIDSec'09*, Leuven, Belgium, July 2009.
4. Gerhard de Koning Gans. Analysis of the Mifare Classic used in the OV-Chipkaart Project, 2008.
5. Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia. A Practical Attack on the MIFARE Classic. In *Proceding of the 8th Smart Card Research and Advanced Applications – CARDIS 2008*, Lecture Notes in Computer Science, Royal Holloway University of London, UK, September 2008. Springer.
6. Flavio D. Garcia, Gerhard de Koning Gans, Ruben Muijrers, Peter van Rossum, Roel Verdult, and Ronny Wichers Schreur. Dismantling MIFARE Classic. In *Proceding of the 13th European Symposium on Research in Computer Security – ESORICS 2008*, volume 5283 of *Lecture Notes in Computer Science*, pages 97–114, Malaga, Spain, October 2008. Springer.
7. Flavio D. Garcia, Peter van Rossum, Roel Verdult, and Ronny Wichers Schreur. Wirelessly Pickpocketing a Mifare Classic Card. In *IEEE Symposium on Security and Privacy — S&P '09*, Oakland, California, USA, May 2009. IEEE.
8. Gerhard Hancke. Practical Attacks on Proximity Identification Systems (Short Paper). In *IEEE Symposium on Security and Privacy*, Oakland, California, USA, May 2006. IEEE, IEEE Computer Society Press.
9. Ziv Kfir and Avishai Wool. Picking Virtual Pockets Using Relay Attacks on Contactless Smartcard Systems. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005*, Athens, Greece, September 2005. IEEE.
10. EPC Global Network. http ://www.epcglobalinc.org/.
11. RFID Zapper. https ://events.ccc.de/congress/2005/static/r/f/i/RFID-Zapper(EN)_77f3.html.
12. Melanie Rieback, Bruno Crispo, and Andrew Tanenbaum. Is Your Cat Infected with a Computer Virus ? In *Pervasive Computing and Communications*, Pisa, Italy, March 2006. IEEE, IEEE Computer Society Press.
13. Wouter Teepe. Making the Best of Mifare Classic, October 2008. `www.sos.cs.ru.nl/applications/rfid/2008-thebest.pdf`.

Eavesdropping and Protocols Security on RFID Devices

François Vacherand, Elisabeth Crochon, François Dehmas, Jacques Reverdy, Olivier Savry and Pierre-Henri Thévenon

CEA-LETI MINATEC, 17 rue des Martyrs F-38054 Grenoble Cedex 9 francois.vacherand@cea.fr

1 Introduction

The purpose of this paper is to have a better understanding of some vulnerabilities of a contactless RF channel in order to improve the design of future RFID systems. In the last decade, there was a tremendous growth of contactless applications. The most relevant and widespread are ticketing, banking and e-passport. Unfortunately, a new emerging technology opens new doors for hacking. This paper focuses on eavesdropping, a potentially important attack, both for security and privacy concerns, which is well known on wireless communication systems.

The main objective is to quantize performances of eavesdropping experiments on contactless smart cards. The goal is twice. First, these experiments must provide good stuff to risk analysis experts who have to evaluate the security of an RFID system. Second it allows R&D security works to concentrate on the most relevant problems and to have a reference tool to validate countermeasures. The targeted issue is to measure the maximum distance of eavesdropping for both forward and return RFID link, and to evaluate the required complexity of equipment to do that. Secondary issues are to detect potential new weaknesses and side effects on the RFID contactless link that can be exploited by an attacker in a malicious way.

To day, most contactless devices are used in Radio Frequency Identification (RFID) applications. These RFID devices can be split into two main families :

1. The electronic tags, to identify items for inventory or supply chain management. Tags are used for objects traceability. RFID identification tags will give priority to operating distance : from a few centimetres to a few meters to the detriment of embedded computing or processing functions. In this case, exchanges will have minimum confidentiality, the data flow between the reader and the tag will be relatively small and the data processing carried out on the tag will be very simple, if any. Remote reading of the tag without awareness of the owner will be particularly easy when tag range is large and processing capabilities minimum.
2. The smart cards, mainly devoted to identification of a subscriber to a service. These smart cards, suitable for the handling of more confidential data, will give priority to

computation and processing in order to perform complex security tasks such as cryptography calculations to authenticate the holder and to protect data, secure storage of sensitive information in non volatile memory, use of more efficient operating system for multi-application management and downloading of new service applications.

2 Eavesdropping

Eavesdropping belongs to one of the main classes of attacks that may be performed on wireless systems but also on contactless links. Eavesdropping is a passive attack and is possible only when a legitimate reader has started a transaction with a legitimate card. Both forward link and return link have to be considered. However, due of the RF power unbalanced contactless system, there is a large discrepancy on these two links, and basically it is much easier to listen to the reader rather to listen to the card or tag.

Because eavesdropping is listening to an on going contactless transaction, spying equipment does not require powering the tag or the card. So it is possible to design a more sensible and improved RF receiver because there is no blurring from the emitted carrier and it is possible to design and to use specific and adapted antennas.

Qualitative risk analysis on malicious scenarios requires estimating some criteria. For eavesdropping contactless scenario, basically such criteria are the reading distance, the complexity of the spying reader, its cost and the difficulty to deploy it on the attack location. Experiments have been undertaken to build basically low cost receiving equipments to simulate hacker's usual equipments : commercially available devices or low cost electronic design. Such equipment enables first to estimate the cost to complexity feasibility ratio, and second to measure the eavesdropping distances for both forward and return links.

2.1 Experimental results

In order to evaluate different configurations of attack, experiments are run onto two typical electromagnetic locations of the HF near field : the first and second Gauss positions that are shown in 1 left. 1 right displays in a symbolic way the relative eavesdropping areas around the targeted system, comparing forward and return links.

The next two figures illustrate the differences between first and second Gauss first Gauss position has a higher signal-to-noise ratio.

The next two experiments show the practical eavesdropping limits of the current device under tests and spying system in the most suitable position. Different lower or upper limits can be achieved according to the reader/card brand and/or the spying receiver design.

Main conclusion for ISO 14 443 proximity cards is that forward link can be easily eavesdropped at more than 20 meters, and return link at more than 4 meters. In the first order, these figures seem to be repetitive what ever the reader/card couple. Of course many parameters have to be taken into account before generalizing to an unknown system located into an unknown electromagnetic environment.

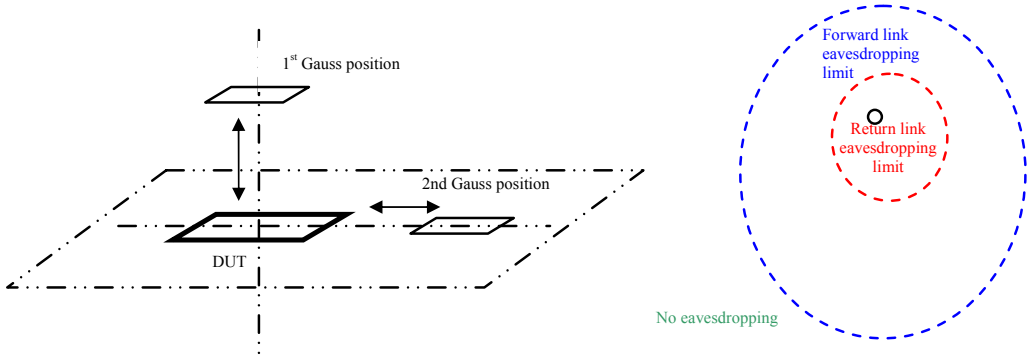


FIGURE 1: Left : First and second Gauss positions for experiments. Right : Forward and return links eavesdropping areas.

3 Side channels and weird attacks

3.1 Eavesdropping on reader power cord and power supply lines

In these scenarios, the hacker is able to register a contactless communication by placing the spying antenna close to the power cord of the reader or near building wirings.

3.2 Indoor EM propagation phenomena and high signal level locations

In some typical indoor applications and set up, it is possible to find very excellent places to receive the contactless signal. It enables very discreet remote eavesdropping.

In the building map just above, the system under eavesdropping is located upper right. When performing measurements, it was noticed that the best place to eavesdrop is located in 1. The electrical wiring of the building is surely the responsible through conduction.

4 Protections against eavesdropping

Many solutions have been proposed to prevent eavesdropping for contactless systems. Some are high end technologies, but others are low cost solutions in order to tackle the low resources constraints of a large majority of contactless systems.

Faraday cage : The well known purpose of the Faraday cage is to stop electromagnetic field. The consequence is that the contactless device which is inside the cage, doesn't receive neither power nor data to be triggered. Faraday cage is used as a very low cost shield solution.

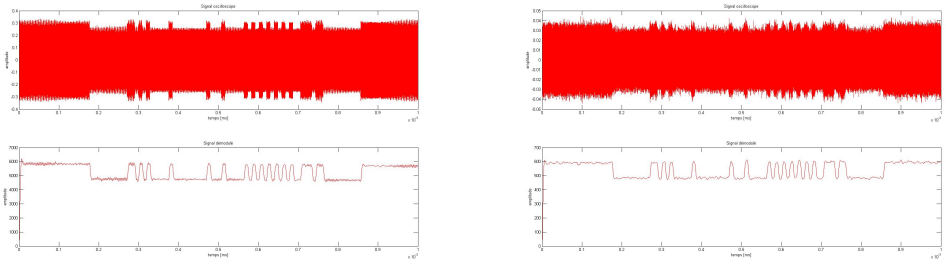


FIGURE 2: Left : ISO 14 443 - Type B - Forward link - First Gauss position - 12 m. Right : ISO 14 443 - Type B - Forward link - Second Gauss position - 12 m.

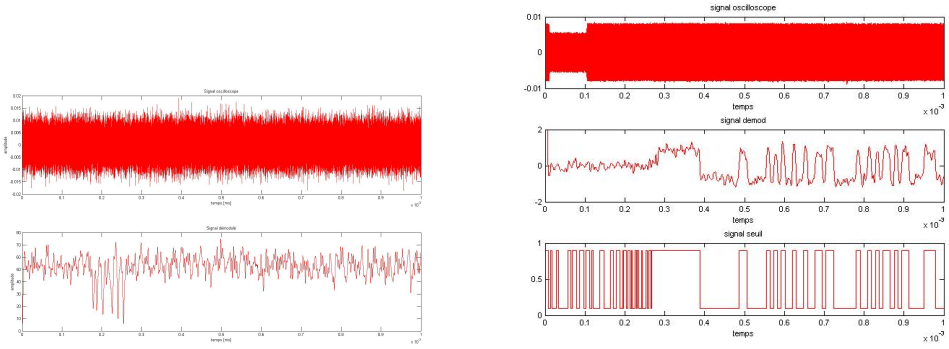


FIGURE 3: Left : ISO 14 443 - Type A - Forward link - First Gauss position - 22 m. Right : ISO 14 443 - Type A - Return link - First Gauss position - 4 m.

Lightweight cryptography : The basic solution to protect confidentiality of data is to cipher them with cryptographic solutions. This technique is well developed and perfectly mastered. The only drawback is that it is resources consuming in power and area on the chip, sometimes with tedious keys management.

Noisy Readers : Possible protections focus on the noisy reader concept, mainly for low resources devices such as tags. Noise is added by the reader to the frequency carrier when the tag is emitting data. This concept protects the return link without modifying the current air interface standards on the tag side.

Low range antennas : Some emerging antennas designs can reduce the range of the RFID systems. This solution does not modify the current devices and so may be attractive to be implemented without current standard modifications.

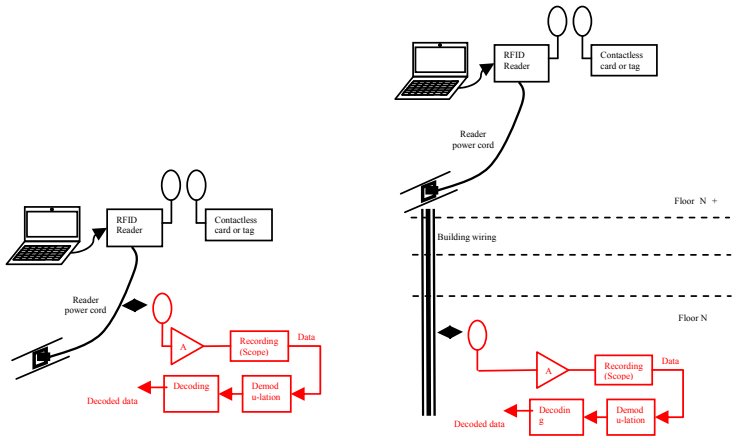


FIGURE 4: Left : Eavesdropping on power cord of the reader. Right : Eavesdropping on building wirings vertically 3 floors away.

5 Conclusions

In this paper we have introduced some experimental results on the possibilities for eavesdropping contactless systems. Anyway, the conclusion is that if systems are correctly designed, there are always some solutions for protection against eavesdropping. The key point is to run risk analysis anytime someone plans to deploy a RFID system and to perform in situ experiments to get credible data to estimate the risk with a sufficient level of confidence. Surveying new attacks is also highly relevant.

References

1. Z. Kfir and A. Wool, Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems, Tel Aviv University, 2004.

2. A. Juels et al., Security and Privacy Issues in e-passport , 2005.

3. G. Ko and P. Karger, Preventing Security and Privacy Attacks on Machine readable Travel Documents, Univ. Columbia and IBM, 2004.

4. B. Schneier, Fatal flaw weakens RFID passports, Wired News 2005.

5. Garfinkel, S. L., Juels A., Pappu R. :RFID Privacy : An Overview of Problems and Proposed Solutions, IEEE Security and Privacy, May/June 2005, pp34-43.

6. C. Castelluccia and G. Avoine. Noisy Tags : A Pretty Good Key Exchange Protocol for RFID Tags. In J. Domingo-Ferrer, J. Posegga, and D. Schreckling, editors, Smart Card Research and Applications, CARDIS 2006. Springer-Verlag.

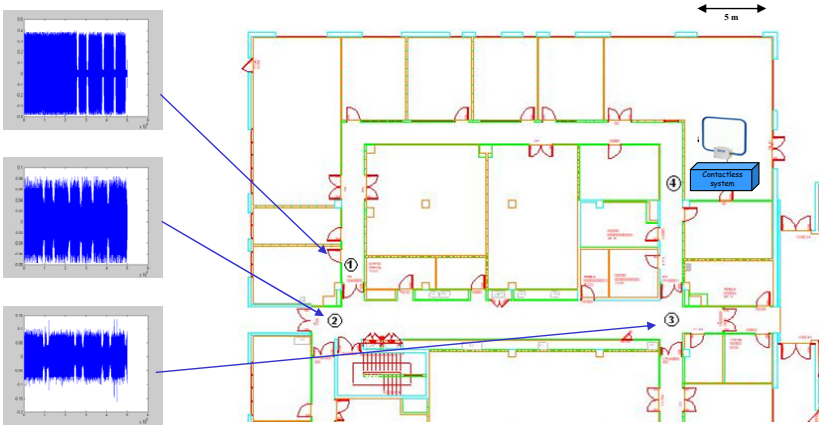


FIGURE 5: Eavesdropping along a horizontal floor.

7. Eurosmart : White paper RFID technology security concerns, understanding secure contactless device versus RFID, October 2007.

8. F. Vacherand et al., Security and Privacy for Contactless Devices, e-Smart'08, Sophia Antipolis France, 2008.

9. G. Hancke, Eavesdropping Attacks on High-Frequency RFID Tokens, RFIDSec08, 2008 10.O. Savry et al., Security and privacy Protection of Contactless Devices, 20th Tyrrhenian Workshop, Pula, Italy 2009.

11.F. Vacherand et al., Risk Analysis on Contactless Link , e-Smart'09, Sophia Antipolis France, 2009.

12.F. Vacherand et al., Experimental Measurements for Risk Analysis Quotation on Contactless Devices, e-Smart'09, Sophia Antipolis France, 2009.

Introduction au NFC et sécurité « sans contact » dans les mobiles

Guillaume Achten[1], Emmanuel Desdoigts[1], Antoine Coutant[2], Christian Damour[2], Fabrice Le Gall[2]

[1] FIME Innovation (<prénom>.<nom>@fime.com)
[2] Orange Business Services/ IT&L@bs (<prénom>.<nom>@aql.fr)

Résumé Dans cet article, nous allons aborder le NFC ainsi que la sécurité « sans contact » dans les téléphones mobiles. Après avoir introduit le principe du NFC comme un sous-ensemble du RFID, les standards et spécifications, les applications ainsi que la question des tests de validation fonctionnelle, nous présentons le NFC dans la téléphonie mobile, ses applications et tests de validation. Enfin, après avoir présenté la problématique de sécurité, nous détaillons, à partir du modèle STRIDE, les menaces de sécurité pouvant s'appliquer aux mobiles NFC. Pour finir, nous donnons quelques pistes contribuant à la sécurité « bout-en-bout » de tels mobiles. **Mots-clés.** NFC, STRIDE, téléphonie mobile, sécurité sans contact.

1 Introduction au NFC

Le terme NFC (*Near Field Communication*) est utilisé pour définir une communication en champs proches donc « sans contact ». Il s'agit d'un sous-ensemble de la technologie RFID (*Radio Frequency Identification*) qui utilise le principe des champs électromagnétiques pour établir une communication dans un environnement défini. Un système RFID est composé d'éléments allant de l'étiquette (aussi appelé *tag*) au réseau collecteur (le lecteur).

Le RFID est une technologie de communication sans fil à distance utilisant un protocole radiofréquence (RF). Elle se base sur les normes ISO 14443 A, B et Felica. L'étiquette RFID est activée par la présence des ondes radio d'un lecteur et peut ainsi transmettre les informations qu'elle stocke (comme un numéro d'identification par exemple). Plus de 3000 brevets ayant trait au domaine RFID ont été déposés entre 2003 et 2007 aux États-Unis et un peu moins de 1000 dans d'autres pays. La prévalence de cette technologie et de ses applications n'est plus à démontrer.

Non seulement le NFC bénéficie des atouts du sans contact, de la communication RF, de la sécurisation mais il peut aussi accéder aux ressources de l'équipement qui l'héberge (téléphone, assistant personnel...). Le principe s'appuie sur le phénomène d'induction électromagnétique qui se caractérise par la création de courant en présence de champ magnétique.

Le NFC permet une communication rapide et facile (dû au sans contact). Aujourd'hui, la distance de communication via un téléphone dit « NFC » est d'environ 2 à 3 centimètres (nul doute que cette distance sera améliorée dans les prochaines années). On entend beaucoup parler de systèmes NFC pour des applications diverses et variées, les plus connues

aujourd'hui étant les applications pour le paiement et le transport intégrées dans le téléphone mobile. Cependant, le domaine des applications possibles est beaucoup plus vaste et nous en donnons un aperçu ci-après.

1.1 Principe de communication

Le principe de communication NFC est simple et repose toujours sur un maître (appelé l'initiateur) et un esclave (appelé la cible). Les termes « initiateur » et « cible » sont ceux utilisés dans les normes. Le système NFC a la particularité d'être bidirectionnel ce qui signifie que le principe de communication peut toujours être inversé. En revanche, il demeure principalement *half-duplex* puisqu'il ne peut exister qu'un seul initiateur à un instant donné (hormis quelques évolutions récentes apportant un mode *full-duplex* ou pair-à-pair, non utilisé actuellement).

La communication commandes/réponses (autrement appelées liaisons montantes et descendantes) va être portée par un signal dans une bande de fréquence donnée. Ces bandes de fréquence correspondent à celles définies dans les normes RFID. Qui dit champ proche, dit également proximité, nous parlons alors d'une distance de communication maximum de 10 centimètres, même si la notion de distance efficace ou portée n'est abordée dans aucun standard (ce sont les régulations locales qui limitent la puissance émise et la largeur de bande donc la distance de communication).

Principe technique Le transfert d'informations d'une base station (appelé aussi initiateur ou lecteur) vers un transpondeur (appelé aussi cible, tag ou puce) s'effectue par radiofréquence (« *à l'aveugle* » c'est-à-dire à distance) et non par lecture optique comme c'est le cas pour les codes barres.

Une puce NFC se compose principalement d'une puce électronique reliée à une antenne. Le principe de fonctionnement du NFC est qu'un transpondeur réagit lorsqu'il reçoit des informations provenant d'une base station, nous parlons alors de liaison montante. La puce NFC reçoit ces informations, les traite et renvoie en retour d'autres informations qu'elle contient vers la base station, nous parlons alors de liaison descendante. Le lecteur pourra à son tour envoyer de nouvelles informations, etc. Ainsi, un dialogue s'établit selon un protocole de communication prédéfini entre une base station et un transpondeur.

La figure 1 schématise le principe de fonctionnement du NFC entre un lecteur (la base station) et une puce NFC (le transpondeur). Un dispositif NFC (également appelé *NFC device*) peut initier une communication avec une cible et donc avoir le rôle de base station, nous dirons alors que le système NFC est initiateur (*NFC initiator*). Ce même dispositif peut à son tour être sollicité par un initiateur et donc être transpondeur, nous dirons alors qu'il est cible (*NFC target*).

Que le dispositif NFC soit initiateur ou cible, la communication sans contact transfère des données sur une fréquence appelée fréquence de porteuse, via une modulation du signal de cette fréquence dont dépend le débit de transfert. Contrairement à ce que l'on pourrait

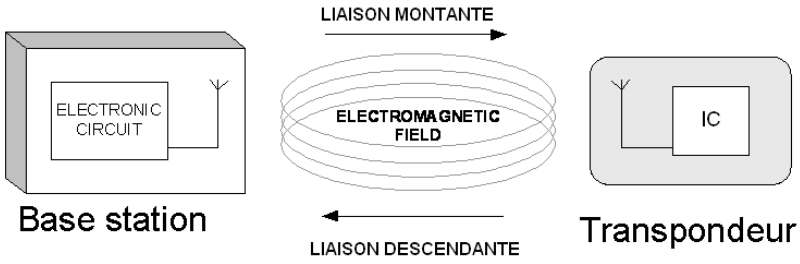


FIGURE 1: Vue d'ensemble du principe technique du NFC

imaginer, le NFC n'est pas forcément synonyme de 13,56 MHz (correspondant à la fréquence de porteuse en HF).

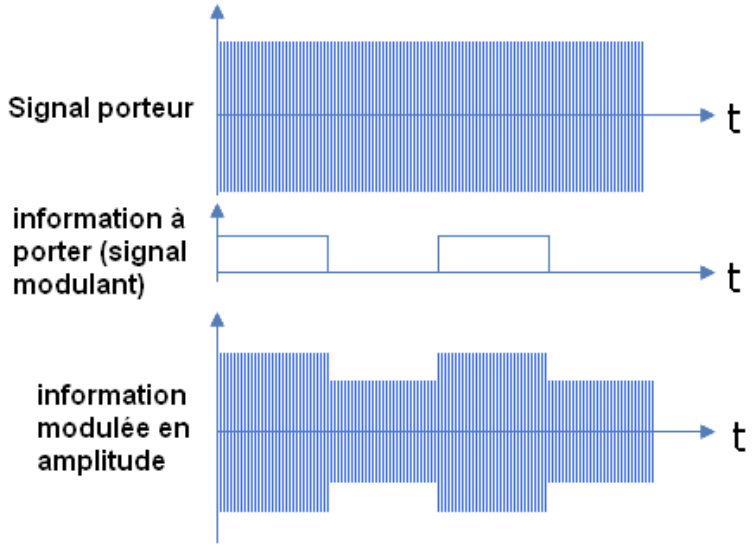


FIGURE 2: Exemple de modulation d'un signal en amplitude

Le choix de la fréquence à 13,56 MHz (bande HF) est dû au débit nécessaire à la plupart des applications, au codage et au spectre en bande de base, à la modulation, au spectre rayonné par cette fréquence de porteuse ainsi qu'aux réglementations en vigueur quasiment uniformes pour cette fréquence quelle que soit la région du monde.

Pour résumer, le NFC est basé sur le concept de messages et de réponses. L'initiateur envoie un message à la cible qui renvoie une réponse. Notons de plus qu'un initiateur peut

« parler » à plusieurs cibles mais pas au même moment. La phase d'initialisation permet à un lecteur de sélectionner la cible afin d'éviter des collisions radiofréquences. Cependant, nous pouvons aussi avoir plusieurs communications d'un lecteur vers plusieurs récepteurs.

Modes de communication et d'usage du dispositif NFC Une interface NFC peut fonctionner suivant deux modes d'usage : le mode « actif » (chacun des dispositifs génère alternativement son propre champ radiofréquence s'il veut envoyer des données) ou le mode « passif » (la cible utilise le champ généré par l'initiateur pour envoyer ses données et est alimentée par le champ généré par le dispositif avec lequel il communique).

Le NFC permet donc la communication entre un initiateur et une cible. Il existe trois modes de communication possibles pour un dispositif NFC ([MELS08]) :

- Mode lecture/écriture : mode permettant principalement de lire des cartes sans contact ou des tags tous les deux passifs (étiquettes communicantes) dans le but de recevoir de l'information, de modifier des données stockées ou d'accéder à du contenu.
- Mode émulation de cartes : le dispositif agit comme une carte à puce. Par exemple, le mobile NFC est associé à un élément de sécurité et émule le fonctionnement d'une carte à puce sans contact.
- Mode peer-to-peer : le dispositif communique avec un autre dispositif NFC (mobile, ordinateur, ...) permettant ainsi un échange local de données. L'un ou l'autre des dispositifs peut être initiateur ou cible.

1.2 Normes et spécifications

Concernant l'évolution des standards et des spécifications, le NFC suscite un intérêt croissant à travers le monde ainsi que de très nombreux travaux de normalisation, de recherche et développement de nouvelles applications selon trois angles de vue :

- le point de vue normatif à des fins d'interopérabilité et de respect des réglementations nationales en vigueur ;
- à travers l'élaboration de nouvelles spécifications permettant de répondre au mieux à de nouveaux besoins ;
- sous l'angle du développement de nouvelles et très nombreuses applications.

Standards ECMA et ISO du NFC Les principaux organismes de normalisation sont : l'ISO (*International Standardisation Organisation*) et l'ECMA (*European Computer Manufacturer Association*). Même si le NFC n'en est encore qu'à ses débuts, il s'appuie sur des normes et spécifications existant depuis plusieurs années ainsi que sur des technologies connues : normes ISO 14443, 15693 ou Felica pour la transmission HF.

L'ECMA a été le premier organisme de normalisation à publier des standards sur le NFC (ECMA 340, ECMA 356 ou ECMA 362). Ces standards ont ensuite été proposés à l'ISO et ont ainsi pu être validés et promulgués en tant que normes à portée mondiale. Le NFC est donc régi par les principales normes suivantes :

- ISO/IEC 18092 (également appelée NFC IP1) : norme définissant l'interface de communication du protocole NFC spécifiant les schémas de modulation, le codage, les vitesses de transfert, la configuration de la trame de l'interface RF ainsi que les schémas d'initialisation et les conditions requises pour le contrôle de collision de données pendant l'initialisation. Par ailleurs, cette norme définit un protocole de transport incluant les méthodes d'activation de protocole, d'échange de données ; elle spécifie aussi deux modes de communication (actif et passif). À noter enfin que cette norme s'inspire très fortement des standards ISO/IEC 14443-A et Felica.
- ISO/IEC 22536 et ISO/IEC 23917 : normes définissant respectivement la méthode de test pour l'interface RF et la méthode de test protocolaire pour le standard NFC IP1.
- ISO/IEC 21481 (également appelée NFC IP2) : définition plus élargie du NFC IP1 intégrant plus de possibilités sur la modulation, le codage mais pas sur le débit.

Le tableau ci-dessous établit les vitesses actées par les normes d'utilisation NFC.

	NFC IP 2			
	NFC IP 1			
	14443 A	Felica	14443 B	15693
Débit (kbits/s)	106	212 ou 424	106	1,6 à 27

Table 1. Vitesses de débit

Spécifications du NFC Forum et de l'ETSI Contrairement à l'ECMA ou l'ISO qui rédigent des standards et des normes, le « NFC Forum » (fondé en avril 2004 par Nokia, NXP Semiconductors et Sony) est un rassemblement d'industriels rédigeant des spécifications. Pour la plupart, les spécifications publiées concernent la partie protocolaire. Il est à noter quelques différences avec les standards ISO puisque, par exemple, la notion de distance est abordée dans ces spécifications.

L'ETSI (European Telecom Standard Institute) s'intéresse bien évidemment au NFC appliqué à la téléphonie mobile. On y retrouve les équivalents des standards ISO/IEC 18092, 22536 et 21841 (respectivement TS 102.190, TS 102.345 et TS 102.312) mais également des spécifications relatives à la connexion de l'interface NFC avec la carte SIM (TS 102.613, TS 102.622).

Le tableau suivant établit la correspondance entre normes et standards des différents organismes travaillant au niveau hardware et software pour le NFC (les cases sur fond ocre signifient que c'est encore à l'état de travaux).

Couches		ECMA	ISO	ETSI	NFC Forum	Contenu
NFC IP1	basses	340	18092	TS 102.190	N/A	Couches basses (RF et digitales)
		356	22536	TS 102.345		Plan de test RF
		362	23917	?		Plan de test digital
NFC IP2	basses	352	21481	TS 102.312	N/A	Couches basses (RF et digitales)
		?	?	?		Plan de test RF
		?	?	?		Plan de test digital
NFC Forum	basses	N/A			Digital	Description RF et jeu de commandes
					Activity	Interaction entre les commandes
					?	Plan de test RF
					Test cases	Plan de test digital
GSM A	moyennes	373 (??)	28361	TS 102.613		SWP – SHDLC
				TS 102.622		HCI
NFC Forum	hautes	N/A			NDEF	Format de stockage des données
					RTD	TS RTD
					RTD_Text	TS RTD Text
					RTD_URI	TS RTD URI
					Type-1-tag	Spécification Tag 1
					Type-2-tag	Spécification Tag 2
					Type-3-tag	Spécification Tag 3
					Type-4-tag	Spécification Tag 4
					SmartPoster	RTD smart poster

Table 2. Spécifications NFC

Standards de la sécurité dans le NFC La sécurité dans le NFC consiste à prendre en compte tous les aspects de la sécurité impliqués dans les applications de cette technologie. Il existe à l'ECMA deux standards du NFC dans la sécurité : ECMA 385 et ECMA 386. Ces standards décrivent la sécurité bas niveau de la transmission (i.e. le chiffrement de l'octet envoyé).

Il faut savoir que certaines applications utilisées ont déjà un chiffrement intégré au niveau applicatif, ce qui fait qu'aujourd'hui le standard est sujet à controverse.

1.3 Applications du NFC

Les applications en NFC sont très nombreuses, nous pouvons en retrouver dans la grande consommation (TV, appareil photo, ...), les appareils domestiques (réfrigérateurs, machine à laver, ...), la téléphonie mobile, la monétique, la billettique, la traçabilité, la logistique, la communication, la santé, etc.

Le tableau ci-dessous est un résumé des objectifs ainsi que des types d'applications attendus dans le domaine.

Objectif	Type d'applications
Déterminer la présence d'un objet	Gestion de biens
Fixer le lieu où se situe un objet	Traçabilité
Déterminer la provenance d'un objet	Contrôle d'authenticité
Assurer le lien entre le tag et l'objet taggé	Légitimité de l'identification
Valider l'information d'un objet pour prise de décision	Contrôle de processus
Authentifier le porteur d'un objet	Contrôle d'accès
Effectuer une transaction financière (ou opération billettique)	Paiement et transport avec authentification

Table 3. Objectifs et applications du domaine NFC

La téléphonie mobile est l'application qui va représenter la plus grosse part dans le marché de la communication en champ proche, les applications NFC peuvent se diviser en 4 types d'actions :

- « Touch and Go » : application où l'utilisateur doit juste avoir une action de passage de son produit devant un lecteur (contrôle d'accès, billetterie, ticket de transport, ...), il suffit d'approcher le support NFC pour établir le contact ;
- « Touch and Confirm » : application nécessitant l'intervention de l'utilisateur (utilisation de mot de passe, de code PIN, de bouton de validation, ...) pour confirmer une itération (un paiement par exemple) ;
- « Touch and Connect » : application liant deux systèmes NFC pour permettre un transfert de données en peer-to-peer (échange d'images, de musique, synchronisation de carnet d'adresses, ...) ;
- « Touch and Explore » : il s'agit ici de systèmes NFC contenant plusieurs applications de telle sorte qu'une fois la connexion établie, un utilisateur a le choix entre plusieurs actions ou services.

Tous ces exemples n'impliquent pas forcément de téléphone mobile, ne fonctionnent pas forcément à 13,56 MHz et les applications ne sont pas uniquement du paiement ou du transport. Cependant, le NFC à 13,56 MHz dans le téléphone mobile va représenter plus de 80

1.4 Tests de validation fonctionnelle du NFC

Abordons maintenant la question des tests de validation fonctionnelle du NFC au niveau de son interface de communication sans contact, sous l'angle des prescripteurs ou autorités par domaine, des processus ou schémas de validation et/ou de certification.

D'une façon générale, les prescripteurs ou autorités par domaine vont définir ou ont défini les processus et schémas de validation, certification, les référentiels et méthodologies de test applicables à ce jour (conformité à un référentiel, interopérabilité, autres tests éventuels). Les prescripteurs ou autorités peuvent être :

- les acteurs du monde bancaire (domaine du paiement ou du micro-paiement) ;

– les acteurs du domaine de la billettique ;
– les autres acteurs éventuels...

Dans le cas du mobile NFC, il s'agit par exemple de valider la portabilité d'une application générique sur plusieurs systèmes d'information constitués d'un mobile et d'une carte SIM (*Subscriber Identity Module*). Plus généralement il s'agit de faire abstraction de l'entité « *NFC Device* » en tant qu'élément technique, mais de la considérer sous ses aspects fonctionnels. Une même application doit fonctionner de la même façon quel que soit le support technique dans lequel elle est intégrée.

Ce domaine est encore non stabilisé et ces aspects ne peuvent être détaillés dans le présent article.

2 NFC dans la téléphonie mobile

Ce chapitre présente le mobile NFC, ses applications ainsi que la question des tests de validation fonctionnelle.

Dans le domaine des appareils mobiles, le « sans fil » joue un rôle important. La diversité des applications et leurs origines, parmi autant de fournisseurs de services sur des architectures de plate-forme ouverte, autorise le chargement de nouvelles applications ou de données à l'initiative du porteur (de l'utilisateur) via des interfaces variées :

– interface dite de proximité (par câble avec un PC, infrarouge, Bluetooth, ...)
– interface par accès direct à Internet (Wi-Fi 802.11a/b/g/n) ou par accès au réseau de l'opérateur (SMS / WAP / MMS, GSM / GPRS / EDGE / UMTS / HSDPA, ...)

Le mobile est un objet communiquant sécurisé susceptible dŚapporter de nouveaux services grâce à son clavier, son écran et sa capacité de communication (rechargement, paiement...).

2.1 Présentation du mobile NFC

La téléphonie mobile s'est développée de manière exponentielle depuis le début des années 1990 et bénéficie aujourd'hui d'améliorations importantes (miniaturisation des composants électroniques, usages variés...).

Aujourd'hui, le mobile NFC est un mobile équipé d'éléments NFC permettant ainsi différentes actions de la part d'un utilisateur : paiement, authentification, connexion, etc. Le NFC intègre la technologie sans contact dans les téléphones portables en apportant la possibilité d'une interaction avec les appareils électroniques.

L'avantage du NFC dans le mobile est que cette technologie fonctionne même si le téléphone est hors-tension.

Éléments NFC presents La figure 3 présente une architecture de mobile NFC (illustration issue de [GSMA2]).

Les différents éléments présents dans le téléphone sont le *NFC Controller*, l'antenne et le *Secure Element* (élément sécurisé en terme de mémoire et d'environnement d'exécution)

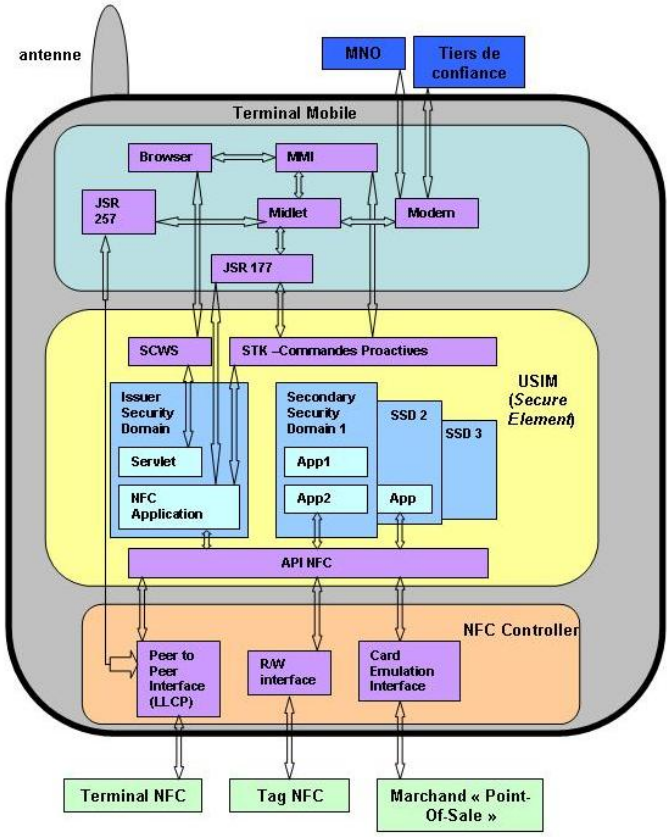


FIGURE 3: Exemple d'architecture de mobile NFC

qui est un environnement dynamique dans lequel le code et les données des applications sont stockés de façon sûre et l'exécution des applications se fait également de façon sûre. Sur le schéma précédent, le *Secure Element* est représenté par l'USIM (*Universal Subscriber Identity Module*) qui est une des implémentations de *Secure Element*. Différents acteurs communiquent avec le *Secure Element*, que cela soit l'opérateur MNO (*Mobile Network Operator*) ou des entités tierces parties.

Différentes interfaces et protocoles ont été développés pour traiter de l'association *Secure Element* – puce NFC sur mobile :

- HCI (*Host Controller Interface*) : le NFC Forum et l'ETSI ont défini une interface d'échanges entre la puce NFC et le *Secure Element* (TS 102.622) ;
- SWP (*Single Wire Protocol*) : la spécification TS 102.613 formalise les échanges d'informations entre carte SIM et module NFC ;
- Protocoles et interfaces propriétaires.

Systèmes d'exploitation et logiciels pour mobiles Les systèmes d'exploitation pour mobiles sont sensiblement différents de ceux développés pour les ordinateurs personnels de par des contraintes d'énergie et d'espace mémoire associés à du matériel spécifique, ainsi que de contraintes comme le support d'un usage interactif et sporadique...

D'autres différences sont induites par la partie logicielle du système plutôt que par le noyau du système d'exploitation. Les différences du système logiciel tirent leur origine des contraintes très différentes de l'interface utilisateur de ces appareils, comme l'absence d'un clavier complet et l'affichage relativement de petite taille. Il y a beaucoup de systèmes d'exploitation pour mobiles tels que Symbian OS, Palm OS, Linux, Windows CE...

De même, les applications développées pour un appareil mobile ne sont pas exactement les mêmes que celles conçues pour un système d'exploitation traditionnel car les appareils mobiles sont caractérisés par un très petit affichage, un clavier réduit, une souris remplacée par un écran tactile...

La plupart des applications sont développées pour une entrée minimale de texte et souvent affichent une boîte de sélection à la place d'un champ de texte. D'autres différences sont dues au faible espace de stockage disponible ainsi qu'à la faible vitesse des processeurs. Généralement, les appareils mobiles sont conçus pour ne supporter qu'une seule application interactive à la fois (appareils mono-tâches donc). Cependant, sur un appareil iPhone d'Apple par exemple, il est possible d'outrepasser les droits d'utilisation de l'appareil et ainsi exécuter deux tâches en parallèle.

En général, les applications peuvent être classées en deux groupes :

- soit elles ressemblent à une version allégée d'une application existante sur ordinateur personnel (comme un traitement de texte ou un navigateur Internet) ;
- soit elles sont développées spécifiquement pour être utilisées sur un appareil mobile.

Un point important dans le développement des applications NFC dans le monde du téléphone mobile est le langage utilisé pour le développement des nouvelles applications sur carte USIM. En effet, pour les solutions SIM-Centrique, les USIM utilisent le langage Java Card. Ce langage objet permet l'installation et l'utilisation de plusieurs applications sur une même carte.

Le Java Card permet donc d'associer sur une même carte une application de type « voix » et plusieurs applications de type « data » utilisant le NFC pour communiquer avec le monde extérieur, transport, paiement... Sans cette technologie, l'essor du modèle à base de SIM-Centrique qui, actuellement, est celui le plus utilisé sur le marché n'aurait pas pu fonctionner.

2.2 Applications du mobile NFC

Depuis quelques années, le mobile NFC s'introduit dans la vie courante. Les applications du mobile NFC sont diverses et variées mais la plupart d'entre elles concernent encore le contrôle d'accès.

Aux Pays-Bas, un test a été mis en place pendant la saison de football 2005-2006. Les supporters pouvaient utiliser leurs téléphones NFC afin d'accéder au stade de football du club Roda JC, ainsi que pour effectuer des achats dans les stands de nourriture et dans les magasins de supporters.

En France, des usagers de transports en commun utilisent actuellement la technologie NFC associée au mobile pour valider un titre de transport : Strasbourg, Paris, Rennes...

Fin 2008, le dernier téléphone mobile 6212 Classic Nokia équipé de NFC est en mesure aussi de fournir une liste d'applications comme le paiement sans contact, le transfert d'argent et le paiement à distance par exemple.

Durant l'année 2009, un nouveau dispositif d'embarquement de l'aéroport Nice Côte d'Azur, sur la ligne Nice-Orly, a été testé : le « Pass and Fly ». En passant le mobile devant une borne Pass and Fly, la carte d'embarquement du voyageur est téléchargée dans la puce NFC et, lors du contrôle de sécurité, le voyageur présente le téléphone à une seconde borne NFC. Le personnel de sécurité voit ainsi s'afficher sur l'écran la carte d'embarquement et le passager peut à la fois être identifié et obtenir une carte d'embarquement numérique.

Le NFC dans la téléphonie mobile est promis à un bel avenir.

2.3 Tests de validation fonctionnelle du mobile NFC

Il est indispensable que les acteurs du marché se réunissent par métier afin de définir les règles à appliquer pour valider ou certifier leurs fonctionnalités. Typiquement, c'est l'exemple des trois principaux opérateurs de téléphonie mobile français (Bouygues Telecom, Orange et SFR) qui ont créé pour cela l'AFSCM (*Association Française du Sans Contact Mobile*).

La validation porte sur le principe du cloisonnement entre applications embarquées et efficacité du firewalling embarqué avec les risques de corruption des données utilisées par une autre application, voire de capture d'informations sensibles telles que les clés, les informations personnelles de l'utilisateur ou ses codes d'accès. Le principe de l'établissement clair des responsabilités sur un terminal mobile multi-applications constitue également une problématique avérée. En effet, ces applications peuvent émaner de fournisseurs de services divers et variés ; tous n'étant pas d'un niveau de confiance homogène.

Dans cette optique, il faut mentionner les travaux de l'AFSCM autour de la conception et de la mise en œuvre d'un processus et d'un schéma commun et formalisé de validation fonctionnelle et sécuritaire préalable des applications des fournisseurs de services, auxquelles à terme, ils restreindront l'autorisation de téléchargement dans les téléphones mobiles de leurs abonnés.

Dans ce contexte, il est prévu le recours à des laboratoires tiers de confiance (entité de validation fonctionnelle et sécuritaire) préalablement dûment qualifiés par l'AFSCM. Les acteurs sont l'AFSCM, le fournisseur de services NFC (SP) qui devra soumettre l'application développée à une ou plusieurs entité(s) de validation fonctionnelle et sécuritaire référencées par l'AFSCM.

Les entités de validation fonctionnelle et sécuritaire détiennent les rôles suivants :
- mettre à disposition des moyens techniques reconnus par l'AFSCM et les fournisseurs de service permettant de certifier et d'identifier le code de l'application ayant fait l'objet de la validation ;
- prouver et s'engager fermement sur l'adéquation entre le code développé et le respect du référentiel fonctionnel et des règles de gestion et de développement ;
- s'assurer de l'étanchéité de ce nouveau service vis-à-vis des autres services NFC ;
- fournir une analyse suivant une grille de niveau de gravité du risque et présenter les recommandations pour la correction des problèmes.

Par contre, c'est le groupe technique et validation de l'AFSCM qui validera les rapports de validation fournis par les entités de validation fonctionnelle et sécuritaire, fournira un support d'expertise aux MNO sur les applications (un MNO peut vouloir être conseillé sur certains risques liés à la mise à disposition d'une application), autorisera/mettra à disposition les applications qui auront été correctement validées, examinera la demande de référencement d'une entité de validation, dressera un avis et les recommandations nécessaires vis-à-vis d'une entité de validation, référencera les entités de validation ayant été déclarées conformes au processus.

Le schéma ci-après présente l'exemple d'un processus de validation fonctionnelle pour les mobiles NFC en particulier. Ce processus couvre la réception des échantillons à tester ainsi que la validation suivant les critères définis par les opérateurs.

Les référentiels et méthodologies de tests applicables sont en cours de discussion et de rédaction par les acteurs du marché. Les référentiels existants dépendent de projets précis (par exemple : P€GASUS, Payez Mobile, Quickpass). Cependant, ce domaine est encore non stabilisé et ces aspects ne peuvent être détaillés dans le présent article.

Actuellement, le parc existant pour la téléphonie mobile ne permet pas de définir un processus d'interopérabilité significatif. Néanmoins, ce point est primordial (en particulier dans la téléphonie mobile) suite aux nombreuses difficultés d'intégration d'une application sur plusieurs supports différents.

D'autres types de tests peuvent aussi être appliqués : positionnement relatif des dispositifs NFC et perturbations électromagnétiques liées à l'environnement (traversée de matériaux cartons d'emballage produit ou autres matériaux, compatibilité électromagnétique et brouillage involontaire, réflexions multiples sur des parties métalliques engendrant diffraction, brouillages et surmodulation, phénomènes d'entrée en résonance, etc.) ou bien encore les mesures d'exposition humaine aux rayonnements engendrés.

3 Problèmes de sécurité du « sans contact »

La sécurité dans le NFC consiste à prendre en compte tous les aspects de la sécurité impliqués dans les applications de cette technologie.

Les attaques sur un mode de fonctionnement NFC peuvent être les mêmes que celles portées dans le monde du sans contact classique (séparer l'antenne de la puce, destruction

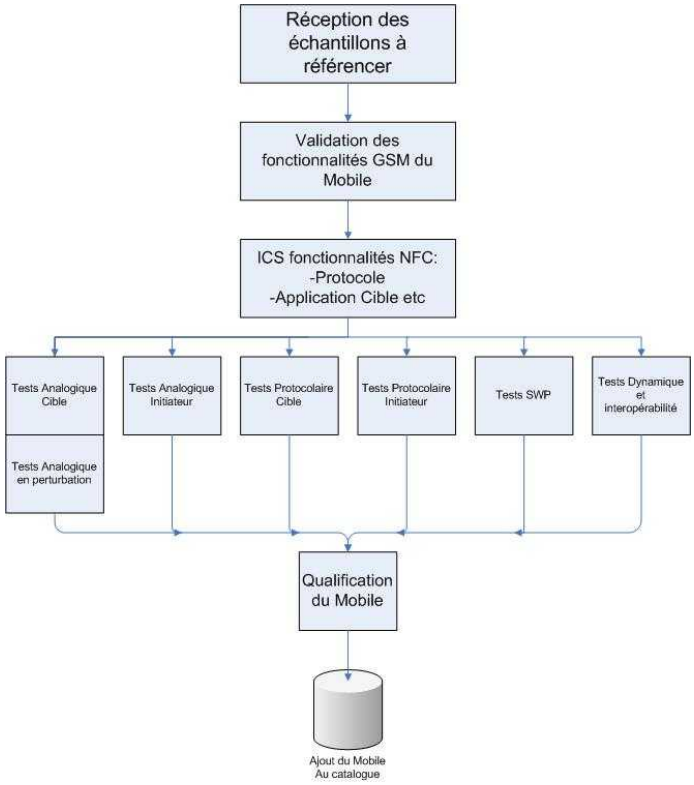


FIGURE 4: Exemple de processus de validation fonctionnelle pour les mobiles NFC

mécanique, etc.). Le principe même du sans contact amène une faille sur les modes d'accès mais l'applicatif reste inchangé. Par exemple, une application bancaire sur carte à contact est la même que sur un élément sans contact. Sa sécurité est garantie par la qualité du composant électronique et par la rigueur du développement effectué de façon sécuritaire. L'attaque en elle-même sera du même niveau pour l'applicatif quel que soit le dispositif (à contact ou non). En revanche, son invisibilité d'accès est un point problématique pour le sans contact principalement.

En général, les dangers des technologies sans contact apportent une problématique importante sur la notion de la sécurité des données personnelles et sur le droit à l'anonymat (ou protection de la vie privée). Ces deux éléments sont les risques majeurs du sans contact évoqués par les associations de consommateurs et les opposants à ces technologies, pouvant conduire à un rejet de leur adoption en masse par les utilisateurs concernés.

Le présent chapitre aborde la problématique de sécurité dans les mobiles NFC puis les menaces potentielles sur ces mobiles sous l'angle du modèle STRIDE. En effet, les téléphones mobiles ayant une interface supplémentaire, de nouvelles menaces de sécurité apparaissent.

Enfin, nous aborderons quelques éléments de réponse afin d'apporter une solution de sécurité de « bout en bout ».

3.1 Compréhension de la problématique

Les problèmes liés à la sécurité des appareils mobiles sont différents des problèmes de sécurité des ordinateurs personnels ou des serveurs. Comprendre ces différences est important dans le but d'appréhender la sécurité dans les appareils mobiles.

La problématique de la sécurité des appareils mobiles NFC se distingue de la sécurité informatique conventionnelle sur plusieurs aspects ([Sim07]) :

Mobilité : les appareils mobiles ne sont pas forcément gardés dans un endroit sécurisé, ils peuvent donc être volés ou manipulés. Voler un appareil mobile est beaucoup plus simple que de pénétrer dans un ordinateur personnel.

Fonctionnalités réduites : il manque un certain nombre de fonctionnalités aux appareils mobiles par rapport aux ordinateurs (possibilité limitée de traitement par exemple). Le manque de fonctionnalités peut alors faciliter certaines attaques par déni de service et cela complique l'implantation de mécanisme d'authentification (traditionnellement le couple nom d'utilisateur / mot de passe).

Convergence technologique : les appareils mobiles combinent énormément de technologies différentes en un seul matériel (un PDA, un téléphone, un baladeur MP3, un appareil photo numérique...) ce qui conduit alors à plus de risques de sécurité. Chaque nouvelle fonctionnalité ajoute au moins une nouvelle cible qui peut être potentiellement attaquée.

Forte connectivité : beaucoup d'appareils supportent de multiples façons de se connecter à Internet ou à tout autre réseau ce qui implique autant de « portes » pour les attaquants. La diversité de ces interfaces engendre des risques d'attaques par services croisés (*cross-services attacks*, voir [MVDL06]) comme par exemple accéder par l'interface LAN sans fil à l'interface téléphonique pour composer un numéro.

Forte personnalisation : les appareils mobiles ne sont généralement pas partagés entre les utilisateurs et, a priori, ils ne sont jamais loin de leur propriétaire. Une forte personnalisation, couplée avec une forte connectivité, augmente la menace de violation de la vie privée (un appareil mobile se situe là où se trouve son propriétaire et donc localiser le mobile signifie localiser son propriétaire).

Reste encore à mentionner l'impact sur la sécurité des sources diversifiées et non maîtrisées de téléchargement multiple d'applications pouvant s'avérer extrêmement important sachant les risques d'utilisation d'applications non maîtrisées (voire hostiles ou malveillantes) et enfin le risque de téléchargement de *maliciels* (vers, virus, chevaux de Troie, logiciels espions, etc.).

Et quand bien même une application reconnue de confiance est installée, il subsiste encore des risques d'infection de cette application par des techniques d'injection de code. Par

exemple, en juillet 2009, la société Etisalat (Émirats Arabes Unis) a distribué un spyware, permettant l'interception de messages et d'emails, à ses 145.000 clients utilisant BlackBerry, en le présentant comme une mise à jour pour améliorer les performances. Le principe est extrêmement simple : cette mise à jour a installé un fichier Java qui envoie une copie des messages à un serveur d'Etilasat à l'insu de l'utilisateur.

Ainsi, la sécurité des appareils mobiles est bien plus complexe que celle des ordinateurs de bureau. Tous ces aspects apportent de nouvelles implications comme l'augmentation de la complexité lors d'audits de sécurité sur les appareils mobiles.

3.2 Menaces envisageables

Le modèle STRIDE ([TDST06]) permet de décrire les menaces de sécurité en réalisant une taxonomie de celles-ci. Ce modèle permet d'associer à chaque catégorie des contre-mesures permettant d'aller à l'encontre de ces attaques et permet aussi de déterminer les risques liés à l'usage de la technologie NFC.

Les menaces envisageables pour un appareil mobile ne sont pas seulement applicables au dispositif NFC mais aussi au niveau applicatif (cas des attaques par services croisés). Par exemple, pour réaliser un déni de service ou une usurpation d'identité, un attaquant injecte un virus ou un cheval de Troie dans un appareil mobile suite à un vol de l'appareil mobile, grâce à un message frauduleux de type MMS (*Multimedia Messaging Service*) ou SMS (*Short Message Service*), ou suite à une mise à jour frauduleuse (exemple précédent du spyware d'Etisalat)...

Spoofing identity (usurpation d'identité) Les attaques d'usurpation d'identité incluent tout ce qui est fait par un attaquant cherchant à se faire passer pour un utilisateur légitime et ainsi obtenir et/ou accéder à des données d'identification d'une personne (login et mot de passe par exemple).

La menace « perte ou vol d'un appareil mobile » n'est pas une menace spécifique aux appareils mobiles mais ces derniers sont plus susceptibles de disparaître qu'un ordinateur ce qui peut entraîner une perte de la confidentialité et/ou une détérioration volontaire (installation d'un logiciel espion par exemple dans le cas où l'appareil réapparaît après un certain temps).

Nous retrouvons aussi, dans cette catégorie de menaces, le clonage (*cloning*) d'une puce NFC dans une autre, les attaques par relais (*Man-in-the-Middle*) ainsi que les attaques par rejeu (*replay attack*) du signal transmis entre une puce valide et un lecteur.

L'attaque de type *cloning* peut être indétectable et mise en œuvre par un adversaire déterminé. La meilleure façon de contrer ce type de malveillance est de protéger la puce suivant les règles de l'état de l'art (authenticité, intégrité, confidentialité). À titre d'exemple, début 2006, en Allemagne, Lukas Grunwald clone la puce RFID de son propre passeport avec du matériel du commerce.

Une attaque par relais se base sur deux terminaux, un appelé « *ghost* » (fausse étiquette ou *fake tag*) et l'autre appelé « *leech* » (lecteur de l'attaquant ou *adversary reader*). L'illustration suivante décrit le principe de ce type d'attaque.

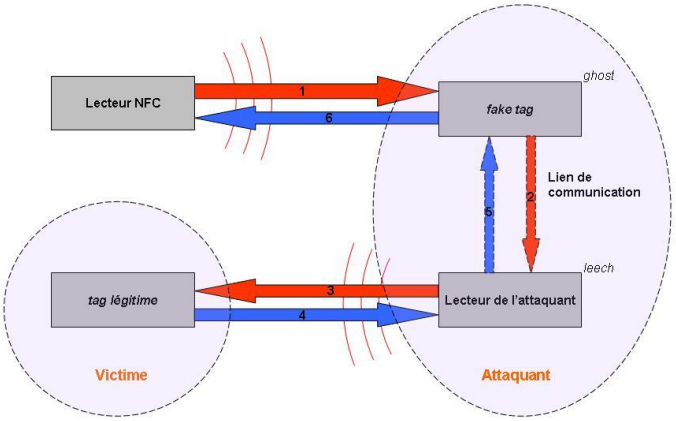


FIGURE 5: Illustration de l'attaque par relais ou « man-in-the-middle »

Le scénario de cette attaque est le suivant :

1. Un lecteur NFC envoie un message d'identification au *ghost* qui se comporte comme une carte classique ;
2. Le *ghost* reçoit donc le message et l'envoie au *leech* en utilisant un canal de communication rapide dans un délai minimum et sans aucune manipulation de données ;
3. Le *leech* reçoit le message, imite le lecteur « réel » et transmet le message à l'étiquette victime ;
4. La victime renvoie donc son message au *leech* ;
5. Le *leech* envoie la réponse reçue au *ghost* ;
6. Le *ghost* envoie la réponse reçue par le *leech* au lecteur NFC initial.

Il est à noter que ce processus est totalement transparent vis-à-vis des victimes. De plus, en utilisant un *ghost* et un *leech*, nous pouvons avoir une distance entre le lecteur « réel » et l'étiquette victime pratiquement illimitée. Utiliser cette technique permet donc de créer un relais.

Dans le cas d'une attaque par rejeu, un attaquant, muni d'un lecteur portatif convenablement programmé, peut secrètement lire et enregistrer une transmission de données d'une puce vers un lecteur. Ensuite, il lui suffit de retransmettre ces données afin de paraître être un utilisateur valide.

Pour se prémunir des attaques de ce type, une contre-mesure peut être d'utiliser des moyens appropriés d'authentification entre un lecteur et une étiquette (saisie d'un code PIN par exemple ce qui fait perdre beaucoup d'intérêt à cette technologie). Une autre solution de sécurité peut être qu'un lecteur dispose d'un temps maximal de réponse attendue. Pour finir, les secrets doivent être protégés de façon conforme à l'état de l'art et il n'est pas recommandé de les partager.

Tampering with data (altération de données) Dans cette catégorie, se classent les menaces dont le but de l'attaquant est de modifier, ajouter, effacer ou réordonner des données. Pour pouvoir modifier, ajouter, effacer ou réordonner des données, une écoute du canal de communication sans fil peut permettre à un attaquant d'extraire des informations confidentielles (noms d'utilisateurs et mots de passe par exemple) si les transmissions ne sont pas chiffrées.

Une attaque basée sur les infrastructures (serveur, lecteur, ...) est aussi à envisager. De même, un attaquant ayant réussi à prendre le contrôle partiel ou total d'un appareil mobile peut y injecter du code, transmettre ses propres informations, etc.

Il y a trois types d'attaques pour cette catégorie :

Modification pendant la communication : un attaquant est situé entre l'émetteur et le destinataire. L'attaquant, qui intercepte le signal, peut, a priori, modifier le signal et transmettre un signal modifié au destinataire. La possibilité de mener cette attaque (changer un 1 en 0 ou vice-versa) dépend de l'amplitude de la modulation du signal qui diffère selon que l'on est en mode passif ou actif. Les travaux décrits dans [HB06] ont montré que la modification était possible si le chevauchement du signal de l'attaquant avec le signal d'origine était totalement exact.

Modification avant la communication : dans ce type d'attaque, nous retrouvons la modification d'une puce, l'effacement d'une puce, l'enregistrement des informations d'un attaquant, ... Concernant les mobiles NFC, la principale attaque est la modification d'une puce NFC sur un appareil mobile (remplacement, ajout d'informations, ...).

Insertion de données : ce type d'attaque est décrit dans [HB06]. Nous nous plaçons toujours dans le cas où un attaquant est situé entre un émetteur et un récepteur. L'insertion de données peut fonctionner si le temps de réponse du destinataire est long et si l'attaquant répond strictement avant le destinataire. En cas de chevauchement des données, ces dernières seront alors corrompues et cela correspondra à un déni de service.

Les contre-mesures associées à cette catégorie d'attaque sont la protection en lecture et/ou écriture, une transmission chiffrée, le chiffrement des données stockées... Une authentification de l'utilisateur, un hachage des données, une signature des données ou l'utilisation de protocoles résistants (disposant d'une preuve de sécurité) sont autant de moyens permettant d'éviter ce type d'attaques.

Repudiation (reniement) Les menaces de répudiation impliquent des utilisateurs refusant d'admettre qu'ils ont réalisés une action quelconque et qu'aucune autre partie ne peut prouver le contraire. Un attaquant cherche donc à réaliser des actions à l'insu du propriétaire légitime qui ne peut nier ces dernières.

Par exemple, les attaques par surfacturation sont des attaques impliquant un service payant donné dont le but ici est de charger le compte de la victime de frais supplémentaires. La seule chose dont l'attaquant a besoin de faire est d'envoyer ce genre de trafic vers la victime (car le mobile est connecté en permanence au réseau et la facturation se fait en fonction du volume de données transférées). Le fournisseur ne vérifie pas si le trafic a été demandé par la victime et facture donc celui-ci.

Ce type de menace peut arriver dans le cas d'une mauvaise implémentation pour les deux interlocuteurs de la communication et aucun d'eux n'est en mesure de justifier l'action réalisée. Pour contrer ces menaces, des signatures numériques ou un horodatage peuvent être envisagés.

Information disclosure (divulgation d'informations) Dans cette catégorie, se classent les menaces dont le but de l'attaquant (utilisateur illégitime donc non autorisé) est de parvenir à obtenir des informations (accéder aux données personnelles par exemple) :

Écoute passive : ces attaques cherchent à traquer, identifier le propriétaire d'un appareil, nous retrouvons :

- **Eavesdropping ou « écoute aux portes »** : en utilisant un canal sans contact, le NFC n'offre pas de protection contre « l'écoute passive ». Il est ainsi possible pour un attaquant d'écouter une conversation privée et de récupérer les données.
- **Skimming** : dans le but de lire des tags, il est possible d'utiliser un « skimmer » (ou imitateur) composé d'un lecteur, d'un amplificateur de courant, d'un buffer de réception, d'une antenne et d'une source de courant comme indiqué dans [KW06].
- **Tracking et vie privée** : récupérer des informations relatives à la vie privée d'autrui.

Side-channel attack : les attaques de ce type (par canaux cachés) sont analogues à celles qui existent dans le domaine des cartes à contact avec la capture d'information sur les canaux cachés. L'analyse de puissance est l'art de trouver des informations au sujet d'un secret à partir des aspects physiques de l'implémentation du cryptosystème (analyse des champs électromagnétiques générés par les pointes de courant en particulier) sans attaquer l'algorithme lui-même. Cette attaque se concentre sur l'analyse des changements de consommation d'énergie de puces utilisant un cryptosystème. Cependant, ce type d'attaque nécessite d'avoir en sa possession du matériel coûteux et des connaissances solides dans la discipline de l'électromagnétisme et des protocoles de communication.

L'absence de lien physique dans le NFC rend la communication plus aisée mais d'autant plus risquée. Par exemple, à chaque fois, qu'une carte communique avec un lecteur, celui-ci peut récupérer le *User Device Identification Number* (UID pour les carte ISO 14443 de type

A et PUPI pour celle de type B), ce numéro peut être intercepté et utilisé pour tracer qui a utilisé ce lecteur voire pour entrer dans le système.

Comme toutes les technologies sans fil, le NFC ne s'affranchit pas des contraintes liées au fait que la sécurité du transport de la communication est fragilisée par l'absence de lien physique. Il faut donc pouvoir s'assurer que la communication est réalisée avec la bonne tierce partie, que la communication n'est pas écoutée ni altérée. Pour se prémunir de ces attaques, il est nécessaire d'utiliser un algorithme de chiffrement largement éprouvé dans le milieu académique, de protéger les secrets et de ne pas les partager.

Denial of service (déni de service) Ici, le but de l'attaquant est de réaliser un refus d'accès à un système pour un utilisateur valide ou de corrompre un système. Ce type d'attaque peut être, a priori, accomplie facilement et est difficilement prévisible. Le déni de service cherche à rendre un service ou un appareil inutilisable (momentanément ou non) pour son utilisateur. Dans ce cas, nous pouvons citer les attaques suivantes :

- *Jamming* : attaque par encombrement et perturbation (i.e. brouillage de communication), l'utilisation d'un appareil de type *RFID Jammer* (ou brouilleur) permet, par exemple, de perturber des données transmises dans la gamme de fréquence utilisée. Cela correspond à l'ajout de bruits électromagnétiques pour inonder le champ RF et ainsi empêcher l'analyse du signal par un lecteur. Il est possible de contourner ce problème en détectant et vérifiant le champ RF afin de déterminer s'il y aura collision ou non.
- *Zapping* : le but de cette attaque est la destruction d'un tag, le fait de détruire un tag NFC est de fait un déni de service. Cette attaque peut être réalisée avec une décharge électromagnétique ou un envoi de commandes bloquantes. Pour désactiver ou détruire une puce, nous utiliserons un RFID zapper (ou EMP gun) qui copie la méthode du micro-onde (à une échelle plus petite).
- Attaques liées aux cartes duales et cartes combi :
  - Attaque de l'interface la plus faible (cas des cartes duales) : attaques réalisées sur l'interface qui a le niveau de sécurité le plus faible.
  - *Crosstalking* (cas des cartes combi) : possibilité de profiter des droits sur une application « contact » pour lancer l'application fonctionnant sur une autre interface « sans contact ».
  - *Handover* : applicable dans le cas où l'on passe d'un canal de communication à un autre (risques de sécurité). Si le produit ne distingue pas le passage à un autre canal, on risque de se retrouver à utiliser un canal avec les privilèges d'un autre canal (ceci pouvant mener à des failles de sécurité). Par exemple dans le cas d'une mauvaise gestion des priorités entre interfaces (une interface peut être prioritaire par rapport à une autre). À titre d'exemple, voici les menaces que l'on peut rencontrer dû à une mauvaise implémentation : exploitation d'une mauvaise gestion d'un reset ou variation intentionnelle des conditions de fonctionnement entraînant une mauvaise

initialisation, un mauvais reset (nettoyage des mémoires, des clés de chiffrement des mémoires, etc.
- Autres dénis de services liés aux cartes :
  - Transaction effectuée sur plusieurs cartes d'un porteur au lieu d'une seule (le targetting) ou transaction effectuée sur une carte au lieu d'une autre.
  - Un tag contenant une commande d'attaque (assimilée à un virus) au lieu de données comme une injection de requêtes SQL, une attaque de type Cross-Site Scripting... (pour approfondir le sujet, on pourra se référer à l'article [RCT06]).

Le *jamming* ou le *zapping* sont des attaques contre lesquelles il est très difficile de se prémunir. Il existe peu de solutions de sécurité pour éviter ce type de malveillance (la protection la plus efficace étant la cage de Faraday).

Les vers, virus ou chevaux de Troie sont des menaces pour les appareils mobiles de la même manière qu'ils le sont pour les ordinateurs. Ils volent ou détruisent les données et peuvent rendre les systèmes infectés inutilisables. Les vers, virus ou chevaux de Troie peut être reçus par MMS ou SMS. Il est donc indispensable de considérer que toute donnée venant de l'extérieur doit être considérée comme potentiellement dangereuse.

Elevation of privilege (augmentation des droits) Ce type de menace permet à un utilisateur de gagner des accès privilégiés (obtenir plus de droits d'accès dans un système par exemple) et ainsi compromettre ou détruire un système entier. Ce genre de menaces inclut les situations dans lesquels un attaquant a pénétré les défenses du système pour exploiter et réaliser des dommages au système (intrusion, virus, ...).

Un attaquant ayant obtenu des droits d'administrateur pourra de fait insérer du code ou des données malicieuses dans la base de données pouvant impliquer des dommages à tous les niveaux de communication. Pour éviter ce genre de cas, il faut qu'un utilisateur ait le moins de droits possibles.

Par exemple, dans le cas des produits iPhone d'Apple, le « *jailbreak* » est une attaque de ce type consistant à modifier les droits en écriture sur la partition système root afin de modifier le système de l'appareil. Selon Apple, le *jailbreak* est à considérer comme un acte illégal et compromet la sécurité ainsi que la fiabilité de l'iPhone...

3.3 Solutions de sécurité de « bout en bout »

Cette section aborde la question de la sécurisation de bout en bout des échanges de données entre deux dispositifs NFC ; laquelle implique de créer un « chaîne de confiance » parmi les différentes composantes logicielles et matérielles impliquées dans une communication sécurisée entre deux dispositifs NFC. La sécurité dans le mobile est encore un domaine de recherche relativement jeune. Nous allons considérer trois axes principaux pour sécuriser un mobile NFC :
- sécurité du mobile (dispositif NFC et applications)
- sécurité du canal de communication

– sécurité du système (le lecteur)

Avant de commencer, notons qu'authentifier le porteur d'une puce (par login et mot de passe par exemple) permet de mettre en œuvre une protection efficace contre certaines attaques citées précédemment.

Sécurité du mobile Pour tester la sécurité du mobile NFC, le dispositif NFC ne doit pas être le seul élément sécurisé. Il est nécessaire que les applications hébergées sur un mobile soient aussi sécurisées que possible.

Nous allons considérer ici l'apport du fuzzing qui est une méthode s'appuyant sur des outils logiciels (appelés des *fuzzers*) pour automatiser l'identification de bugs ou de failles dans des applications. Le fuzzing, dans le domaine de la sécurité informatique, permet de découvrir relativement rapidement des vulnérabilités (des erreurs) parmi des milliers de lignes de code d'un programme. Un avantage du fuzzing est la simplicité d'écriture des programmes de test sans nécessairement connaître le fonctionnement du système. Cette méthode d'analyse est aussi désignée par « test en boîte noire ».

Le fuzzing n'est pas à mettre en concurrence avec la méthode des tests unitaires car ces derniers ne testent qu'une unité de calcul et indiquent que cette dernière semble avoir un résultat correct pour un ensemble d'entrée de données alors que le fuzzing teste une application dans son ensemble.

Le processus de fuzzing consiste à vérifier les entrées possibles (« quasi » conformes et générées aléatoirement) pour une application donnée et à forcer des opérations dans le cas où celle-ci réagit de manière anormale. Cette technique permet donc de tester la réaction d'un programme à des entrées inhabituelles. Si le programme échoue (par exemple, en se terminant anormalement) alors ce dernier est défectueux. Il ne faut pas voir le fuzzing comme une technique élaborée d'évaluation de la sécurité mais plutôt comme un outil supplémentaire.

En juillet 2007, suite à la sortie de l'appareil iPhone d'Apple un mois auparavant, les auteurs de [MHM07] ont découvert une vulnérabilité dans l'iPhone causée par l'application MobileSafari grâce à la technique de fuzzing. En conclusion, les auteurs annoncent qu'Apple a pris les précautions nécessaires pour sécuriser le dispositif (en ne laissant pas à disposition le code source aux attaquants) mais aucune précaution n'a été prise concernant les applications.

Dans [MM09], Mulliner et Miller ont trouvé des messages de type SMS pouvant causer des arrêts involontaires (des crashes) sur des mobiles iPhone et Androïd (sans pour autant les dévoiler dans leur étude !). Ces messages ont été trouvés en générant des SMS par la technique du fuzzing. Les auteurs se penchent en ce moment sur le cas de Windows Mobile.

Il apparaît préférable d'effectuer des tests de fuzzing sur le dispositif NFC mais aussi sur chacune des applications hébergées. La sécurité d'un mobile NFC doit être basée sur les échanges de flux mais aussi sur les applications existantes.

Sécurité du canal de communication Le canal sécurisé vient du monde de la carte à puce et plus précisément du monde bancaire. Il est défini par l'organisme de standardisation GlobalPlatform. Cette entité standardise la gestion des applications (installation, chargement des données et mise à jour), la gestion des clés et autres fonctions durant la vie entière (le cycle de vie) du système d'information. Cet organisme gère donc tout le cycle de vie de l'application mais aussi du système dans lequel les applications sont installées.

Entités intervenant dans les échanges Les principaux acteurs du processus lorsque l'on parle de *Secure Element* dans un mobile NFC sont, avec l'encarteur (vendeur de cartes SIM [*Subscriber Identity Mobile*]) :

- le MNO (*Mobile Network Operator*), propriétaire de l'UICC (*Universal Integrated Circuit Card*, carte sur laquelle réside l'application SIM), disposant généralement d'une plateforme OTA (*Over The Air*) de téléchargement ;
- les SP (*Service Providers*, entités comme les banques, les compagnies de transport...), fournissant un service à des clients et qui ont besoin que leur application soit présente sur une carte UICC ;
- des TSM (*Trusted Service Managers*) qui sont des tiers de confiance fournissant les possibilités techniques de déploiements des applications des SP sur le mobile.

D'autres rôles optionnels peuvent s'intercaler comme des agents intermédiaires commerciaux ou une autorité de contrôle CA (*Controlling Authority*) telle que :

- la CKLA (*Confidential Key Loading Authority*, défini dans [GP09]) permettant d'avoir un jeu de clés cryptographiques initiales pour le domaine de sécurité ISD dans une carte ;
- l'autorité DAP (*Data Authentication Pattern*, défini dans [GP09]) pour la signature de façon sécurisée de toute application avant son chargement dans la carte.

Secure Element et Secure Domain Les domaines de sécurité peuvent être utilisés pour la gestion des applications d'un fournisseur de service (SP) sur l'ensemble des *Secure Elements* mais en pratique essentiellement sur des cartes SIM. Un *Secure Element* peut contenir un ISD (*Issuer Security Domain*) appartenant au MNO et plusieurs SSD (*Supplementary Security Domain*) appartenant à un SP ou à un TSM. Ainsi, de multiples applications provenant de différents SP et du MNO peuvent être hébergés dans différents domaines séparés dans un *Secure Element*. Un domaine de sécurité contient un jeu de clés cryptographiques permettant la mise en œuvre d'un *Secure Channel* avec le MNO, SP ou TSM concernés.

Secure Channel Le principe est d'établir un canal sécurisé (*secure channel*) et un secret partagé (*shared secret*). La spécification est composée de deux standards (offrant une protection contre l'écoute ou la modification de données) :

- ECMA 385 (NFC-SEC : NFCIP-1 Security Services and Protocol) : ce standard spécifie le canal sécurisé NFC-SEC et les services de secret partagé pour NFCIP-1 et les PDUs et protocoles pour ces services.

– ECMA 386 (NFC-SEC-01 – standard de cryptographie NFC-SEC utilisant ECDH et AES) : ce standard spécifie les contenus de message et les méthodes cryptographiques utilisées dans ECMA 385. De plus, ce standard spécifie des mécanismes cryptographiques utilisant le protocole ECHM (*Ellipic Curves Diffie-Hellman*) pour la négociation des clés et l'algorithme AES pour le chiffrement et l'intégrité des données.

Le protocole de sécurité se décompose en deux phases : phase d'établissement / d'échange des clés et phase d'échanges sécurisés de données (chiffrement et intégrité).

NFC-SEC-01 est potentiellement vulnérable à une attaque de type *Man-in-the-Middle*. L'analyse sur les implémentations permettra d'identifier si une telle attaque est possible dans des cas réels d'usage.

Pour les produits sans contact, l'écoute illégale est l'attaque la plus citée. Elle consiste simplement à disposer un équipement dans l'entourage d'une communication sans contact et à capter au moyen de celui-ci un signal contenant les informations permettant la compréhension des données échangées entre le produit et le lecteur. La prévention de cette menace impose la mise en place d'un canal de communication chiffré.

La cryptographie est l'une des techniques que les fabricants utilisent pour assurer la sécurité néanmoins, la plupart des algorithmes utilisables présente des lacunes en lien avec cette technologie. Certains algorithmes sont trop complexes pour être portés sur une puce NFC, d'autres trop lents ou trop faciles à déchiffrer.

Architectures en cours de standardisation Plusieurs organismes de normalisation travaillent sur une architecture qui répondrait au besoin de sécurité, notamment GlobalPlatform ([GP09]), la Smart Card Alliance ([SCA09]) ou encore la GSMA ([GSMA1] et [GSMA2]). Ces architectures et les entités intervenant dans ces architectures ont pour but d'assurer la sécurité de bout en bout et notamment la réalisation de la gestion des clés cryptographiques, des domaines de sécurité (création, téléchargement, ...), des applications NFC sur mobile (création, téléchargement, ...) et du canal de communication.

Sécurité du lecteur NFC L'appareil mobile et le canal de communication doivent être sécurisés mais le lecteur recevant ou lisant les informations d'une puce NFC doit, lui aussi, être sécurisé.

Il est nécessaire de garder à l'esprit que toute donnée venant de l'extérieur doit être considérée comme potentiellement dangereuse (ce qui peut éviter des attaques de type viral). Supposons un lecteur infecté par un virus suite à une communication avec une étiquette frauduleuse et supposons que ce virus se propage de proche en proche... Nous avons alors l'effet « boule de neige » qui peut être désastreux dans certains domaines.

Autres solutions de sécurité Les auteurs de [MVDL06] ont développé un mécanisme de sécurité basé sur l'étiquetage des processus et des ressources système pour empêcher les attaques par services croisés (*cross-services attacks*). Celui-ci définit trois types d'objets,

les processus p, les ressources r et les interfaces i. Les processus et ressources possèdent un ensemble associé d'étiquettes. Chaque étiquette représente le fait que soit directement, soit indirectement, le processus ou la ressource ait été en contact avec une interface réseau spécifique.

Le mécanisme de sécurité inclut un composant de surveillance qui intercepte les appels systèmes potentiellement dangereux effectués par les processus. Ce sont les appels systèmes qui accèdent aux interfaces, qui accèdent ou exécutent les ressources, qui créent des ressources ainsi que de nouveaux processus. Quand un de ces appels systèmes est intercepté, les étiquettes du processus associé sont examinées en tenant compte d'un fichier global de règles qui spécifie quels sont les types d'actions permis, suivant les étiquettes associés au processus. Le résultat de l'analyse peut établir que l'accès est refusé ou autorisé et, de plus, les étiquettes des ressources / processus impliqués dans l'opération sont modifiées.

Il faut toutefois noter que l'utilisation de ce mécanisme d'étiquette implique une petite surcharge dans le système, notamment lorsqu'une application gère de nombreuses connections. Mais ceci constitue peut être le prix de la sécurité. D'autres solutions de sécurisation peuvent être les suivantes :

- En protégeant une puce NFC dans une cage de Faraday, il est possible de prévenir des attaques de copie voire même de traçage malveillant. La trame métallique fait écran et empêche toute lecture. Afin de limiter la possibilité de lecture à distance, certains états (USA par exemple) ont inséré dans une des pages de la couverture du passeport électronique une trame métallique empêchant la lecture si le passeport n'est pas au préalable ouvert. Les passeports anglais ne bénéficiant pas de cette protection, il est recommandé pour un Britannique d'insérer son passeport RFID dans une enveloppe de protection contenant des tramages métalliques.
- En 2007, les auteurs de [SPDRR07] proposèrent de sécuriser des puces RFID utilisant les fréquences UHF en introduisant un bruit lors de la communication entre un lecteur et un tag. Évidemment, chacun des deux acteurs est capable de filtrer ce bruit afin de retrouver la communication originale. L'ajout de ce bruit rendrait alors impossible l'écoute passive sans avoir connaissance du nombre aléatoire générant ce bruit.
- Dans [Dim08], l'auteur propose d'ajouter un proxy entre une puce et un lecteur. Le proxy chiffrerait les requêtes du lecteur et déchiffrerait les réponses du tag.

De plus, les auteurs attirent l'attention sur la nécessité d'effectuer des contre-mesures efficaces sur lŚimplémentation des algorithmes cryptographiques inclus dans des puces afin que les industriels ne soient plus mis à défaut lors d'un piratage. Quel que soit l'algorithme cryptographique utilisé (à clé secrète ou publique), il faut aussi trouver une solution permettant de protéger efficacement la clé.

4 Conclusion

Le NFC est donc une technologie de proximité qui permettra de faciliter la vie des usagers tout en permettant des échanges sécurisés. Aujourd'hui, le NFC devient le centre

des préoccupations de nombreux acteurs du marché (opérateurs, constructeurs, encarteurs, acteurs issus du monde bancaire). Ces acteurs, dont les intérêts divergent, sont fortement impliqués dans la standardisation NFC et dans plusieurs organismes de normalisation. Plusieurs standards cohabitent sans pour autant qu'une solution soit totalement acceptée par tous, ralentissant ainsi le déploiement.

Toutefois, cette technologie se répand à une vitesse accélérée ces dernières années et bénéficie d'une prospective favorable. Le NFC suscite toujours des préoccupations particulières au sujet de la sécurité et de la protection de la vie privée. Le NFC ne doit pas être considéré comme un concurrent direct de Bluetooth ou du Wi-Fi mais plutôt comme destiné à cohabiter avec ces technologies.

Un mobile NFC ne doit pas seulement être sécurisé au niveau de son interface sans contact mais aussi au niveau applicatif (un moyen rapide et efficace de trouver des failles étant le fuzzing). Pour se prémunir des attaques, il ne faut pas mettre en place une seule protection, mais plusieurs. Une compréhension claire de chaque attaque potentielle permet de choisir la protection adaptée. Un concepteur doit aussi garder en mémoire que toute donnée venant de l'extérieur doit être considérée comme potentiellement dangereuse et se poser les deux questions suivantes :

– « Contre qui (ou quoi) mon système doit-il être résistant ? »
– « Quel est le point le plus faible dans mon système ? »

En conclusion, dans un mobile NFC, il est nécessaire de sécuriser le dispositif suivant trois axes principaux :

– protection du mobile lui-même en protégeant le dispositif NFC présent ainsi que les applications présentes dans l'appareil,
– protection du canal de communication (utilisation du chiffrement et de l'authentification),
– protection du système de lecture et de traitement du NFC.

Références

[BMMOS08] U. Biader Ceipidor, C.M. Medaglia, A. Moroni, G. Orlandi and S. Sposato. NFC : Integration between RFID and Mobile, state of the art and future developments. Workshop on Emerging Technologies for Radio-frequency Identification, 2008

[Dim08] T. Dimitriou. Proxy Framework for Enhanced RFID Security and Privacy. 5th IEEE Consumer Communications and Networking Conference, 2008.

[GP09] GlobalPlatform. GlobalPlatform's Proposition for NFC Mobile : Secure Element Management and Messaging. White Paper, April 2009

[GSMA1] GSMA. Pay-Buy-Mobile, Business Opportunity Analysis. Public White Paper, Version 1.0, November 2007

[GSMA2] GSMA. Mobile NFC technical guidelines. Version 2.0, November 2007.

[HB06] E. Haselsteiner and Klemens BreitfuSS. Security in Near Field Communication (NFC). RFID Security, volume 6, 2006.

[JMW05] A. Juels, D. Molnar and D. Wagner. Security and privacy issues in e-passports. SecureComm. 2005.

[JS08] W. Jansen and K. Scarfone. Guidelines on Cell Phone and PDA Security. NIST Special Publication, volume 800, page 124, October 2008.

[KW06] I. Kirschenbaum, A. Wool. How to build a Low-Cost, Extended-Range RFID Skimmer. In Proceedings of the 15th USENIX Security Symposium, pages 43-57, 2006.

[MELS08] G. Madlmayr, J. Ecker, J. Langer and J. Scharinger. Near Field Communication : State of Standardization. First International Conference on The Internet of Things, pages 10-15, 2008.

[MHM07] C. Miller, J. Honoroff and J. Mason. Security Evaluation of Apple's iPhone. Technical Report, Independent Security Evaluators, 2007.

[MM09] C. Mulliner and C. Miller. Fuzzing the Phone in your Phone. Black Hat, 2009.

[Mul08] C. Mulliner. Attacking NFC Mobile Phones. EUSecWest, 2008.

[MVDL06] C. Mulliner, G. Vigna, D. Dagon and W. Lee. Using Labeling to Prevent Cross-Service Attacks Against Smart Phones. Lecture Notes in Computer Science, volume 4064, pages 91-108, 2006.

[Ore07] Y. Oren. Remote Power Analysis of RFID Tags. Cryptology ePrint Archive, Report 2007/330, 2007.

[OS06] Y. Oren and A. Shamir. Power Analysis of RFID Tags. Appeared in the rump session of Advances in Cryptology, CRYPTO, 2006.

[RCT06] M.R. Rieback, B. Crispo and A.S. Tanenbaum. Is Your Cat Infected with a Computer Virus ? PerCom–Fourth Annual IEEE International Conference on Pervasive Computing and Communications, Pisa-Italy, pages 13-17, 2006.

[Sim07] N. Simon. Sécurité dans les smartphones. Mémoire de Licence, Université Libre de Bruxelles, Faculté des Sciences, Département d'Informatique, 2007.

[SCA09] Smart Card Alliance. Security of Proximity Mobile Payments. A Smart Card Alliance Contactless and Mobile Payments Council White Paper, May 2009.

[SPDRR07] O. Savry, F. Pebay-Peyroula, F. Dehmas, G. Robert and J. Reverdy. RFID Noisy Reader How to Prevent from Eavesdropping on the Communication ? Lecture Notes in Computer Science, volume 4727, 2007.

[TDST06] D.R. Thompson, J. Di, H. Sunkara and C. Thompson. Categorizing RFID Privacy Threats with STRIDE. In Proceedings ACM's Symposium on Usable Privacy and Security held at CMU, 2006.

NFC, Java Card, and Certification

Éric Vétillard and Guillaume Dufay

Trusted Labs – 5, rue du Bailliage, 78000 Versailles, France
eric.vetillard, guillaume.dufay@trusted-labs.com

Abstract One of the applications of the NFC interface on mobile phones is the dematerialization of smart card applications, using NFC's card emulation mode. We here address the security aspects of this dematerialization, in particular relatively to the security of open smart card systems, and on the certification of the smart card platforms and applications. We present the work done in the past years at Trusted Labs to identify novel ways to certify cards and applications in the context of a NFC deployment, in particular by using composition of certifications in new ways.
Keywords : NFC, Java Card, GlobalPlatform, Security certification, Common Criteria.

1 Introduction

One of the promises of NFC on mobile phones is to allow smart card applications to be dematerialized, allowing a mobile phone to be used as a payment card, a transport card, or a student card. Technically, the infrastructure has been ready for years. The Java Card specification provides a programmatic foundation to build portable applications, and the GlobalPlatform specification provides a highly flexible platform for the management of card applications, even in configurations that involve several application providers that don't trust each other. There are nevertheless a few important questions that need to be addressed, and that have proven problematic :

- On the technical side, an important question is to decide where the dematerialized card applications will reside : on the SIM card, controlled by the network operator, on a secure element embedded on the phone, controlled by the manufacturer or one of its partners, or on a removable secure element, controlled by any issuer.
- On the business side, there remain some difficulties to be addressed on the business model that manages the relationship between various application providers who have always issued their own cards in the past, and now need to find a way to share the costs and revenues of a single deployment, and to find an appropriate way to manage branding issues.
- On the security side, there is a similar problem, as application providers from different sectors (telecom, banking, transport) have implemented very different risk management strategies in the past, and have very different approaches to the security of cards, in particular regarding their certification.

The two last issues are not directly related to NFC, as they would apply equally to any situation in which multiple applications, from several different application providers, need to be installed on a single card, controlled by a single issuer.

The present paper focuses on the security aspects, on which Trusted Labs has worked over the past years in different contexts, as consultants for our customers, and also as partners in collaborative R&D projects.

Part of the work presented here has been performed in the context of consulting work for the *Payez Mobile* association, which focuses on mobile payment and involves all three French mobile network operators, as well as some of the largest French banks.

The EPOMI [1] collaborative project focuses on the certification of sensitive mobile applications, such as mobile payment, ticketing, and mobile television. The project joins all actors involved (financial institutions, mobile operators, certification authority, consulting firms) in an attempt to define the most appropriate way to certify the security of applications over time in the context of a NFC deployment. Since the applications considered are often considered as those that requires the highest level of security, these results could be reused in many other circumstances. Preliminary results from the EPOMI project are also considered in the present paper.

In the rest of this paper, we will first define precisely the issues that we need to face, then describe some solutions that have already been proposed, regarding in particular the use of composition in the certification of Java Card applications, and we will finally describe the ongoing work, and the challenge that needs to be addressed in the near future.

2 Security certification in the context of NFC

Java Card has been introduced over then 10 years ago, and it has since then become the dominant application framework on smart cards. In particular, Java Card is present on a large proportion of SIM cards, over 90

This may surprise some people, but there have been very few deployments so far of smart cards that carry several applications from several application providers. Although the technology has been ready for a long time, NFC is the first compelling use case for such deployments, and it forces all the actors to finally address the issues related to these deployments, in particular regarding business models and security. We here focus on security, and we will look at two of the major issues, which are the lifecycle of cards and applications, and their security certification. We will compare the approaches taken in various industries, and then suggest some leads for possible solutions.

2.1 Card lifecycle

The card lifecycle of banking cards is very well-defined. All banking cards are certified (for instance by Visa and/or MasterCard), both functionally and security-wise. The certificates are valid for a given period (for instance, three years), during which the vendor can sell the cards to issuing banks. Then, once a card is issued, it is only valid for a limited

1. The EPOMI project is a collaborative research and development project, partially funded by the French government, and sponsored by the E-Secure Transactions cluster.

time, usually two or three years for smart cards. The objective for all these delays is to ensure that cards are withdrawn before their security is made completely obsolete by new attacks.

The situation of SIM cards is quite different. Every operator defines one or several card profiles, which defines the options that it wants to be implemented on the cards. The operator then validates that the cards proposed by vendors correctly implement their profile(s), but the acceptance process rarely includes any security testing. In addition, SIM cards usually don't have an expiration date, and many SIM cards in use today have been issued 5 to 10 years ago. SIM cards are most often changed when users change operators, or when they want to use a feature that their older card does not support (for instance, 3G networks).

Another difference is that the telecom specifications evolve rather fast. Vendors often develop a new range of products every year, or at least significantly update their product line every year. This contrasts sharply with other industries, where specifications remain stable over many years, and products are developed

2.2 Security certification

Security certification is an old and mandatory part of the acceptance process in sensitive application providers, whereas it is often overlooked by telecom operators. There are also significant differences even between sensitive application providers in the way they certify applications.

For instance, there are significant differences between the practices of the financial industry (i.e., EMVCo), and the practices of the transport or pay-TV industries or of government agencies. Despite these differences, all these applications are potential candidates for dematerialization in NFC mobile phones.

There are here three levels of issues :

- Application security. All sensitive application providers define requirements for the implementations of their applications, but there are significant differences in the certification processes that they put in place.
- Platform security. Some application providers impose security requirements on platforms, in particular regarding the management of applications and the isolation between different applications. In most cases, these requirements are not explicitly defined, and they are a consequence of more general application-level requirements.
- Other applications' security. Some application providers have requirements that need to apply on other applications, in particular regarding the way in which applications can collaborate.

The issue of application security is easy to address, since every application provider is free to impose any certification process to its developers and partners. The issue of platform security is more difficult, since additional security countermeasures come at a price, and vendors that do not require these features may be reluctant to pay for the additional cost.

Finally, requirements on other applications can be extremely problematic, since they can force an application to be evaluated every time another application is deployed.

Of course, negotiations are happening around the various industry consortia and ongoing experiments. For instance, on the platform side, the model is evolving toward a secure space rental model, that would allow telecom operators to get some revenue from the presence of sensitive applications, and would therefore justify the deployment of a more secure platform. As a consequence, a consensus is also appearing about the required security level for this platform [1,3], since the EAL4+ (augmented with AVA-VAN.5, in order to take into account attackers with a high attack potential) certification level seems appropriate for banking applications, as well as for most other sensitive applications.

3 Composition of certifications

3.1 Certification costs

The security certification of a smart card and its applications can become very expensive if a significant number of options need to be taken into account. In such a case, the typical requirements in terms of certification in the Common Criteria framework are as follows :

- Evaluate the chip on which the smart card operating system needs to be implemented.
- Evaluate the card's operating system, typically as an open system (to which applications can be added, even after issuance).
- Evaluate the applications that need to be, independently of one another.

In practice, an operating system cannot be evaluated independently of the chip it is implemented on, because it depends on its security features. Similarly, an application can only be evaluated together with its underlying operating system and chip, in order to make a complete product (called a composite product).

This problem becomes really costly if we start taking into consideration its combinatorial aspects. If you consider as an example that a sensitive mobile application needs to be certified in France, with 3 operators, and an estimated 3 SIM platforms per operator. Even if some of these SIM cards come from the same vendor, they will use sufficiently different configurations to justify a different certification for each one of them. This represents nine (costly) certifications, which will have to be renewed every time a new version of the platform or of the application is released.

Chips that host secure operating systems usually go through a Common Criteria certification, and composition is very often used between a chip and an operating system [2]. This actually leads to some simplifications in the evaluation of the second product (operating system on an already evaluated chip), since some of the attacks are not reproduced. In particular, the attacks that target the hardware directly, such as probing, are only performed during the chip's evaluation.

As of today, the composition model is less often used for the composition of an application with an operating system embedded on a chip. The classical attacks (observation, fault

induction, etc.) are performed on the operating system, and then again on the application, with little reuse of the previous results, and more importantly, with no reduction in the evaluation time (and cost).

This can be greatly enhanced by considering the fact that an operating system usually exposes an API that provides access to its security functions (cryptography, authentication). This API can be thoroughly tested during the operating system's evaluation. These basic operations then do not need to be tested again, and the application's evaluation can focus on the security features that have been added in the application itself.

Let's consider a simple example. A platform includes an implementation of a cryptography algorithm that is sensitive to DPA, but only with 100,000 samples or more. An application built on this platform includes a specific countermeasure to fix that vulnerability by adding a counter that limits the overall number of operations to 10,000 (10 times less than the limit above).

An evaluator of the application should focus first on the counter, and try to break this mechanism in order to be able to perform at least 100,000 samples of the cryptographic algorithm. In case of failure, there is no point in performing the DPA attacks on the algorithm. Only in case of success is it interesting to combine both attacks, in order to verify that they remain possible when combined.

Ultimately, the objective is to go even further, and to define a way to make the security of SIM platforms interoperable, which is covered in ğ3.3.

3.2 Adapting the certification of applications to requirements

By default, when a security product is certified in the Common Criteria process, its entire code base needs to be evaluated. However, in a NFC smart card product, all applications may not have the same requirements in terms of security. Some applications are sensitive, because they manage sensitive and valuable assets, and they need to be fully evaluated (e.g., payment applications). Some other applications are non-sensitive, because their assets have a limited value, and they don't need to undergo a specific evaluation. However, since these applications need to be integrated into the product, they may be part of an attack path, and some kind of evaluation is required.

The main difference between these two kinds of applications lies in the security properties that need to be proven. For non-sensitive applications, our objective is to prove that they are innocuous to other applications, and to the underlying platforms. For sensitive applications, in addition to that objective, we also need to prove that the application adequately protects its assets. This is a very significant difference, because the second property is application-specific (it depends on the specific assets and on the specific functions of the application), and it will require a specific certification. On the contrary, the first property is generic (the same property needs to be proven on all applications, regardless of their specification), which means that the same standardized evaluation can be applied to all non-sensitive applications.

In the Protection Profile that has been defined by the French mobile operators for the *Payez Mobile* project, we have proposed a set of generic, restrictive rules for non-sensitive applications, which have also been submitted for use in the context of the EPOMI project. The rules remain quite simple :

1. The binary code for these applications needs to be verified in order to be accepted.
2. The application code must not be a library, and it must not use object sharing, neither as a client nor as a server.
3. The use of a few specific API's is explicitly forbidden in non-sensitive applications.
4. The application must declare the features and algorithms that it uses.

Our objective is to define a minimal set of requirements that allow a non-sensitive application to be loaded on a trusted platform, while guaranteeing that this application is not able to attack the sensitive applications on the same platforms. In addition, this set of requirements has been built in a way that allows us to automate the proof.

To this purpose, we use a static analysis tool built internally at Trusted Labs [6], which is able to prove properties on CAP files, i.e., on applications in their binary form, which can then be signed. For the rules stated above, such a tool is rather simple to build on the basis of a standard bytecode verifier. In terms of isolation, only rules 1 and 2 are really important ; rules 3 or 4 are secondary rules that may be used to enforce specific issuer or application provider rules.

Rule 1 makes bytecode verification mandatory. In the context of Java Card, bytecode verification cannot be performed on a single file, because part of the binary file linking is performed before the verification. This means that the bytecode verification process must include some linking information (included in the Java Card export files) that corresponds exactly to the libraries that are deployed on the actual card. If the file differ, even slightly, it becomes possible to perform logical attacks, as demonstrated by Lanet and Iguchi-Cartigny. [4]. We have developed a methodology to perform such verification, which guarantees that logical attacks based on linking cannot be applied, by ensuring that the bytecode verification is always performed in the appropriate context. This rule will actually need to be applied on all applications, sensitive or not, in order to ensure the type safety of the card.

Rule 2 is here to prove that the application is not allowed to share any data with another application in any way. In Java Card, this is quite simple to do, because the applications are separated by a firewall, whose effect is roughly equivalent to the use of different class loader for each application. Hence, there are only two ways to share data : either through static fields defined in shared libraries, or through a Shareable interface. By forbidding them in a rule, and by proving through static analysis that all non-sensitive applications obey that rule, we can be sure that data sharing is not accessible to these applications.

In practice, we need to allow a limited amount of sharing, because shareable interfaces are actually used in standard APIs. For instance, the ToolkitInterface implemented by all SIM Toolkit applications, or the SecureChannel interface that provides access to secure messaging through an application's security domain, are both shareable interfaces, whose use

must be allowed. However, by strictly limiting the use of these interfaces to the requirements of the application framework, the isolation between application remains guaranteed.

Of course, there are limitations to this technique. First, any application that needs to collaborate with another application through shared code and data has to be considered as a sensitive application, and therefore undergo a costly and long formal security certification. We still hope that many applications will fall in the non-sensitive category, especially among the rather simple SIM Toolkit applications that are often deployed on SIM cards. Another limitation is that the automated verification only guarantees a few type safety and isolation properties ; the issuer still needs to verify through other means that the application does not use too much resources. Static analysis can be used to prove that memory consumption is limited on many applications, but its results are limited as soon as generic personalization commands are used, since these commands may actually allocate any amount of memory.

3.3 Evaluating applications independently of the platform

The next step is to evaluate the applications independently of the underlying software platform, or at least to maximize the part of the evaluation that can be mutualized between two different applications. In a recent evaluation performed by Trusted Labs on behalf of Trusted Logic and SFR, we have demonstrated a first step. If a card is certified at a given level with the ability to load applications on it, it is possible to keep the same certification level after adding a new application (post-issuance). This results from the certification work described above, and it applies both to non-sensitive applications (after proving that they satisfy the verification and isolation rules), and to sensitive applications, after certification at a suitable assurance level.

The next step is here to demonstrate that Java Card applications can be portable from one platform to another, not only at the functional level, but also at the security level. In order to achieve this portability, the applications need to be built on top of a platform that is well-defined in terms of security, and that includes the basic security functions required by the applications.

The Java Card and GlobalPlatform specifications only define this platform partly, as they are missing two important things :

- No security items are defined for security functions like cryptography and authentication.
- Some features are missing in Java Card, such as the ability to manage counters securely, and to manage generic secure storage.

The missing items are currently being built, in the context of the EPOMI project. One of the project's objectives is to define an interoperable security layer on SIM platforms. This can be achieved by adding a few security measures to these platforms, and most importantly, by submitting all security functions in the platform to the same security testing. Subsequently, the usage recommendations associated to all platforms certified through this process should be the same, with the objective of modifying the distribution of security objectives between

the application and the platform. The more common security measures are added to the platform, the easier a new sensitive application will be certified.

4 Ongoing and future work

4.1 Card software maintenance

As we have seen in the lifecycle description, SIM cards are usually deployed for a long time, much longer than other cards. In addition, by putting several applications on the same card, we increase the risk that at least one of the applications becomes vulnerable after some time. This issue raises two major questions :

– How to know when an application has become vulnerable ?
– How to fix the vulnerabilities of an application without changing the card ?

The first question needs to be answered jointly by the card issuer and the application provider, by agreeing on periodical security "check-ups" of the platform and its applications. In most cases, we should even be able to identify vulnerabilities early enough to take the time to fix them properly. For instance, the possibility of performing combined logical-physical attacks has recently been made public [5]. Such attacks may allow an attacker to use verified applications to perform illegal operations, in ways that still need to be clarified. The static analysis rules may then be updated to consider these new attacks, and all applications can be analyzed again in order to verify that they do not contain any offensive code.

The second question is more difficult. In purely technical terms, the update of card applications and card system software is difficult, but far from impossible. Platform and application updates are routinely performed on larger systems, and while this feature adds a few security issues to be addressed, there is a clear potential gain in adding such a feature. On smart cards, the fact that such an update is likely to happen over-the-air remains an innovation, which has an impact on security issues.

Performing such updates raises some issues about the security certification of the platform and its applications. When updating an application, a re-evaluation would be required in order to keep its certification valid ; and when updating the platform, a re-evaluation of the platform and of all its applications would be required in order to keep their certifications valid. Mobile payment increases the importance of this issue, since SIM cards are not replaced as regularly as payment cards. The maintenance of the applications' security certifications represents a significant cost, and the EPOMI project is exploring some options in order to decrease that certification cost related to maintenance.

4.2 Interaction models on NFC phones

In pure card emulation mode, a NFC application is the exact equivalent of a contactless smart card application, which doesn't allow any interaction with the end-user. However, since NFC applications run on a mobile phone, it is very tempting to leverage the presence

of a screen and keyboard to allow the end user to interact with the application in new ways (for instance, to check a balance, or the status of a subscription).

There are many ways to implement such interactions with mobile phones :

- SIM Toolkit applications. Such applications reside on the smart card, and they provide a basic interface that is supported on most phones.
- Smart card-based Web applications. This technology is only emerging today, but it can be seen as the successor of SIM Toolkit : a technology that allows the interaction to be defined on the SIM card, using an interface (in that case a Web browser) that is supported on most phones.
- Mobile applications. This technology is specific to every mobile application framework and/or mobile operating system, but it allows the development of highly interactive applications, tailored to the specific mobile platform.

In all cases, and in particular in the last case (where the interaction is entirely controlled from the phone), the security of the interaction depends on the security of the mobile phone. This leads to a difficult problem, mostly due to the complexity of a mobile phone (large amount of software, usually combined from many developers and vendors). Standard certification schemes, such as those used for smart cards or for payment terminals, cannot be readily applied on phones, and we are looking for innovative solutions.

This issue does not need to be addressed immediately, because mobile phone interactions remain hard to attack (practically) today. However, as the value of the assets managed through such interactions grow, the level of risk will increase, and some kind of security certification is likely to become a requirement.

5 Conclusion

The introduction of NFC puts the issues related to the management of applications from several providers on a single card in full light, in particular regarding security. We have seen that the difficulty comes from the different practices in the various vertical industries that issue smart card applications, and that there are ways to reduce the costs associated to security certifications of complex smart card products. Such issues are in fact often closely related to the business models that can be identified, since the costs associated to security certifications are high, and they can undermine the feasibility of a project.

The industry is moving toward interoperability at the security level, and there are several efforts, in particular between the financial and the telecom industries, whose goal is to define interoperable security features or certification schemes.

The next challenges will be to work on the certification process itself, in order to reduce their cost significantly. For some applications, the issue of interaction models will also need to be addressed.

References (partial)

[1] Sun Microsystems. *Java Card System Open Configuration Protection Profile, Version 2.1*. To be certified in October 2009.

[2] CCDB, *Composite product evaluation for Smart Cards and similar devices*, September 2007, Version 1.0 - Revision 1, September 2007, CCDB-2007-09-001

[3] SFR, (U)SIM Java Card Platform Protection Profile *Evolutive Certification Scheme for (U)SIM cards*, June 2009, currently in evaluation.

[4] Jean-Louis Lanet and Julien Iguchi-Cartigny. *EMAN Attack : a Trojan in a Smart Card*. Presented at CESAR'08, Rennes, 2008. Available from `http://www.msi.unilim.fr/~lanet/upload/Cesar2008-pub.pdf`.

[5] Guillaume Barbu. Fault Attacks on Java Card 3.0 Virtual Machine. Presented at e-Smart 2009. September 2009.

[6] Éric Vétillard and Renaud Marlet. Automated Enforcement of Portability and Security Policies. Proceedings of e-Smart 2003 Conference, Sophia Antipolis, 2003

Troisième partie

Security in Wireless Sensor Networks : A Military Perspective (Invited talk)

Konrad Wrona

NATO C3 Agency, Oude Waalsdorperweg 61
2597 AK The Hague, The Netherlands
Konrad.Wrona@nc3a.nato.int

Keywords : Wireless sensor networks, security, military applications, multi-level security.

Extended Abstract

Wireless sensor networks (WSN) and RFID technology gain increased importance in the military environment. Situational awareness and informational superiority are important elements of the modern military doctrine - the network centric operations [1]. Both WSN and RFID are critical technologies for enabling this capability.

The main objective of using WSN and RFID in military systems is to provide so-called information superiority [2]. Information superiority derives from the ability to create a relative information advantage vis-à-vis an adversary. The typical applications where use of WSN and RFID can offer information superiority include logistics, force protection and combat assistance [3]. Example of current NATO projects related to remote sensing and tracking include perimeter monitoring and convoy tracking in Afghanistan. DARPA sponsors several projects related to use of sensor networks in military applications [4].

Use of sensor networks and RFID technology in military environment introduces several challenges. In addition to high reliability and environmental resistance, the military systems, especially deployed in areas potentially controlled by an adversary, have to provide an adequate level of tamper resistance or tamper evidence. The communication links, especially wireless channels, have to be adequately secured, too. The system has to be easy to deploy, operate, maintain and recover from possible faults and attacks. And, finally, the solution has to be easily integrated with the existing military systems.

One of the fundamental challenges in military communications and information systems (CIS) is dealing with different security classification levels of information. Most of the current military systems operate according to Bell-La Padula security model [5]. An extra care has to be taken when designing information flows within the system in order to meet the relevant organizational security policies. In particular, a flow of information from "low" domain (e.g. unclassified network of sensors) to the "high" domain (e.g. secret network including intelligence analysis system and repository of historical data) requires enforcement of a one-way information flow, e.g. by using a data diode [6]. However, use of such one-way communication device implies also that no control information or queries can be sent

back directly from the secret network to the sensors. Simple solutions, such as including sensor network itself in the secret domain are not practical because of the cost and technical constraints.

Discussion of classification of information leads also to an interesting question concerning when the data collected by sensors becomes a classified information. As the raw data collected by sensor nodes can be in most cases sensed by anybody, including the enemy, it is often regarded as unclassified information. Therefore both sensors and communication channels between and from the sensors do not need to meet the strict requirements on security of classified CIS, which would be difficult to meet due to the technological limitations. However, the aggregated or processed data is often regarded as classified, which implies that sink nodes or systems performing in-network processing might be regarded as classified, too.

Another interesting question is a definition of a term "sensor network". Typical WSN scenarios studied in academia, assume a large scale distributed network of tiny autonomous devices. This challenging environment provides an interesting platform for identification and investigation of many new research issues and can lead to interesting practical solutions in the future. However, most of the currently deployed military sensing systems rely on much bigger sensors and much more centralized communication topologies. In fact, the term "sensor network" is often used in military environment in order to describe an interconnected system of radar stations and other long-range sensing instruments.

One of the important challenges that have to be addressed before the WSN gains widespread acceptance in military applications is that the currently proposed WSN architectures often do not provide adequate security. Wireless sensor networks face some usual security threats, including threats to confidentiality, integrity and availability [7]. However, the constraint resources available to the nodes make addressing these threats a challenging task [8]. The spectrum of the technical security issues introduced by the classical WSN scenarios is extremely wide, ranging from physical security of the nodes through light-weight cryptographic mechanisms [9] and efficient security protocols to secure data aggregation [10] and secure integration into context-aware applications [11]. The highly distributed character of the WSN has also an important impact on choice of security mechanisms which are suitable for securing communication and data processing within in the network. Interestingly enough, although the distributed character and the large scale of sensor networks may be an obstacle for using some well-known security mechanism, e.g. used in the Internet, at the same time these characteristics open opportunities for developing new approaches to security. The possible approaches include relying on redundancy of evidence and on limited ability of an attacker to gain control over substantial number of nodes or to monitor the substantial amount of communication exchange between nodes.

The security in WSN is an important R&D topic, which is not only critical for enabling real-life applications of sensor networks, but also allows us to better understand limitations of existing security mechanism and fosters development of new, more efficient, alternatives.

Despite of substantial amount of research performed in this area in the recent years, many of the security problems are still open and provide interesting area for further investigation.

References

1. Alberts, D., Garstka, J., Stein, F. : Network Centric Warfare : Developing and Leveraging Information Superiority 2nd edn. CCRP Publication Services (1999)

2. Alberts, D., Garstka, J., Hayes, R., Signori, D. : Understanding Information Age Warfare. CCRP Publication Services (2001)

3. Winkler, M., Tuchs, K.-D., Hughes, K., Barclay, G. : Theoretical and Practical Aspects of Military Wireless Sensor Networks. In : Proceedings of the Military Communications and Information Systems Conference, Bonn (2007)

4. Volgyesi, P., Balogh, G., Nadas, A., Nash, C., Ledeczi, A. : Shooter Localization and Weapon Classification with Soldier-Wearable Networked Sensors. In : Proceedings of the 5th International Conference on Mobile Systems, Applications, and Services (MobiSys), San Juan, Puerto Rico (2007)

5. Bell, D. : Looking Back at the Bell-La Padula Model. In : Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC 2005) (2005)

6. Tenix Datagate Inc : Interactive Link Data Diode Device. Common Criteria Security Target Doc. No. 9162P01000001, Issue No. 5.1, National Information Assurance Partnership (NIAP), Virginia (2005)

7. Kim, M., Lee, Y., Ryou, J. : What Are Possible Security Threats in Ubiquitous Sensor Network Environment ? In : Managing Next Generation Networks and Services - Proceedings of the APNOMS 2007, Sapporo, Japan, vol. LNCS 4773, pp.437-446 (2007)

8. Liu, D., Ning, P. : Security for Wireless Sensor Networks. Springer (2007)

9. Eisenbarth, T., Kumar, S., Paar, C., Poschmann, A., Uhsadel, L. : A Survey of Lightweight-Cryptography Implementations. IEEE Design and Test of Computers 24(6), 522-533 (2007)

10. Sorniotti, A., Gomez, L., Wrona, K., Odorico, L. : Secure and trusted in-network data processing in wireless sensor networks : A Survey. International Journal of Information Assurance and Security 2(4) (2007)

11. Compagna, L., Lotz, V., Wrona, K. : Towards adaptive security for ubiquitous computing systems : MOSQUITO and Serenity. In Mühlhäuser, M., Gurevych, I., eds. : Handbook of Research on Ubiquitous Computing Technology for Real Time Enterprises. Idea Group Publishing (2008)

A Distributed Intrusion Detection System for Wireless Sensor Networks

Lionel Besson, Philippe Leleu

Thales Communications France
Colombes, France

Abstract Wireless sensor networks (WSN) are low-cost solutions that can be used in a variety of application areas. However, they are highly susceptible to attacks and it is very probable that an intruder catches already existing security measures out. AWISSENET (Ad-hoc personal area network & WIreless Sensor SEcure NETwork) is a project funded by the European Union Information and Communication Technologies Program that is focused on security and resilience across ad-hoc personal area networks and wireless sensor networks, and provides a security toolbox for trusted route selection, secure service discovery and intrusion detection. This paper deals with intrusion detection systems for WSNs and how it is used in the AWISSENET project.

1 Wireless Sensor Networks and security

1.1 Introduction

An ad-hoc wireless sensor network (WSN) is a network composed of a large number of low-cost and simple devices called sensor nodes which are monitoring physical or environmental conditions like temperature, sound, pressure, etc. and using the wireless radio to communicate these measurements to a base station. They are used in a many military and civilian application areas, including emergency response, medical monitoring, homeland security and environmental monitoring. The open and distributed nature of the network, and the limited resources of the nodes make WSNs highly vulnerable to attacks. We first introduce the attacker's goals and define a set of security requirements for such networks. We then explain how security solutions are usually provided to WSNs, and the need for intrusion detection systems (IDS) to act as a second line of defense when the other techniques are deceived by a successful intruder. Finally, we present the internals of IDS for sensor networks, and how it is implemented in the AWISSENET project.

1.2 Attackers goals

The attacker goals regarding WSNs can be multiple, depending on how easy it is for him to launch an attack, and the kind of damages he wants to inflict to the network. Moreover, some attacks can be seen as early steps to wider attacks that rely on some prerequisites.

Overhearing data is probably the most evident goal. Retrieving sensitive data is very easy if communications are not or weakly encrypted. Even when they are, patterns in

communications can be used by traffic analysis in order to locate the critical nodes of the network [9]. Rate monitoring attacks use the packet-sending rate to determine the possible location of the base station (the closer a node is from the base station, the higher the sending rate). In a time correlation attack, the correlation in the sending time of packets is used to determine the paths of the network and deduce the important nodes of the network as the preferred destination of these paths.

Injecting fake data consists in sending false information to the network that will be taken as legitimate. Fake information can simply be related to the sensor values (for example, one could use temperature measurements to lure the firemen to a wrong place where there is no fire), or used to trick some of the internal mechanisms of the sensor network (like introducing routing loops by advertising inexistent links).

Reduce the performance of the network can be easily achieved by exhausting the scarce network resources, such as energy or bandwidth. It is usually achieved by sending a large amount of packets that will either force the network to drop some packets because it is not able to treat them all, or initiate processes that will consume a lot of power (The radio chip is itself the module that consumes the most energy).

Breaking parts of the network links is used to hide some parts of the area covered by the network from the base stations. For example, an attacker can break into the network, send false routing information in order to be seen as a routeur for a whole set of nodes, and then refuse to forward traffic, thus creating a network partition. This attack is known as the black hole attack.

Damaging the whole network operation is the most damaging, but also the less discreet goal of an attacker. If such goal is achieved, the network is unable to fulfil its primary role (sending sensor values to the base stations) and thus becomes useless. Due to the ad hoc nature of WSNs, this is usually achieved by attacking the routing protocol.

1.3 Security requirements

Regarding previous paragraph, we can define a list of security requirements that a secure WSN should fulfil :

Robust and reliable network. The impact of attacks should be minimized, so that the compromise of a small set of nodes should not break the entire security of the network.

Data authenticity is making sure that messages have been sent from a valid source.

Data integrity ensures that data has not been altered while in transit by an adversary. It is a critical point for WSNs, since a message will be routed by many nodes without any control on them.

Data confidentiality is keeping information secret from unauthorized parties. This is usually done by encrypting communications, but traffic analysis attacks should also been taken into account.

Data freshness is needed to avoid replay attacks. Replaying old messages is very easy when considering WSNs. For example, one could capture authenticated link broadcasts and

replay them once the topology of the network has changed, thus breaking the routing rules. Timestamp mechanisms are usually used to ensure that a message has been forged recently.

1.4 Securing Wireless Sensor Networks

They are two main approaches for securing a WSN : adapt the existing protocols to counter the possible attacks, or use security frameworks that provide security functions like authentication, integrity, confidentiality or timestamping mechanims.

Securing existing protocols makes it easier for using in different environments, since you don't have much integration work to do. However, you need to consider the security of each protocol your network relies on in order to achieve the global security of the network. The secured version of the AODV protocol (SAODV, [13]) is a good illustration of such an approach.

Security frameworks aim at providing a generic security package that covers the basic security needs for WSNs and can be integrated into sensor network applications. They require having each protocol deployed in the network being able to use the framework. Secure sensor link layer protocols such as TinySec [10], ZigBee [11] or MiniSec [12] enjoy significant attention in the community.

As presented in the introduction, the open and distributed nature of communications of WSNs make it impossible to concentrate all security functions in a central point, so that each node of the network needs to execute several security functions. Combined with the limited resources of sensor nodes, this requires to carefully considering the cost of the security mechanisms that are deployed. As a consequence, it is very probable that a node gets compromised at some point. Intrusion Detection Systems for WSNs act as a second line of defense. Their role is to detect attacks before they are successful and compromise the security of the network, and to expel intruders and compromised nodes from the network.

2 Intrusion Detection for WSNs

2.1 Specificities and challenges

IDS for sensor networks differ in many ways from the one used in legacy networks. The challenges that IDS have to take up in the particular field of WSNs include :

- *Automated decision* : nodes must be truly autonomous and adapt to the evolution of the network and environment.
- *Limited resources* : security functions must take into account the scarce bandwidth, memory, energy and computational power.
- *Localize auditing* : a node can only see what is happening in its immediate neighborhood.
- *No node is trustworthy* : nodes can be quite easily compromised, and should not be trusted.

– *Distributed IDS* : intrusion detection must happen on several nodes in order to detect distributed attacks.
– *Security of the IDS itself* : malicious nodes should not be able to deceive the IDS.

In the following sections, we introduce the internals of IDS for WSNs and detail the specific case of the AWISSENET distributed intrusion detection system.

2.2 Network Architecture

Usual IDS are typically *stand-alone IDS*, where each node runs an independent intrusion detector. This is particularly true for network-based intrusion detection systems, which often consist in a powerful server located in the demilitarized zone or at network borders, and thus are able both to capture all network traffic and to analyse the content of individual packets for malicious traffic (Fig. 1). Such systems cannot perform satisfyingly in WSNs, since local audit data are not enough to have a good comprehension of what is happening in the network. Cooperation between the different nodes is compulsory in order to achieve efficient detection, because local evidences are often inconclusive. They are three main network architectures that can be found in the literature.

Hierarchical IDS are systems where specific nodes are in charge of monitoring their neighbours, with various level of cooperation between cluster heads, as presented in [1]. They are particularly suited for multi-layered network architectures.

Distributed IDS meet the decentralized nature of ad-hoc wireless sensor networks, where each node is responsible for collecting local audit data, and share this knowledge globally in order to carry out a global intrusion detection system [2] [3].

Finally, *Mobile Agent Based IDS* use pieces of mobile code charged with a specific mission and sent to other nodes. Depending on the system, the mission can be to analyse the local audit data of other nodes and bringing back the results to the originator [4], or to run a specific attack detection on a node in order to distribute the detection tasks amongst the network [5].

The AWISSENET architecture is a hybrid one between the hierarchical and the distributed approach. Only a subset of the AWISSENET nodes run intrusion algorithms, in order to cope with the heterogeneity of the network and maximize the detection efficiency / resource cost ratio. The network is partitioned into several multi-hop clusters, each one having a node with a specific role (the cluster head). Inside each cluster, and at the global level between cluster heads, we use a distributed architecture. The intrusions detections and assumptions, and the other IDS messages are exchanged inside a cluster, and the cluster members cooperatively take the decisions. The cluster head is then responsible for iterating the same process at the global network level. This approach enables more scalability, since having a completely distributed IDS would flood the network when they are too many nodes. It also minimizes the drawbacks of the hierarchical architectures by introducing a high cooperation between the nodes.

Clusters are statically determined when the network is deployed, taking into account several parameters, like the number of nodes able to run an IDS agent, the repartition of the IDS nodes, the topology of the network, or the mobility of the nodes.

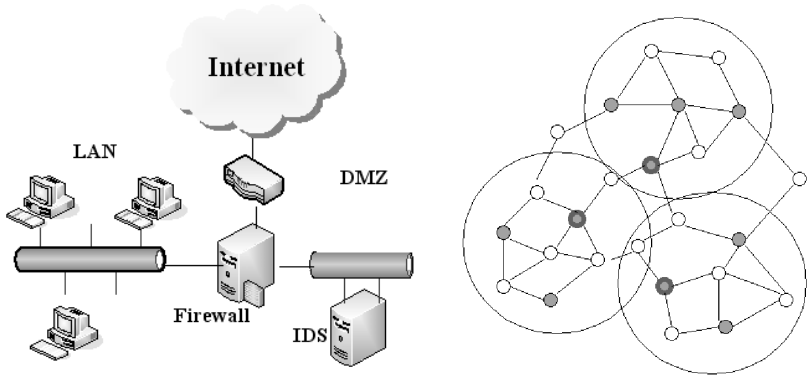


FIGURE 1: The left figure presents a typical IDS use in a classical infrastructure network. The right one illustrates the nwetwork of the AWISSENET distributed IDS. Gray nodes are IDSs, circled ones are cluster heads.

2.3 Collecting Audit Data

Audit data are collected by local agents analysing local sources of information, which can be hardware or network based.

Physically manipulating a sensor node to retrieve cryptographic material like the keys used for encryption on the network, or to reprogram it are two examples of attacks that can be detected by monitoring the hardware. The devices can implement anti-tamper mechanisms or watch for abnormal sensor values (like accelerometer) in order to detect such attempts and declare themselves as about to get compromised.

However, using the vulnerabilities of software (and especially the routing protocol) is often a simpler and easier way for an attacker to break into the network. Thus, the role of the distributed IDS is to analyze the overheard traffic and look for suspicious patterns. Due to the ad-hoc nature of the network, a single node has only a partial knowledge of what is happening. Luckily, nodes do not only have access to the packets sent to them, but can also overhear traffic passing between neighbouring nodes and act as "watchdogs" (Fig. 2). This gives the possibility to detect abnormal behaviours even if the node isn't directly involved in the attack. For example, watchdogs can detect nodes forwarding selectively packets, or modifying them, but also gather metrics about distributed attacks, like nodes flooding the network with route replies [6].

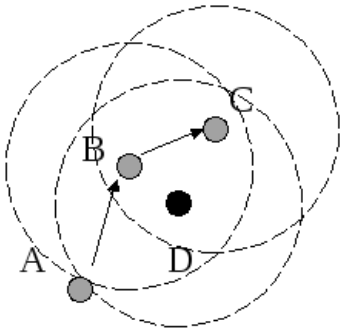


FIGURE 2: Example of a spontaneous watchdog : node D can see if B is forwarding correctly the packet from A to C

2.4 Intrusion detection

IDS need to distinguish between normal and abnormal activities in order to detect attacks against the network before they are successful. Detection techniques are usually classified into three categories.

Misuse detection (also known as signature-based detection) consists in comparing audit data with known attack patterns. This technique is the one mainly used for classical IDS, but is not widely suitable for WSNs, since the (many) patterns that must be stored in the system and the expensive comparison algorithms will soon exhaust the node resources. Moreover, misuse detection suffers from a lack of flexibility and is useless when trying to detect previously unknown attacks.

Anomaly detection systems describe the 'normal' behaviour of the network and detect any activity that differs significantly from it, and are thus potentially capable of detecting new attacks. The normal behaviour is usually established via automated training [7].

Specification-based detection is similar to anomaly detection, but the correct behaviour of the network is manually defined. It allows a smaller rate of false alarms, but the development of detailed specifications is difficult and makes it less flexible to the different environments.

Depending on the context (for example which routing protocol is used, or the services deployed in the network) and the capabilities of the heterogeneous nodes, different intrusion detection algorithms can be used in order to offer the best ratio between detection efficiency and resources consumption. The AWISSENET distributed IDS proposes a plug-in based architecture in order to enable an easy and flexible management of the algorithms running on each node, which can be of any of the three kinds of detection techniques aforementioned.

A data manager is used for collecting, storing and centralizing data and metrics used by the different plug-ins, thus avoiding useless computations and resource waste.

2.5 Decision Making and Recovery

Once a local IDS agent has raised an alarm internally, the next question that arises is who is going to make the final decision that a node is effectively an intruder and which action should be taken. *Independent Decision-making Systems* are usually used in cluster-based architectures because they leave the decision that a node is effectively an intruder to specific nodes (usually the cluster heads) [1]. The alternative solution is called *Cooperative Intrusion Detection Systems*. When an attack seems to have been detected, the node appeals to neighbouring nodes in order to output a global decision. This is often done via a voting mechanism.

The AWISSENET IDS uses its hybrid architecture in order to output a global decision on the status of a node. Alerts raised by the local IDS agents can express, depending on the algorithms, the certainty to have detected an intrusion, or only the assumption that something abnormal is happening, with inconclusive evidence. Leaving the decision to a single node would imply a high rate of false positives and false negatives, because the data collected locally is often not enough to output an appropriate intrusion detection decision. The cooperation between the nodes aims at sharing the audit data and the algorithms conclusion in order to correctly detect intruders at the network level.

The nodes belonging to the cluster share these alerts, and a voting mechanism is launched to output a decision at the cluster level and decide whether the alert should be forwarded to the network level or not. The same knowledge sharing and voting mechanism is used between the cluster heads to output a global decision at the network level. This decision (which can be the identification of an intrusion and / or an intruder, or simply a false alarm) is sent back to the nodes by the cluster heads. The intruder is then isolated from the network via the routing module, and if needed, cryptographic material is updated.

2.6 Secure IDS exchanges

As the decisions taken by the IDS can expel a node from the network, it should be very careful not being compromised, and needs to ensure the integrity of the messages exchanged between the nodes and that they are sent by legitimate ones.

The AWISSENET DIDS uses timestamps and digests to secure the communications between the IDS agents, which are inspired by the secure OLSR plug-in [8]. Secret keys are shared inside each cluster and between the cluster heads and used to produce and check the digests of the messages. Timestamps are used to determine the freshness of the messages and prevent replay attacks. In order to securely synchronize (or re-synchronize if needed) clocks between two nodes, an exchange of timestamps is done with challenge-response messages.

Any message received with an invalid timestamp or digest is then discarded by the IDS agent, and an alert is raised. This mechanism has been chosen in order to have reasonably secured messages without using too expensive cryptographic material. However, the voting mechanism uses blind signatures [14] in order to especially secure those exchanges.

3 Resources usage and implementation

Our experiments have shown that the sensor motes currently available on the market have very limited resources, so that implementing a distributed intrusion detection system on it can be quite discouraging. Before being able to take into account the power consumption, the first challenge is simply to deal with the low memory of the nodes. The AWISSENET test-bed is mainly composed from Crossbow's Micaz and Iris motes [1], which respectively only have 4KB and 8KB of RAM. As the project is also integrating modules for secure routing and secure service discovery, the memory limitation is quickly exceeded. This implies to carefully choose the amount of audit data that is gathered, thus making intrusion detection more difficult. The AWISSENET IDS uses several mechanisms in order to reduce its resources usage.

As seen in 2.4, the plug-in architecture allows to select efficiently the algorithms that will be deployed on the network and optimize the audit data, since the metrics shared by different plug-ins will only be collected once.

Anomaly detection algorithms should be the algorithms of choice, since they use less memory and still efficient in detecting a wide variety of attacks. However, pattern-matching techniques should be used on a per-case basis ; they aren't suitable for ensuring the overall security of the network, but are the most efficient when targeting attacks against a specific protocol, like the routing one. We have simulated and implemented algorithms that detect black hole, grey hole and selective forwarding attacks, but also attacks like the RREP flooding attack, integrity attack and some cases of Sybil attacks.

Applying the security measures of classical networks to WSNs is difficult, not to say impossible. Cryptographic operations and especially asymmetric cryptography are often very costly and should be avoided as much as possible in sensor networks. Moreover, nodes don't have enough memory to store the public keys of the other members when networks are built with hundreds of nodes. The AWISSENET IDS thus uses symmetric keys and timestamps in order to secure its exchanges.

Finally, the AWISSENET project is using low-cost, low-power programmable logic devices (CPLD, [15]) in order to implement the most resource demanding functions (and especially cryptographic ones) on hardware, thus speeding up the algorithms and reducing the power consumption up to 1 / 100th of that used by a microcontroller.

1. http ://www.xbow.com/Products/productdetails.aspx ?sid=156

4 Conclusion

AWSNs impose new challenges on the design of IDS, which are more imperative than ever due to the unattended operations in open environments. We propose to implement a flexible and efficient intrusion detection system, which can then be used in a variety of wireless network and devices.

Références

1. O. Kachirski, R. Guba, D. Schwartz, S. Stoecklin, and E. Yilmaz : Casebased agents for packet-level intrusion detection in ad hoc networks. In Proceedings of the 17th International Symposium on Computer and Information Sciences. CRC Press, October 2002, pp.315-320
2. I. Stamouli : Real-time Intrusion Detection for Ad Hoc Networks. Master of Science dissertation, University of Dublin, 2003
3. K. Ioannis, T. Dimitriou, and F. C. Freiling : Towards Intrusion Detection in Wireless Sensor Networks. 13th European Wireless Conference, Paris, April 1997
4. P. Albers, O. Camp ; J-M. Percher, B. Jouga, L. Mé, and R. Puttini : Security in Ad Hoc Networks, a General Intrusion Detection Architecture Enhancing Trust Based Approaches. In Proceedings of the 1st International Workshop on Wireless Information Systems, April 2002
5. Y. Zhang, W. Lee, and Y. Huang : Intrusion Detection Techniques for Mobile Wireless Networks. ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003.
6. R. Roman, J. Zhou, and J. Lopez : Applying Intrusion Detection Systems to Wireless Sensor Networks. Consumer Communications and Networking Conference, 2006, pp. 640-644
7. V. Bhuse and A. Gupta : Anomaly intrusion detection in wireless sensor networks. Journal of High Speed Networks, Vol. 15, No. 1, pp. 33-51, 2006
8. A. Hafslund, A. Tonnesen, R.B. Rotvik, J. Anderson, and O. Kure : Secure extension to the OLSR protocol. 1st OLSR Interop & Workshop, San Diego, 2004
9. J. Deng, R. Han, and S. Mishra : Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks. In Proceedings of the 1st Conference on Security and Privacy for Emerging Areas in Communications Networks, Athens, September 2005
10. C. Karlof, N. Sastry, and D. Wagner : TinySec, A link layer security architecture for wireless sensor networks. In Proceedings of the 2nd ACM conference on Embedded Networked Sensor Systems, November 2004.
11. ZigBee Alliance : ZigBee Specification. Technical Report Document 053474r06, June 2005.
12. M. Luk, G. Mezzour, A. Perrig, and V. Gligor : MiniSec, A Secure Sensor Network Communication Architecture. In Proceedings of International Conference on information Processing in Sensor Networks, Cambridge, April 2007.
13. M. Guerrero Zapata and N. Asokan : Securing Ad Hoc Routing Protocols. In Proceedings of the 2002 ACM Workshop on Wireless Security, pp. 1-10, September 2002.
14. D. Chaum : Blind signatures for untraceable payments. Advances in Cryptology, Crypto '82, Springer-Verlag pp. 188-203, 1983.
15. Xilinx : CoolRunner-II CPLD Family. Product specification, DS090 (v3.0), March 2007.

Analyse de la menace sur les applications sans fil de courte et de moyenne portée

Éric Bornette, Didier Eymery

Centre d'électronique de l'armement
BP 57419 la Roche Marguerite 35174 BRUZ-CEDEX
eric.bornette, didier.eymery@dga.defense.gouv.fr

Résumé Les applications sans fil apportent une réelle simplification dans le déploiement d'un système en diminuant la contrainte physique. Leurs performances sont comparables à celle des applications filaires mais qu'en est-il en matière de sécurité ? L'étude du point de vue de l'attaquant d'une application sans fil permet de poser le problème sous l'angle de l'analyse de la menace : « quel effort doit consentir l'attaquant pour atteindre son objectif, quelles voies peut-il emprunter ? ». Dans ce cadre, la construction de scénarios d'attaque permet de comparer les rapports gain/coût d'une attaque dans le cas d'une application sans fil et dans celui d'une application filaire.
Mots clés : sécurité des systèmes d'information, menace, sans fil, attaque.

1 Introduction

Le but de cet article est d'aborder le problème de la sécurité des applications sans fil courte et moyenne portée (type NFC à Wi-Fi). Cet article décrit une analyse de la menace sur un système utilisant ce type de moyen en l'abordant sous l'angle d'un agresseur potentiel.

Dans un premier temps, pour faciliter la lecture, nous effectuerons une description du mode général des transmissions sans fil, puis nous détaillerons le processus d'attaque. Ensuite, nous prendrons comme hypothèse que le système, cible de l'attaque, utilise une ou plusieurs applications sans fil et qu'il représente un intérêt pour l'agresseur. Il compte tirer un gain (image, ego, argent...) de son attaque. Il va consentir un effort en fonction de ses capacités et de sa volonté pour atteindre son objectif sur le système. Nous nous intéressons à une menace de type « opportuniste », c'est-à-dire qu'elle n'est pas forcément à l'état de l'art. Par contre, pour atteindre son objectif, l'agresseur exploite l'ensemble de ses capacités techniques, dans les domaines de l'électronique et de l'informatique. Nous décrivons, dans l'article, un cycle complet d'attaque du système équipé d'application sans fil en essayant de montrer ce qui est spécifique à l'emploi de ce type de moyen et ce qui ne l'est pas.

2 Description des applications sans fil.

2.1) Emploi des applications sans fil.

On peut différencier les différents cadres d'emploi des moyens « sans fil » et des moyens « filaires » :

- au sein d'un système payement sécurisé,
- transmission de données entre ordinateurs,
- utilisation ludique (connexion d'une manette sur une console de jeu…).

On peut aussi montrer que le choix entre ces deux solutions peut être est motivé par différents critères :

- coûts,
- type de service,
- qualité de service,
- capacité d'élongation entre deux composantes reliées par un moyen « sans fil »…

Le tableau suivant présente une synthèse comparative de l'emploi de moyens « filaire » et de moyens « sans fil ».

	Sans fil	***Filaire***
Coût d'acquisition	Plus important	Moins important
Coût d'installation	Bien moins important	Beaucoup plus important
Coût d'utilisation	Pas de surcoût en local. Plus important pour services payants.	Pas de surcoût en local.
Service mobilité	Important suivant technologie	Très localisé.
Service sécurisé	Ne peut pas reposer sur la sécurité physique.	Renforcé par la sécurité physique en local.
Service débit	A partir de quelques Ko	A partir de quelques Ko
Maintenance	Charge moins importante	Charge plus importante

Cette comparaison fait ressortir que les applications « sans fil » offrent des services comparables à celles qui utilisent des médias filaires. Cependant, elles sont beaucoup plus faciles et rapides à utiliser. Leur premier intérêt repose sur la limitation de la contrainte physique (passage de câble, protection des supports physiques…).

2.2) Caractérisation technique des applications « sans fil ».

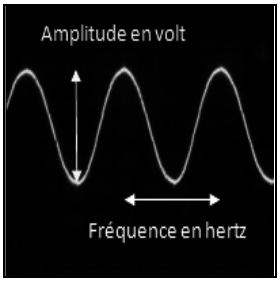
La description d'applications « sans fil » nécessite l'emploi de nombreux termes du vocabulaire de l'électronique, du traitement du signal. Il convient de rappeler ces notions afin de comprendre les explications qui sont données au sein du chapitre 3. Le lecteur qui possède déjà ces prérequis peut directement accéder au chapitre 3.

2.21) Moyens de caractérisation et de mesure d'un signal électrique.

Un signal électrique peut être visualisé par un **oscilloscope** qui présente l'évolution de sa **tension** (sa puissance en quelque sorte) au cours du **temps.** Cependant, il faut savoir (cf. Fourier) que tout signal utile S(t), quelle que soit sa forme, peut être décomposé en une somme de fonctions du type :

$$s(t) = A(t)*\sin[2\Pi*F(t)+\varphi(t)]$$

Cette propriété implique que l'on ne s'intéresse alors plus qu'aux fonctions s(t) : les sinusoïdes.



L'**amplitude** A(t), exprimée en volt, représente la puissance du signal qu'on mesurera en **décibel par rapport au milliwatt** (dBm). Un écart de puissance, quant à lui, se mesurera en **décibel** (dB).

La **fréquence** F(t) représente la vitesse à laquelle la sinusoïde bat : le nombre de battements par seconde se mesurera en **Hertz** (Hz).

FIGURE 1 : Visualisation d'une sinusoïde sur un oscilloscope

La **phase** φ(t) représente l'endroit où se trouve la sinusoïde dans le cycle de son battement : il s'agit d'un angle que l'on mesurera en degré (°).

L'ensemble des fonctions s(t) du signal S(t) s'appelle le **spectre du signal** S(t). On peut le visualiser sous la forme d'un diagramme représentant la puissance A en ordonnée et la fréquence F en abscisse. Ce spectre peut être visualisé avec un appareil appelé **analyseur de spectre**.

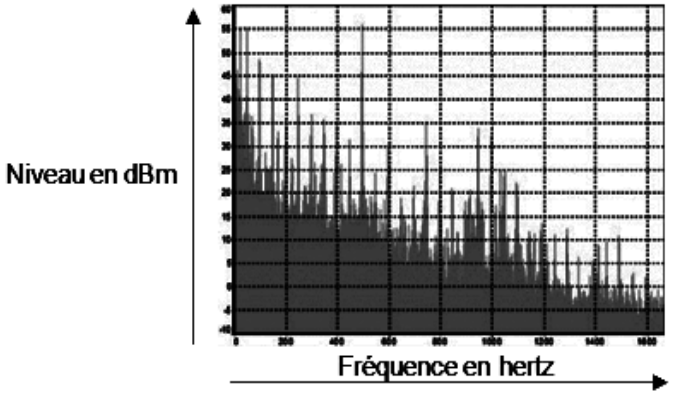


FIGURE 2 : Vue spectrale d'un signal S(t)

2.22) Caractérisation du débit.

On appelle **bande de base** le signal utile brut. De plus, les informations vont être échangées à une certaine vitesse. La quantité d'informations échangées par unité de temps est appelée **débit** (bit/s). On parle également de **débit symbole** (Symbole/s), ces deux débits sont proportionnels.

Ce débit symbole, noté D, a une influence directe sur les constituants s(t) du signal utile. En effet, le signal utile brut est constitué uniquement de sinusoïdes de fréquence comprises entre 0 et D Hz.

2.23) Transmission du signal.

La **transmission d'un signal** S(t) par le biais d'un moyen radio, est rendue possible si ce signal possède des composantes s(t) dans une plage de fréquences très supérieure à celle de la bande de base. De manière empirique, on décale le spectre du signal pour utiliser une fréquence libre et plus élevée. On **module** le signal brut S(t) avec un signal porteur Sc(t) de façon à produire un signal modulé transportable qui occupe une bande de fréquence [Fc-D, Fc+D].

Le signal utile ainsi modulé occupe une bande de fréquence de B = 2*D Hz, appelée **largeur de bande**. Il est nécessaire que les appareils utilisés pour traiter le signal possèdent une bande passante suffisante, c'est-à-dire, supérieure à B.

Pour combiner S(t) avec Sc(t), qui est une sinusoïde pure, il est possible d'agir sur les 3 paramètres de la sinusoïde Sc(t) : Ac(t) pour l'amplitude, Fc(t) pour la fréquence et φc(t) pour

la phase. Suivant l'élément sur lequel on agit, on parlera respectivement de modulation d'amplitude, de modulation de fréquence et de modulation de phase.

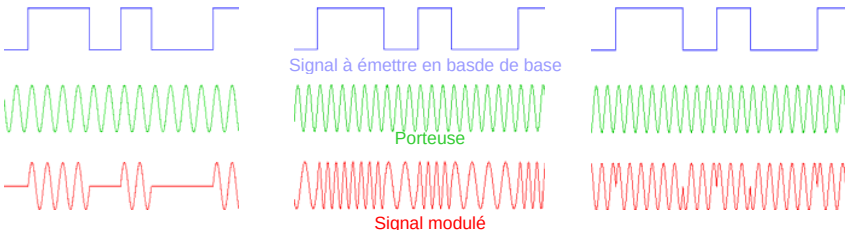


FIGURE 3 : Illustration des trois types de modulation (amplitude, fréquence, phase).

Il faut noter qu'il est également possible d'agir sur plusieurs paramètres à la fois pour réaliser des modulations plus évoluées. De manière empirique, nous avons constaté que les éléments de Sc(t) qui vont être modifiés dépendront directement de S(t). On peut, par exemple, avoir Ac(t) = f (S(t)). Un coefficient de proportionnalité est appliqué, il est appelé **taux de modulation** T.

Enfin, si le signal S(t) change de forme de façon discontinue à intervalle régulier et prend un ensemble fini et bien défini de valeurs, on parle de **modulation numérique**. C'est le cas lorsque l'on traduit les bits à transmettre en signal électrique : à chaque valeur bien définie, appelée **symbole**, correspond un groupe de bits déterminé. A contrario, lorsque S(t) change perpétuellement de façon continue, on parle de **modulation analogique**.

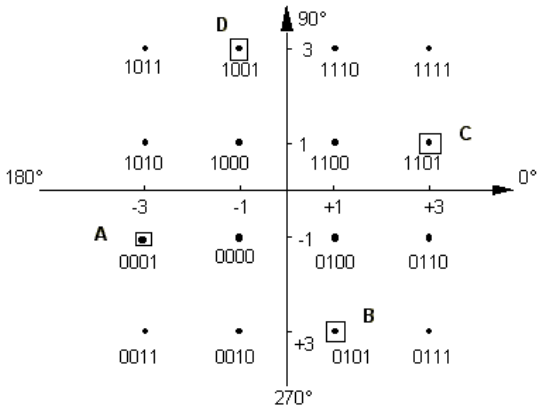
Une fois le signal S(t) modulé, le nouveau signal E(t) est émis au moyen d'un émetteur.

2.24) Capture du signal.

Un récepteur peut capturer le signal R(t). Ce signal E(t) a été émis par un émetteur. R(t) diffère de celui émis. En effet, ce signal a subi un certain nombre de perturbations liées à sa diffusion. Il est bruité et parasité par d'autres signaux. Aussi, pour se rapprocher le plus possible du signal émis, il est nécessaire d'appliquer un certain nombre de traitements. Il faudra filtrer le signal R(t) afin de l'épurer au maximum pour éliminer le plus possible de bruit et de parasites, mais également l'amplifier (d'un certain gain exprimé en dB) pour que les altérations dues à la chaîne de traitement soient négligeables.

Après ce prétraitement, le but est de retrouver le signal S(t) qui a été modulé et émis. Autrement dit, il faut démoduler R(t) en un signal qui se rapproche le plus possible de S(t) : il faut donc retrouver les paramètres Ac(t), Fc(t) ou φc(t) de la porteuse. A partir de R(t), le processus de démodulation produit 2 signaux : I(t) et Q(t). Ces deux signaux sont issus d'un

produit entre R(t) et respectivement un cos[2Π*Fc(t)] et un sin[2Π*Fc(t)]. C'est grâce à ces signaux que tout se déduit. Ils sont représentés sur un diagramme IQ, avec I(t) en abscisse et Q(t) en ordonnée. L'appareil permettant de le visualiser s'appelle un **analyseur vectoriel**.



Lorsque l'on regarde le diagramme IQ d'un signal issu d'une modulation numérique on obtient un ensemble d'îlots (ou nuages) de points. Chaque îlot correspond à une des valeurs possibles de la modulation numérique (symbole).
L'ensemble de ces îlots s'appelle une constellation.

FIGURE 4 : exemple de constellation

2.25) Amélioration de la qualité du signal.

La réception des bits émis peut être entachée d'erreurs pouvant provenir d'une désynchronisation entre l'émetteur et le récepteur, ou de parasitage et bruitage. Afin que le récepteur puisse en corriger un maximum, différents mécanismes peuvent être mis en place.

Le **codage de canal** permet de lutter contre la désynchronisation en s'assurant qu'aucune séquence trop longue de 0 ou de 1 n'existe dans les données transmises.
Un code correcteur d'erreur permet au récepteur de trouver et de corriger un bit mal décodé grâce aux autres bits reçus.

L'étalement de spectre est un autre moyen permettant de s'affranchir de certains parasites. De façon empirique, il s'agit d'émettre N bits pour 1 bit utile, mais à une vitesse N fois plus grande. Les N bits sont choisis d'une façon particulière et sont liés entre eux. On parle d'étalement de spectre dans la mesure où la largeur de bande du signal émis est N fois plus importante que le même signal non étalé. Un autre usage est le **Transec** (transmission security) dans la mesure où il faut connaître la correspondance entre les N bits émis et le bit réel.

L'évasion en fréquence consiste à changer périodiquement la fréquence Fc du signal porteur. Le but, entre autres, est également de s'affranchir de certains parasites. Un autre usage est le Transec dans la mesure où il faut connaître la politique des sauts.

2.26) Multiplexage du signal.

Les bits échangés doivent être structurés pour que les deux parties, émetteur et récepteur, s'y retrouvent. Cette structuration est réalisée au moyen de différents protocoles s'enchaînant les uns les autres comme des « poupées russes ».
Afin, de maximiser l'utilisation d'une plage de fréquence, il est possible d'agréger plusieurs communications au sein d'un flux plus gros appelé multiplexe. Le multiplexage peut être réalisé :

- en fréquence (**FDMA**) : les données de différentes communications sont émises simultanément sur des porteuses disjointes ;
- en temps (**TDMA**) : les données de différentes communications sont émises alternativement ;
- mixte des deux précédents (**CDMA**).

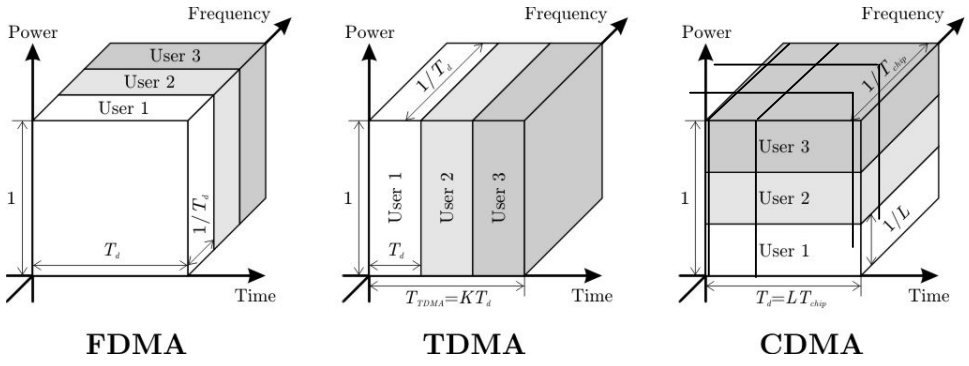


FIGURE 5 : multiplexage FDMA, TDMA, CDMA

2.27) Protection du signal.

Les données émises peuvent être protégées à la fois en confidentialité et en intégrité par des mécanismes de chiffrement. Lorsqu'un tel mécanisme agit au niveau le plus bas de la chaîne d'émission/réception, on parle de **Transec**. Lorsque ce mécanisme est mis en œuvre dans les couches hautes (au niveau du logiciel de décapsulation des protocoles), on parle de **Comsec** (communication security).

2.28) Notions complémentaires.

Il y a encore de nombreux termes qui devraient être présentés. On peut citer le rapport signal à bruit, le « G/T » d'une antenne, la PIRE d'une liaison... Les éléments présentés ci-dessus sont suffisante pour aborder la suite de ce document.

2.3) Modèle générique d'une application sans fil.

Le modèle présenté en figure 6 permet de lister et de positionner entre eux les éléments qui rentrent dans la constitution d'une chaine d'émission et de réception (E/R). Il permet aussi de présenter les constituants qui devront être réalisés par l'attaquant, comme décrits dans le paragraphe 3.

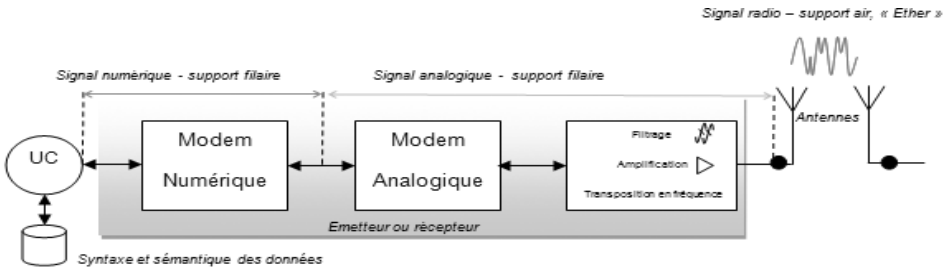


FIGURE 6 : modèle générique d'une chaîne d'émission ou de réception par radio

2.4) Modèle générique d'une transmission par un média «filaire».

La figure 7 présente le modèle générique utilisé pour un support filaire « classique ». Celui-ci peut être de type cuivre, fibre optique…

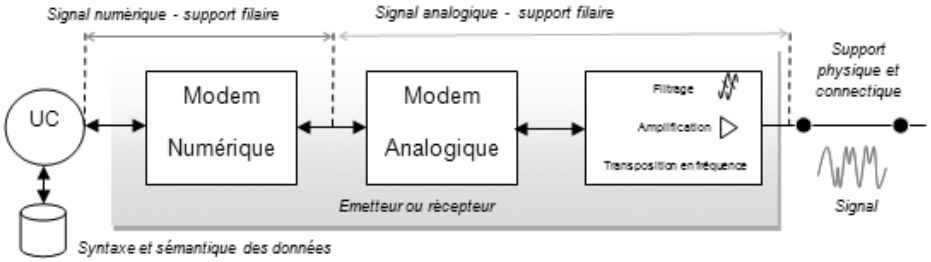


FIGURE 7 : modèle générique d'une chaîne d'émission ou de réception via un média filaire

2.5) Comparaison des deux modèles.

Nous allons maintenant comparer ces deux modèles en nous positionnant du point de vue de l'attaquant. La description des actions que doit réaliser un hostile pour atteindre un objectif sur un système sera basée sur ces modèles génériques (figure 6, 7 et 8).

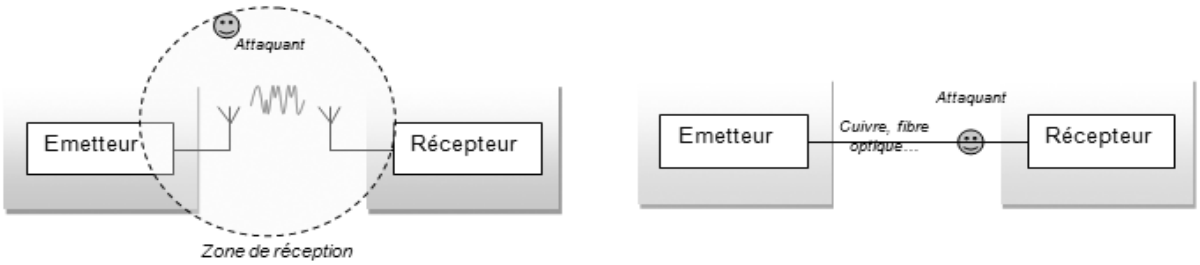


FIGURE 8 : Attaquant sur le modèle "radio" et sur le modèle « filaire »

Une chaine de transmission, sur un média de type filaire, est comparable à la chaîne de transmission sans fil. Cependant, c'est l'accès au média de communication qui est différent. En effet, il est difficile de circonscrire « géographiquement » une émission radio ce qui facilite l'accès à la communication. Pour une liaison filaire, l'attaquant doit accéder physiquement au média de communication (figure 8 droite) ou en proximité proche pour l'exploitation des signaux compromettants.

2.6 Exemples pour les applications sans fil.

Afin d'illustrer les éléments présentés jusqu'ici, ces modèles sont déclinés pour deux exemples très courants , le « radio frequency identification » (RFID) et le « wireless fidelity » (Wi-Fi).

2.61 Exemple du RFID.

Le RFID est un cas d'application courte portée. Nous présentons ici le cas d'une application reposant sur la norme ISO14443-A. L'exemple est un contrôle d'accès par « badge sans contact » pour accéder à un bâtiment dans le cadre du contrôle d'accès physique. Le badge (PICC) va échanger des données avec « le lecteur » (PCD) dans le but d'accorder (ou non) l'accès au bâtiment par le détenteur du badge. Notons que le PCD n'est en fait qu'un émetteur / récepteur utilisé par une application informatique classique fonctionnant sur un PC. Evidemment, le PICC intègre ces deux composants : émetteur / récepteur et application informatique minimale. Le PICC et le PCD sont conformes au modèle générique présenté précédemment (figure 8).

Ici, la chaîne de transmission du PCD vers le PICC (figure 10) est différente de la chaîne de transmission du PICC vers le PCD (figure 11). On peut noter que nous avons volontairement décomposé, plus finement, les différents étages dans les modèles qui suivent (figure 9 et 10).

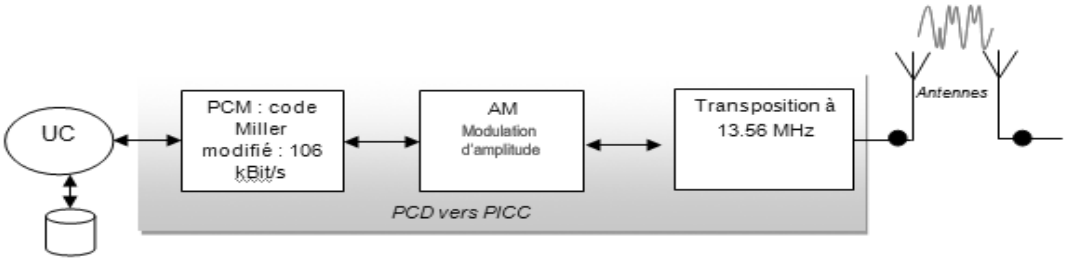


FIGURE 9 : Chaîne PCD vers PICC

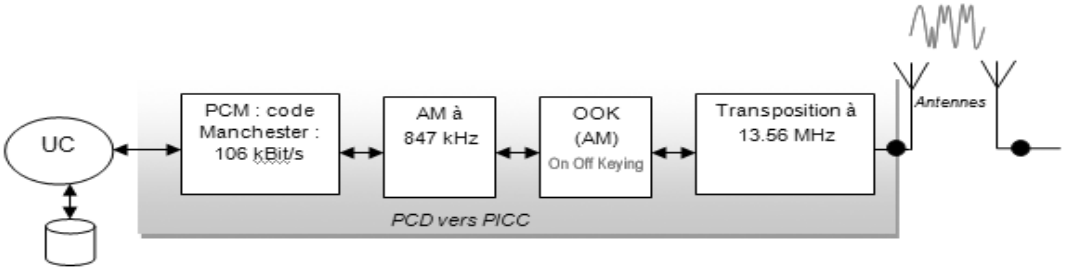


FIGURE 10 : Chaîne PICC vers PCD

On peut se positionner entre le PICC et le PCD, comme proposé dans la figure 8 et capter les échanges radio. La figure 11 montre le signal observé à l'aide d'un oscilloscope.

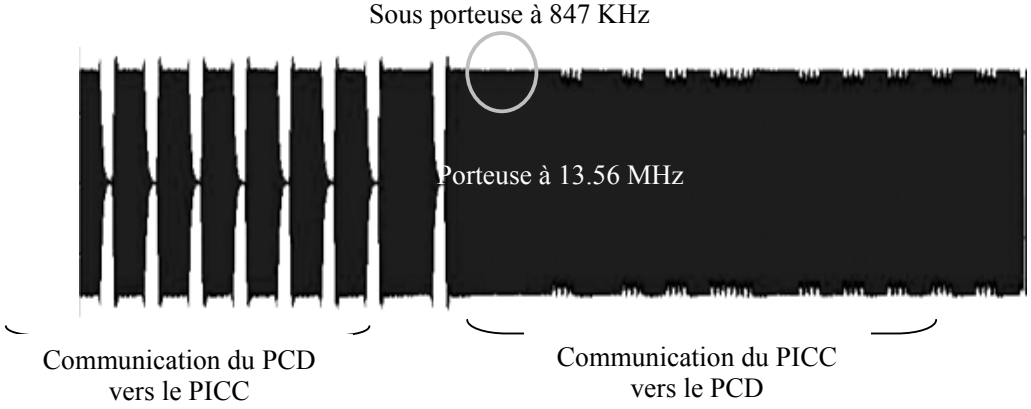


FIGURE 11 : Visualisation du signal réel "PCD vers PICC" et la réponse

2.62 Exemple du Wi-Fi.

Nous présentons, ici, une communication Wi-Fi moyenne portée, reposant uniquement sur la norme IEEE 802.11a. Il existe 14 canaux de 22 MHz de bande répartis dans la bande de fréquence 2.4 à 2.5 GHz. La forme d'onde est dite à « étalement de spectre » avec un code à 11 « chip » : cela revient à émettre 11 bit pour 1 bit utile. Un exemple est un PC portable communicant avec un « acces point » (AP) jouant, par exemple, le rôle de passerelle vers Internet.

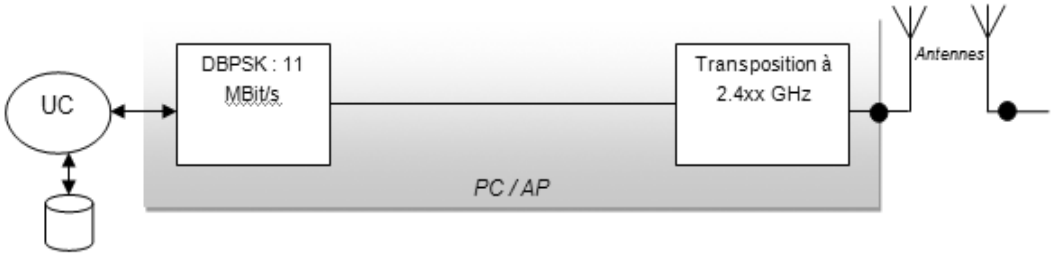


FIGURE 12 : Chaîne PC vers AP pour un débit utile de 1 MBit/S

Notons qu'en fonction du débit, la modulation change :

- 1MBit/s utile, 11 MBit/s émis Differential Binary Phase Shift Keying DBPSK (1 Bit/Symbole),
- 2MBit/s utile, 22 MBit/s émis en Differential Quadrature Phase Shift Keying DQPSK (2 Bits/Symbole).

On peut se positionner dans la chaîne entre un émetteur Wi-Fi et un AP par exemple et observer, à l'aide d'un oscilloscope (figure 14), les échanges radio.

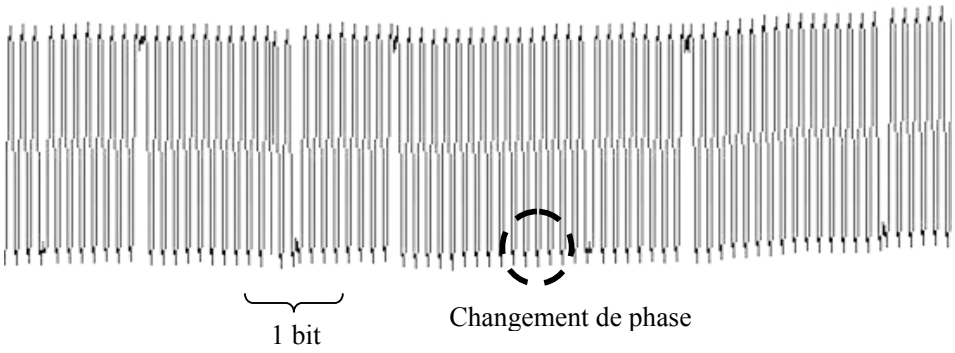


FIGURE 13 : Signal DBPSK d'un média radio Wi-Fi

3 Analyse de la menace sur les applications sans fil.

Après avoir fait un rappel sur les termes et les modèles d'échange dans le cas d'une application radio, nous allons nous placer dans la situation de l'attaquant pour tenter de faire un état des menaces qui pèsent sur ce type de système. Après avoir expliqué la démarche générique liée à l'attaque dans le paragraphe 3.1, nous analyserons les différences engendrées par l'utilisation d'une application sans fil ou filaire, du point de vue de l'attaquant.

3.1) Description générale du processus d'attaque.

Le processus général d'attaque est représenté avec la figure 14. Pour atteindre un objectif sur un système, l'attaquant va successivement et récursivement réaliser les actions suivantes :

- acquérir des connaissances sur le système,
- tenter d'élever ses droits pour réaliser des actions sur des composants du système,
- réaliser des actions jusqu'à atteindre son objectif.

La démarche de l'attaquant est décrite au sein d'un scénario. Celui-ci est composé d'une suite d'actions élémentaires (prise d'empreinte, élévation de droit…). La nature de ces actions élémentaires est directement liée à la nature des objets qui en sont la cible :

- pour une cible humaine : l'ingénierie sociale,
- pour une cible physique : l'intrusion physique,
- pour une cible radio fréquence : l'interception, le brouillage…,
- pour une cible informatique : les techniques classiques de « hacking ».

Chaque action élémentaire peut être quantifiée en termes de coût, de temps de compétence, etc. A travers la démarche présentée dans cet article, nous allons donc tenter de comparer le coût global d'une attaque sur une transmission sans fil par rapport à celui d'une attaque sur une transmission filaire.

Cet article aborde uniquement les actions élémentaires de nature technique.

3.2) Description de l'attaque du système utilisant l'application sans fil.

Sur la base d'un système hypothétique, nous allons décrire les différentes actions élémentaires (figure 14) que peut réaliser l'attaquant pour une atteinte en confidentialité, en intégrité et en disponibilité. Dans chaque cas, nous allons identifier les outils et savoir faire nécessaires, dans la logique du moindre coût et effectuer la quantification globale de l'attaque (point de vue opportuniste).

Pour chaque type d'action nous nous efforcerons de montrer plusieurs solutions possibles, illustrées d'un exemple réel. Ces exemples ne sont pas liés à un même système afin de ne pas

délivrer, au lecteur, une attaque « clé en main ». Ce dernier pourra aisément replacer ces actions dans le cadre d'un exemple complet et cohérent.

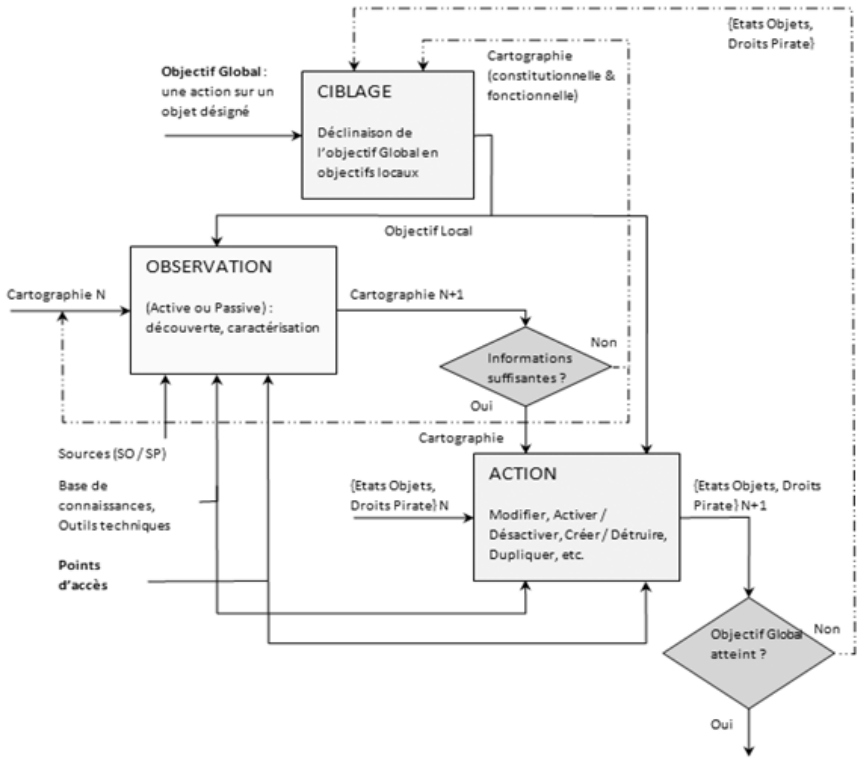


FIGURE 14 : modélisation des actions d'un attaquant

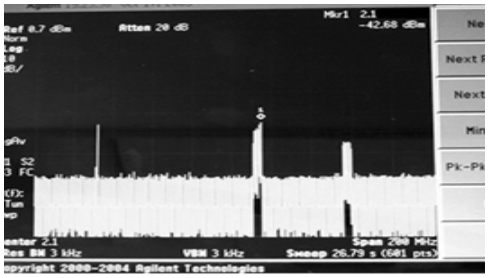
3.2.1) Action « Observation/Découverte » pour déceler l'utilisation d'une application «sans fil».

L'objectif de cette action est de permettre à l'attaquant de déceler l'utilisation d'une application sans fil au sein d'un système. On montre ici quelques méthodes et moyens nécessaires pour estimer les coûts de ces actions élémentaires.

3.2.1.1Découverte par la mesure (analyse spectrale).

Un attaquant peut essayer de mesurer le spectre électromagnétique dans l'environnement physique du système ciblé pour mettre en évidence la présence d'un signal radio lié à une application sans fil. Pour cela, il lui faut l'équipement adéquat, c'est-à-dire un analyseur de spectre. Il faudra aussi, qu'il puisse se positionner dans la zone de propagation d'un signal

radio. Celle-ci est variable en fonction du type de technologie sans fil et des conditions d'utilisation (géographie, bruit, météo…).



Dans une logique de moindre coût, on peut facilement acheter un matériel performant et à moindre coût quand il est mis en vente au domaine en fin de vie « administrative ».

FIGURE 15 : exemple d'analyse de spectre aux alentours de 2 Ghz

3.2.1.2 Par l'exploitation des sources ouvertes.

Dans le cadre de l'analyse spectrale, une connexion Internet, un ordinateur standard et une recherche par mots clés par le biais d'un moteur de recherche peuvent suffire. Cette phase de renseignement permet à l'attaquant de découvrir l'utilisation d'un moyen radio sur le système qui l'intéresse, sans avoir à se déplacer.

Si on cible, par exemple, le système FELIN qui doit équiper les « soldats du futur », une recherche rapide sur le site de la société maître d'œuvre du projet nous donne les éléments suivants : *« …En effet, les sociétés des branches Défense Sécurité et Communication maîtrisent la plupart des technologies électroniques de défense et des télécommunications mises en œuvre dans Félin : l'optronique, permettant la vision nocturne, la restitution d'images vidéo sur des afficheurs miniatures ou encore les moyens de communication constituant un réseau d'information, l'électronique militarisé et portable (miniaturisée pour les militaires), mais aussi les technologies dérivées du monde civil comme le DECT (Digital European Cordless Telephone) ou Bluetooth... Un des principaux défis de Félin est la mise en synergie de toutes ces compétences s'appuyant sur des technologies duales… ».*

3.2.1.3 Par l'observation et par la déduction.

L'observation est un autre moyen de découvrir l'utilisation d'applications dans fil par examen des antennes nécessaires aux moyens E/R. Celles-ci sont souvent à l'air libre. Le type d'antenne utilisée peut nous apporter des informations par déduction (fréquence par exemple cf 3.2.3.2).

Ces deux exemples montrent l'utilisation de moyens radios dans le cadre du pilotage de lignes électriques et dans le cadre d'un déport de gestion de télécommande via GSM. La présence d'aériens facilite donc largement l'action visant à déceler la présence d'une application sans fil par rapport à une application filaire, en particulier pour un attaquant qui choisira sa cible par opportunisme et non par rapport à un objectif très précis.

FIGURE 16 : antennes installées sur un poteau électrique et dans un armoire technique

3.2.1.4 Estimation de coût pour la découverte.

L'attaquant peut donc déceler la présence d'un moyen radio, au sein du système qu'il cible, à moindre coût.

Profil	***Coût***	***Temps***	***Moyen***
Technicien	$<10^3$ euros	Quelques jours	Informatique standard, jumelles, appareil photo, analyseur de spectre + antenne.

3.2.2) Action « Observation/Caractérisation » pour déterminer le type de liaison.

L'objectif de ce type d'action n'est plus de déceler l'utilisation d'une application sans fil mais de commencer à la caractériser. Dans l'exemple donné en 3.2.1.2, l'attaquant a mis en évidence l'utilisation d'un moyen radio. Il doit maintenant en déterminer le type.

3.2.2.1 Par une méthode empirique.

L'esprit de la méthode empirique consiste à comparer des caractéristiques mesurables d'une liaison sans fil à des mesures faites sur une plate-forme de test et ce qui peut être capté sur un

système réel. De cette façon on pourra comparer les résultats entre des mesures effectuées dans l'environnement du système réel et des mesures effectuées sur la plate-forme de test.

3.2.2.2 Par l'exploitation des sources ouvertes.

Comme pour l'action décrite au paragraphe 3.2.1.2 l'exploration des sources ouvertes peut aussi, permettre de lister les caractéristiques sur le moyen sans fil utilisé. Dans l'exemple correspondant, le maître d'œuvre du système nous dit qu'il utilise une techonologie DECT ou Bluetooth, sans plus de précision. Les caractéristiques générales de ces deux technologies sont largement accessibles sur internet. L'exemple suivant est de même nature. Après avoir décelé l'emploi d'une application sans fil, l'attaquant augmente son niveau de connaissance sur le système cible jusqu'au moment il pourra atteindre son objectif final.

TRAITEMENT DES EAUX : UNE STATION D'ÉPURATION HIGH TECH À MONTPELLIER

La station d'épuration Maera, qui vient d'être rénovée à Lattes (34) utilise un réseau informatique avant-gardiste pour gérer 600 équipements capables de traiter les eaux usées de l'agglomération de Montpellier afin de restituer une eau pure à 90 % à plus de 10 Km au large. Une modernisation pour laquelle les partenaires dans la réalisation de ce projet Montpellier Agglomération et Veolia se sont vus remettre hier la triple certification ISO 14001, ISO 9001 et ILO-OSH 2001, mardi 19 février, à l'Hôtel de l'Agglomération de Montpellier.

Georges Frêche, président de l'Agglomération de Montpellier et Antoine Frérot, Directeur général de Véolia Eau ont reçu mardi 19 février la triple certification ISO 14001, ISO 9001 et ILO-OSH 2001 pour les performances la station d'épuration Maera.©Johannes Braun/Naja

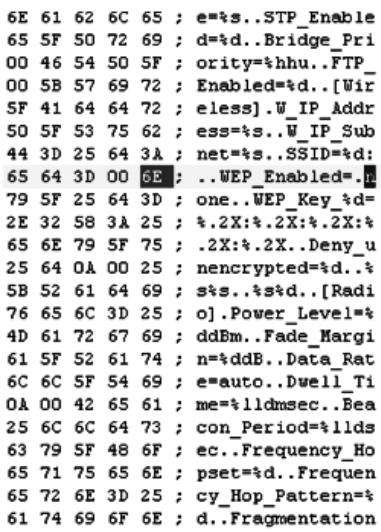
L'agglomération de Montpellier et Véolia Eau ont reçu mardi 19 février de la part du bureau Veritas, la triple certification ISO 14001, ISO 9001 et ILO-OSH 2001, pour la modernisation de la station d'épuration Maera. La station est dotée d'un réseau Ethernet par fibre optique et d'un réseau WIFI pour relier l'armada informatique chargée de gérer les 600 équipements nécessaires au traitement des eaux usées de 470 000 équivalents habitants. Résultat, une eau épurée à plus de 95 % (soit 10 % de plus qu'une station classique) est rejetée à 11 Km au large des côtes. « *Il y a quelques années, les stations d'épuration ne se montraient pas* », souligne Antoine Frérot, Directeur général de Véolia Eau « *M. Frêche vise l'excellence avec cette triple certification alliant souci environnemental, management moderne et rigoureux pour des services de qualité, et santé et sécurité pour les employés* ».

FIGURE 17 : article technique paru dans la presse spécialisée

3.2.2.3 Par l'observation et par la déduction.

Pour augmenter son niveau de connaissance sur le système, l'attaquant peut exploiter les programmes et les fichiers liés aux applications sans fil. En effet, de nombreux constructeurs

offrent la possibilité de charger leurs composants logiciels (driver, firmaware…) directement sur internet. L'analyse rapide des chaînes de caractères présentes dans ces fichiers, à l'aide d'un éditeur hexadécimal gratuit, peut permettre de caractériser précisément les caractéristiques de la liaison radio utilisée.



Cet exemple est celui d'un fichier mis en ligne par le constructeur. C'est une application liée à un modem radio pour une application de type non bureautique. La gamme de fréquence de cet équipement n'est pas du tout celle du Wi-Fi. La recherche des chaînes de caractères, par la méthode décrite ci-dessus, permet de montrer des paramètres techniques importants. Ils permettent de comprendre que cet équipement utilise une technologie mais avec un déplacement de ses fréquences plus haut ou plus bas dans le spectre. Une transposition en fréquence (cf 3.2.4.1.1.3) permettra, à l'attaquant, de tester des attaques « classiques » à la technologie Wi-Fi.

Figure 18 : lecture de chaînes de caractères dans fichier binaire

3.2.2.4 Estimation de coût pour la caractérisation du type de liaison.

Maintenant, l'attaquant a déterminé le type de la liaison sans fil utilisé.

Profil	***Coût***	***Temps***	***Moyen***
Technicien	$< 10^2$ euros	De l'ordre de quelques semaines	Informatique standard, plate-forme de test, accès aux mises à jour de firmware.

3.2.3) Action « Observation_caractérisation » : caractériser les paramètres de la liaison radio.

Après avoir validé l'existence d'une liaison sans fil et déterminé son type, il s'agit maintenant de la caractériser. L'attaquant va donc chercher à recueillir des données techniques précises. Elles sont nécessaires à la conduite de son attaque en itérant les actions présentées précédemment (cf 3.1).

3.2.3.1 Par la mesure.

Comme pour l'action de découverte décrite au paragraphe 3.2.1.1, l'utilisation d'un analyseur de spectre permet de caractériser certains attributs d'une liaison radio et en premier lieu, la fréquence.

Le cas échéant, cette action permettra de valider les informations de caractérisation de liaison. Par exemple, on pourra vérifier l'utilisation réelle de la technologie Wi-Fi, supposée par l'exploitation des sources ouvertes (cf 3.2.2.2).

Les modulations peuvent être caractérisées par l'analyse spectrale (analyseur de spectre) et par l'analyse vectorielle (analyseur vectoriel). L'approche empirique permettra, par comparaison, de déterminer le type de modulation, la puissance, le cycle de vie de l'équipement... Il est important de noter que de nombreuses sources internet permettent de développer ses connaissances en technique radio et en traitement du signal.

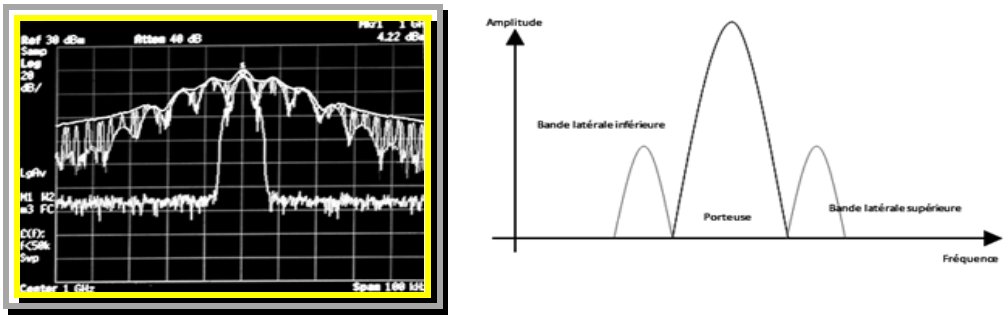


FIGURE 19 : spectres d'une modulation PM et d'une modulation AM

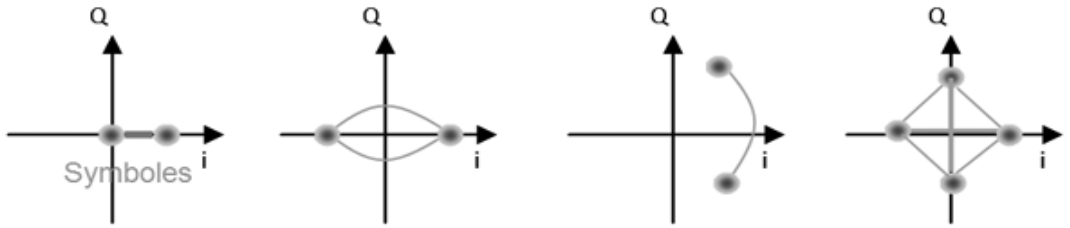


FIGURE 20 : constellations AM, Binary Phase Shift Keying, PM, Quadrature Phase Shift Keying

3.2.3.1 Par l'exploitation des sources ouvertes.

Le recoupement des informations obtenues par internet permet, dans certains cas, d'augmenter le niveau d'information recueilli pour caractériser plus finement une application sans fil. Dans ce cas, il s'agit d'utiliser, de façon opportuniste, les informations disponibles en source ouverte.

Dans l'exemple de la figure 23, la photo de gauche montre une extraction d'une page d'un annuaire professionnel sur internet. L'analyse des ombres portées permet d'observer un mat d'antenne sur lequel sont installés trois équipements radio. La corrélation de ce constat avec les informations accessibles (photo de droite de figure 23) sur le site de l'agence nationale des fréquences (ANFr) permet de supposer que ce site utilise trois faisceaux hertziens aux fréquences indiquées. L'attaquant réalise ici une action de renseignement à moindre coût pour un résultat qui paraît pertinent.

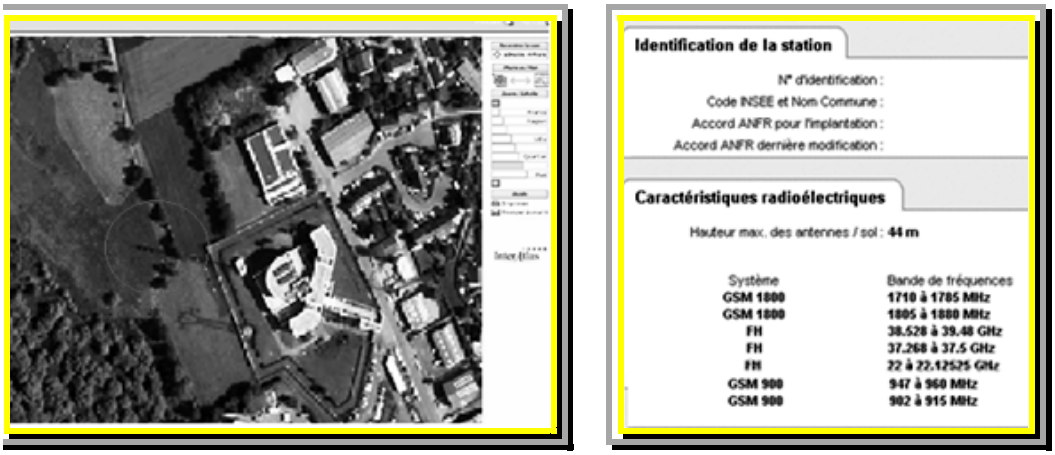
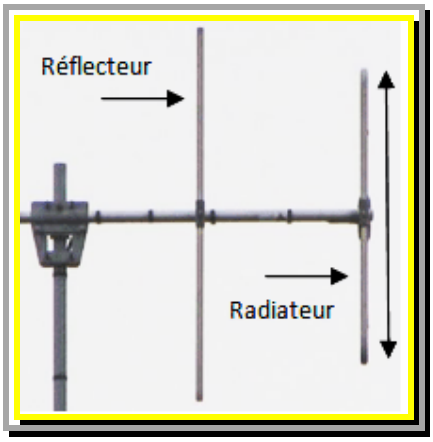


FIGURE 21 : Photo issue des pages jaunes et information de fournie par l'ANFr

3.2.3.2 Par l'observation et par la détection.

Dans le paragraphe 3.2.1.3, l'action d'observation permet de déceler une liaison et le cas échéant d'en caractériser le type (GSM dans l'exemple). On peut aller plus loin et chercher à mettre en évidence certains attributs de cette liaison. Ceci n'est peut être pas forcément nécessaire dans le cadre de l'utilisation d'une technologie sur étagère très répandue comme le Wi-Fi. Par contre, dans le cas de technologie plus confidentielle, cela permet de caractériser la liaison par observation, calcul et déduction.

Pour cela, il faut pouvoir observer la partie « antenne » de la liaison et rechercher les éléments techniques souvent disponibles sur internet. Par exemple, la forme et la taille de l'antenne peut permettre de définir le type de liaison. La direction de l'antenne, quand la liaison est directive peut permettre de localiser les autres équipements qui participent à cette liaison.



Cet exemple présente une antenne dite yagi. Les formules disponibles nous donnent :

- Le réflecteur = 0,495 * lambda.
- Le radiateur = 0,473 * lambda.

Lambda = 300/fréquence en Mhz
Donc comme le radiateur fait 0,5 m on a une fréquence de 300 Mhz environ.

FIGURE 22 : Exemple de calcul de fréquence en fonction des éléments observables de l'antenne.

Les jumelles servent à relever la hauteur en degré du radiateur. La distance qui nous sépare de l'antenne (on peut la mesurer sur une carte) et cet angle nous permettent de calculer la longueur du radiateur (0.5 m ici).

3.2.3.3 Estimation de coût pour la caractérisation des paramètres de la liaison.

L'attaquant a caractérisé les paramètres importants de la liaison sans fil utilisée.

Profil	*Coût*	*Temps*	*Moyen*
Technicien	$<10^3$ euros	Quelques jours	Analyseur de spectre, informatique standard, Jumelles.

3.2.4 Exploitation des informations acquises.

Dans le chapitre précédent, nous avons essayé de montrer, comment l'exploitation des sources ouvertes permet à l'attaquant de concevoir son mode d'attaque. En appliquant la logique présentée par le modèle de l'attaque (figure 14) nous allons concevoir les moyens techniques nécessaires à l'attaque. Pour cela nous nous appuierons sur le modèle générique E/R (figure 6), en recherchant toujours le moindre coût et en adoptant une tactique opportuniste.

3.2.4.1 Réalisation d'une chaîne de réception (attaque en confidentialité).

Dans le cadre d'une attaque en confidentialité, pour écouter une liaison entre un émetteur et un récepteur (figure 8), il faut posséder un récepteur. Le synoptique de la chaine E/R est présenté figure 23. On peut assembler, construire ou acheter ce type d'équipement en fonction du coût, de la nature de l'application sans fil et du contexte de l'attaque.

Notons que le récepteur ou l'ensemble LNB (Low Noise Block) est optionnel. En effet, suivant la fréquence de travail, des modems permettant de traiter directement le signal utile existent.

Après réception des bits bruts, l'attaquant doit encore les traiter à l'aide de l'UC. Ce n'est pas terminé pour autant : il faut appliquer un traitement logiciel, plus ou moins lourd, avant d'accéder aux données utiles (descrambling, correction d'erreur…).
Tous ces étages de traitement peuvent être grandement simplifiés en fonction du type de signal à traiter. Pour le Wi-Fi, de nombreuses « cartes Wi-Fi » permettent d'obtenir des données utiles, à partir d'un signal issu d'une antenne. Il s'agit de produit clé en main dont le coût est très souvent inférieur à celui de la chaîne présentée ci-dessous (figure 25). Dans le cadre de technologies standards et largement diffusées, ces cartes existent fréquemment. Cependant, il reste des cas pour lesquels il faut réaliser cette chaîne de toutes pièces (cas particuliers, technologie confidentielle, besoin de performance de la chaîne).

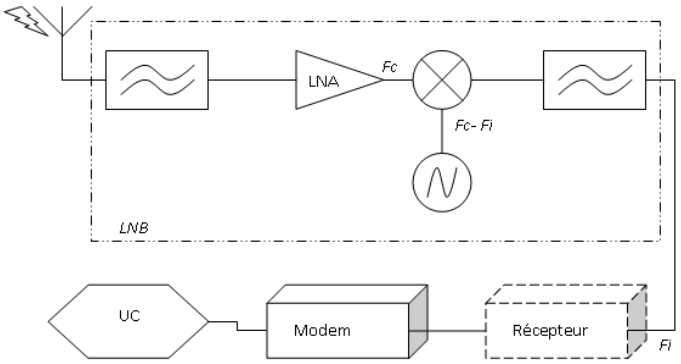


FIGURE 23 : synoptique d'une chaine de réception.

3.2.4.1.1 A partir de composants sur étagère.

3.2.4.1.1.1 Antenne.

L'antenne est le premier élément de la chaîne de réception. De plus, il s'agit principalement du seul point de différence entre un signal radio ou filaire. Une antenne se décompose grossièrement en deux parties : le radiateur et éventuellement le réflecteur. Son choix dépend essentiellement de quatre paramètres :

- la polarisation du signal : linéaire (H/V) ou circulaire (D/G) ;
- le niveau de signal minimum attendu (le gain d'antenne) ;
- l'atténuation de signaux parasites ;
- la gamme de fréquence du signal à recevoir.

Des antennes spécifiques auront un meilleur gain que des antennes « génériques ». En effet, une antenne en polarisation linéaire (ex : antenne Yagi) pourra recevoir indifféremment des signaux de polarisation linéaire ou circulaire. Cependant, une perte de 3dB peut être occasionnée (puissance divisée par deux). En revanche, des antennes à polarisation circulaire (ex : antenne hélicoïdale) seront dédiées à un type de polarisation.

De la même façon, des antennes directives (à opposer à des antennes omnidirectionnelles) ont un meilleur gain et une capacité d'atténuation des signaux parasites (ex : antenne hélicoïdale, Yagi). Le gain peut être accru par l'ajout d'un réflecteur parabolique qui permettra de capter un signal plus fort. Il existe également des antennes qui couvrent une plus large bande de fréquences (ex : antennes dites « log périodique »). Elles permettent de recevoir une large gamme de fréquences.

Antenne yagi Wi-Fi extérieur 18 dBi (dans son tube de protection). 160 euros environ.

Antenne hélicoïdale 400-900 Mhz 14 dB. 600 euros environ.

Cornet 200 Mhz à 40 Ghz. 5000 euros environ.

FIGURE 24 : différents types d'antennes sur étagère.

3.2.4.1.1.2 Filtre.

Après l'antenne vient le filtre passe bande. Comme son nom l'indique, son rôle est d'éliminer le plus possible de signaux indésirables et de ne laisser passer que la bande du signal utile. Son choix dépend donc de :

- la gamme de fréquence du signal à recevoir ;
- sa capacité à atténuer les signaux parasites ;
- l'atténuation induite du signal utile (perte d'insertion).

Les filtres HF sont généralement large bande de 1 à 100 MHz. De plus, ils sont centrés sur une fréquence particulière. Cependant, il existe également des filtres ajustables. Généralement, leur capacité d'atténuation est de 20dB/MHz.

Enfin, notons que le filtre atténue le signal (généralement de 3dB). Aussi, si le signal à recevoir est trop faible et que le signal reçu n'est pas trop parasité, il est possible de se passer du filtre. Cependant, le relief environnant peut être utilisé pour filtrer certains parasites (et accroître la directivité de l'antenne). Si possible, il suffit de placer l'antenne dans une zone encaissée ouverte dans la direction souhaitée.

Filtre professionnel « générique » qui travaille autour des 2.4 Ghz. Le prix est d'environ 500 euros.

Figure 25 : filtre acheté sur étagère

3.2.4.1.1.3 Amplificateur.

L'amplificateur se place après le filtre. Son choix dépend de trois critères importants :

- la gamme de fréquence du signal à recevoir ;
- le niveau de signal minimum attendu (le gain attendu) ;
- le facteur de bruit.

Les amplificateurs sont généralement « large bande ». C'est-à-dire qu'ils amplifient indifféremment (signaux gênants comme signal utile) tout ce qui se trouve dans leur gamme de travail. Or, lorsque leur puissance maximum est atteinte, ils saturent et n'amplifient plus. Aussi, la position de l'ampli par rapport au filtre de tête a son importance : le filtre permet d'éviter que l'ampli soit saturé par des signaux indésirables. Généralement le gain des amplis va de 30dB à 60dB. C'est-à-dire qu'il multiplie la puissance du signal par un facteur compris entre 10^3 et 10^6.

Amplificateur spécialisé Wi-Fi 10 db. Son prix est de 50 euros environ.

Amplificateur professionnel autour de 2.4 Ghz. Gain 30 dB. Très faible bruit. Son prix est de 1500 euros environ.

FIGURE 26 : amplificateurs pour Wi-Fi

Enfin, le choix du facteur de bruit est crucial. En effet, le signal que l'on souhaite amplifier étant généralement très faible, il est impératif de préserver au maximum sa qualité de façon à ce que les étages suivants puissent travailler sereinement. L'ampli est qualifié de LNA (Low Noise Amplificator). Le facteur de bruit doit être choisi inférieur à 1dB.

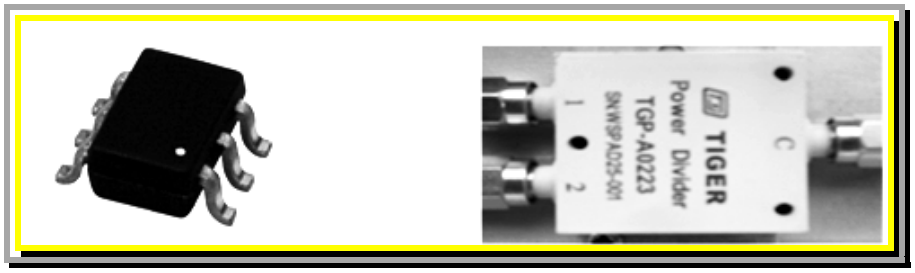
Notons que tant que le signal n'a pas été amplifié, il faut éviter de le parasiter (à travers les câbles notamment). Aussi, le filtre de tête et l'ampli doivent être de qualité et se situer au plus près de l'antenne (généralement accolés à la source). Après cet étage, le signal utile se détache suffisamment du bruit. Il peut donc être manipulé avec beaucoup moins de précautions.

3.2.4.1.1.3 Transposition en fréquence.

Il s'agit ici d'abaisser la fréquence porteuse Fc du signal d'intérêt en Fi, de façon à ce que ce dernier soit manipulable par les étages qui suivent. En effet, les appareils fonctionnant en HF sont généralement plus coûteux que ceux fonctionnant en BF. On va donc chercher à abaisser la fréquence en-dessous des 100MHz. Pour cela, il faut 3 éléments :

- le mélangeur, généralement peu coûteux, permet de combiner (multiplier) deux signaux.
- Le générateur de signal HF permet de produire une « porteuse » pure de fréquence Fc-Fi, qui une fois combinée avec le signal utile de fréquence Fc, permettra d'obtenir le même signal utile mais à la fréquence Fi. Ce type d'équipement peut faire l'objet d'achat tel que celui décrit au paragraphe 3.2.1.1.
- Le filtre permet d'éliminer les signaux parasites issus de la descente en fréquence. Les filtres employés ici sont généralement faciles à trouver car adaptés à une fréquence Fi généralement bien définie (20 MHz ou 70 MHz).

L'ampli, les filtres et la transposition peuvent être intégrés dans un élément appelé LNB (Low Noise Block-concerter). Cependant, on n'en trouve que pour des fréquences et bandes bien spécifiques.



Mélangeur bas de gamme de quelques dizaines d'euros.

Mélangeur professionnel pour un coût d'environ 1000 euros.

FIGURE 27 : différents types de mélangeur

3.2.4.1.1.4 Démodulateur analogique.

Le but est de retirer une éventuelle couche de modulation analogique avant d'attaquer le modem. Ce démodulateur s'appelle généralement un récepteur. Il est capable de travailler directement avec le signal issu de l'antenne. Cependant, ces appareils sont généralement plus

coûteux que ceux travaillant en Fi. De plus, l'avantage d'acquérir un démodulateur en Fi est qu'il est indépendant de Fc, donc réutilisable à souhait.

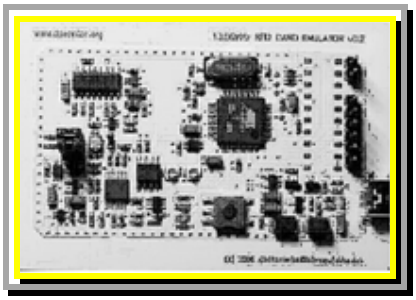
D'autres appareils peuvent faire office de récepteur : un analyseur de taux de modulation par exemple. Cependant, ils fonctionnent avec un niveau d'entrée plus haut.

3.2.4.1.1.5 Démodulateur numérique.

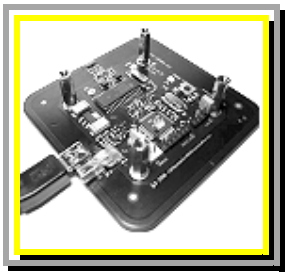
Le but de cet élément est de transformer les signaux en bits. Ce démodulateur s'appelle généralement un modem. Ces appareils peuvent travailler directement à partir du signal issu de l'antenne. Comme pour le démodulateur analogique présenté au chapitre précédent, ces appareils sont généralement plus coûteux que ceux travaillant en Fi. De plus, l'avantage d'acquérir un démodulateur en Fi est qu'il est indépendant de Fc, donc réutilisable à souhait.

3.2.4.1.1.6 Ensemble complet.

Nous présentons ici, des ensembles complets pour illustrer les propos tenus dans le chapitre 3.2.4.1.

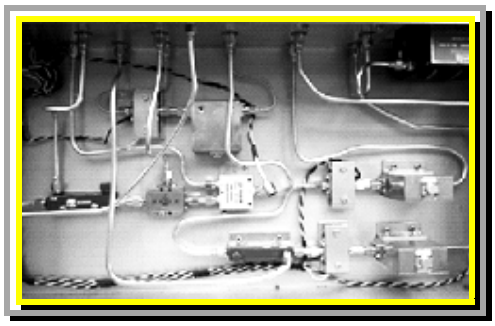


Exemple récepteur PICC RFID. Achat pour 150 euros environ.



Exemple d'émetteur -récepteur PCD RFID. Achat pour 150 euros environ.

Exemple d'intégration de module pour la fonction transposition en fréquence aux alentours des 2.4 Ghz. Il coûte environ 10 K euros et 1 homme mois de travail.
On peut noter, sur cette photo, la nature des connexions entre



les modules. Ce sont des guides d'ondes imposés par la plage de fréquences visée.

FIGURE 28 : exemples de récepteur

3.2.4.1.1.7 Réalisation complète.

Le rôle des différents constituants d'une chaîne de réception a été décrit précédemment au 3.2.4.1.1. Il est possible de diminuer le coût, et d'alléger le poids des matériels en basculant au plus tôt dans le monde informatique. C'est-à-dire qu'il faut numériser le signal dès que possible au moyen d'un CAN (convertisseur analogique/numérique), et réaliser les différentes démodulations informatiquement.

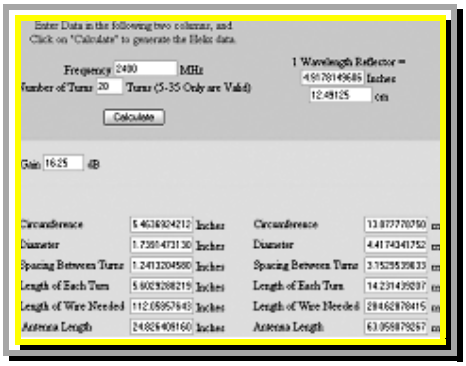
Aujourd'hui les couples numériseurs/PC les plus performants plafonnent généralement à 400 mega sample par seconde. C'est-à-dire que le signal à numériser doit être sous les 100 MHz, donc en Fi.

Cependant, à de grandes vitesses de travail, cela génère des quantités astronomiques de données qu'il faut traiter (10s d'acquisition à 400MS/s et 8bits/Sample produit 4GB de données). Le traitement en « flux tendu » par le PC n'est donc envisageable que pour de faibles vitesses. Il faut réaliser le traitement au cœur du numériseur (en HDL par exemple) et ne remonter vers le PC que la substantifique moelle. Il faut alors des connaissances en traitement du signal et éventuellement en HDL.
Pour des vitesses plus modestes (100kS/s) et un signal ramené dans la bande audio (de 0 à 20kHz), il est possible d'utiliser une carte son comme numériseur. Il faut alors simplement des connaissances en traitement du signal. Notons que l'utilisation d'un numériseur impose le filtrage du signal avant numérisation afin de garantir la qualité de cette dernière. Enfin, on voit qu'on ne peut se passer d'une antenne et d'un LNA (voir d'un LNB). Ces éléments sont néanmoins réalisables de toutes pièces.

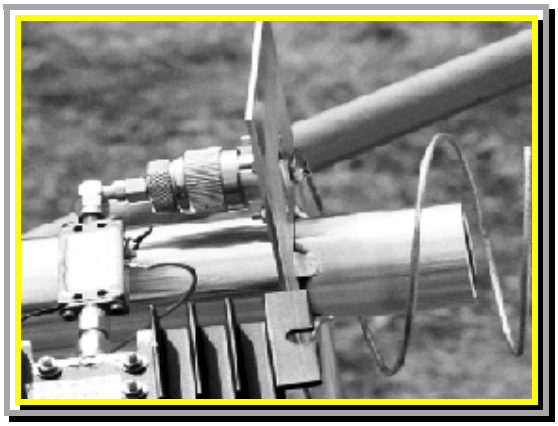
3.2.4.1.2.1 Antenne.

La réalisation d'une source accordée à une fréquence donnée ne demande que peu de moyen. Pour l'exemple d'une antenne hélicoïdale, on peut récupérer les éléments de calcul sur

internet et réaliser « la queue de cochon » à l'aide d'un fil de cuivre assez épais. Celui-ci est à souder sur un connecteur. Le tout est assemblé sur un réflecteur (figure 31).



Outil de calcul d'une source hélicoïdale accessible sur internet.

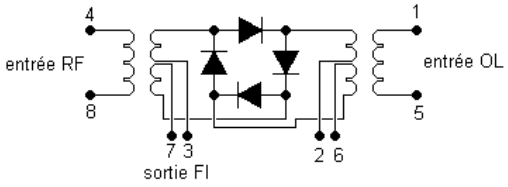


Réalisation d'une source hélicoïdale à l'aide de moyens standards pour quelques euros.

FIGURE 29 : Réalisation d'une source hélicoïdale

3.2.4.1.2.2 Amplificateur, Filtre et transposition.

Le monde de l'électronique est riche en passionnés de tous niveaux qui partagent leur expérience sur internet. On peut, à ce titre accéder à des informations de réalisation des composants présentés plus haut (4.2.4.1.1) comme les amplificateurs, les filtres et les transpositions. On peut montrer, à titre d'exemple, comment réaliser un mélangeur pour faire une transposition. Si cet étage est nécessaire, l'acquisition d'un générateur de fréquence s'impose.



Exemple de montage pour réaliser un mélangeur pour la fonction de transposition. Le signal OL pourra être réalisé avec un oscillateur réglé à la bonne fréquence (Fi = RF + OL ou Fi= RF – OL). Le montage coûte quelques dizaines d'euros.

3.2.4.1.2.2 Démodulateur (modulation analogique).

La partie démodulation peut être réalisée à l'aide d'un montage électronique. L'exemple qui est pris ici, permet de démoduler la composante AM d'une application RIFD entre un PCD et un PICC. La réalisation du montage est très simple et son coût est d'une dizaine d'euros.

FIGURE 30 : démodulation AM d'une liaison entre un PCD et un PICC.

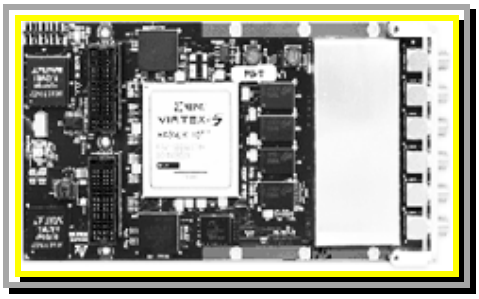
3.2.4.1.2.3 Solution informatique.

Si l'électronique pose des problèmes de mise au point ou d'emploi, il est aussi envisageable de chercher à numériser le signal utile au plus proche de l'antenne et de réaliser, par logiciel, la plupart des étages (figure 25). Le problème est divisé en deux parties :

- la numérisation du signal,
- l'écriture du logiciel ad hoc.

Pour le premier point, le moyen utilisé dépendra de la fréquence ciblée et du débit (cf théorème de Nyquist-Shannon). Dans le cas le plus simple, on pourra utiliser une carte son haut de gamme qui permet pour une centaine d'euros de numériser un signal. Pour les besoins plus importants, on pourra se tourner vers des cartes professionnelles comme celles proposées par la société Innovative (X5-400M) pour un coût de 2 à 5000 euros environ, suivant les options choisies. Dans tous les cas, on pourra tenter de diminuer la problématique de la numérisation en diminuant la fréquence de la porteuse (partie supérieure de la figure 27). Il faut noter que ce type de carte intègre aussi des capacités de génération de signal analogique (DAC) et de traitement FPGA spécialisé pour le traitement du signal.

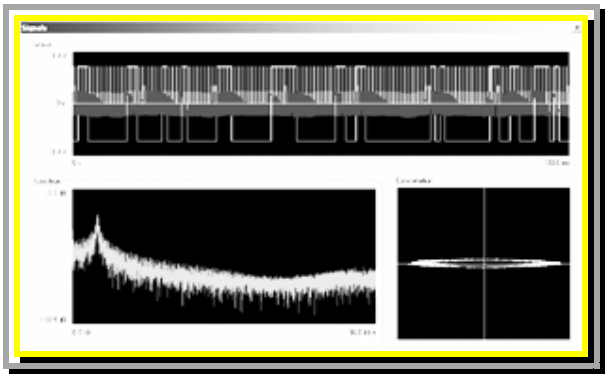
Carte son E-Mu qui possède une capacité d'échantillonnage jusqu'à 192 kS/s sur une bande de 20 kHz. Coût inférieur à 200 euros.



Carte Innovative X5-400 (environ 5000 euros)

- 2 voies A/D 400 MS/s 14 bit
- 2 voies D/A 500 MS/s 16 bit

FIGURE 31 : exemples de moyens de numérisation



La partie logicielle nécessite des moyens informatiques classiques, un ensemble d'outils de développement, une bonne capacité de programmation et une excellente compréhension des bases du traitement du signal.

FIGURE 32 : démodulateur logiciel BPSK

3.2.4.1.3 Estimation du coût de réalisation d'une attaque en confidentialité.

En fonction de la spécificité de l'attaque conduite, l'attaquant a le choix d'acquérir un élément « auto-suffisant » ou de réaliser tout ou partie des moyens nécessaires. Plus l'attaque devra être performante, plus elle nécessitera l'utilisation de moyens performants, faisant ainsi augmenter le coût de l'attaque (forte élongation, technologie fermée et confidentielle…).

Dans le cas d'une attaque en confidentialité, c'est-à-dire que l'attaquant veut accéder au contenu de la communication sans fil, il va réaliser une suite d'actions qui lui permettra d'atteindre son objectif.

Dans un premier temps, il va réaliser une phase de renseignement à l'aide d'actions comme celles décrites 3.2.1. L'apport des informations présentes sur Internet ou l'observation sur site permet de recueillir une part importante des informations nécessaires. Le cas échéant, l'attaquant peut valider ses informations par l'analyse spectrale.

Si la technologie est un standard de fait, la plupart des données nécessaires à la caractérisation de la communication sont accessibles en source ouverte. L'achat d'équipement permet à l'attaquant de vérifier, par la mesure, les informations récoltées. Si la technologie est relativement confidentielle, l'attaquant devra développer une phase de mesure et une phase de retro conception plus importantes.

Grace à cette phase de caractérisation, l'attaquant peut spécifier sa plate-forme d'attaque. Dans le cadre d'une technologie sur étagère, il peut utiliser des équipements sur étagère. La qualité de la capture sera fortement dimensionnée par la qualité de l'antenne utilisée par l'attaquant. Il peut ainsi augmenter la distance entre sa chaîne de capture et l'émetteur du signal. Ce gain peut lui permettre de s'installer en sécurité.

Si l'application sans fil n'est pas une technologie « sur étagère », l'attaquant doit réaliser un étage électronique pour ramener le signal en bande de base. Il peut alors numériser ce signal et traiter par logiciel les phases de démodulation. Il obtient alors les données transportées par le média sans fil. Il se retrouve dans la même situation que s'il s'était branché physiquement sur une connexion filaire. Il lui reste à traiter les suites de 0 et de 1. On se situe maintenant dans une problématique purement informatique qui n'est pas spécifique aux applications sans fil.

Profil	***Coût***	***Temps***	***Moyen***
Technicien	De 0 à 10^4 euros	De l'ordre de quelques semaines	Chaîne spécifique ou équipement sur étagère. Informatique standard.

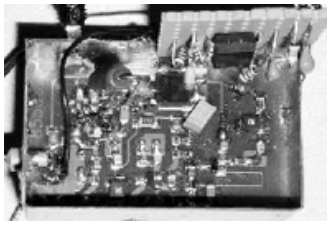
3.2.4.2 Attaque en déni de service (DoS).

3.2.4.2.1 Exemples de moyens.

Un DoS peut être réalisé soit par brouillage, soit par émission cohérente de données. L'émission cohérente impose de réaliser une chaîne d'émission complètement fonctionnelle, alors que le brouillage se borne à émettre des parasites dans la plage de fréquence du signal utile. Ici, nous nous limiterons au brouilleur. La réalisation d'une chaîne d'émission fonctionnelle sera abordée en 3.2.4.3.

L'émission de parasites nécessite l'utilisation d'une antenne, d'un ampli et éventuellement d'une transposition en fréquence. Tous ces éléments sont identiques à la chaîne de réception, à l'exception de l'ampli qui doit être un ampli de puissance. Notons que suivant la puissance que l'on désire émettre, la mise en œuvre et la réalisation manuelle peut s'avérer délicate, voire dangereuse à réaliser (risque d'électrocution, destruction de matériel…).

Brouilleur GPS vendu sur internet pour quelques dizaines d'euros.



Brouilleur GPS réalisé depuis à l'aide de composants électroniques classiques.

Brouilleur GSM de 45 watts (2000 euros environ).

FIGURE 33 : exemples de jammers (brouilleurs) GPS et GSM

La capacité de base de ces équipements peut être adaptée en changeant d'antenne par exemple.

3.2.4.2.2 Estimation du coût pour une attaque DoS.

L'utilisation de montages décrits sur internet ou l'achat de modules « clé en main » permet de conduire une attaque DoS à moindre coût. Il faut préciser que ces montages peuvent être améliorés en leur adjoignant un amplificateur et une antenne qui augmentera leur capacité d'émission ou de réception. Ce type d'attaque est bruyant dès que l'attaquant est obligé d'émettre un signal. L'emploi des matériels présentés en exemples, au paragraphe précédent, n'est pas très compliqué. Il permet d'envisager des scénarios tels que :

- mise hors service d'une fonction qui nécessite la réception d'un signal GPS comme par exemple, certains pilotes automatiques.
- La mise hors service du téléphone GSM utilisé par une personne pour l'obliger à utiliser un autre moyen de communication.
- Brouillage d'une liaison radio au moment de l'envoi d'une télémesure qui fait état d'un acte réalisé par l'attaquant…

Profil	***Coût***	***Temps***	***Moyen***
Technicien	De 0 à 10^3 euros	De l'ordre de quelques jours	Montages électroniques spécialisés.

3.2.4.3 Réalisation d'une chaîne d'émission (attaque en intégrité).

L'émission de données cohérentes possède, à quelques détails près, les mêmes composants qu'une chaîne de réception. Les différences se situent au niveau de l'amplificateur d'émission.

Le démodulateur est remplacé par un modulateur. Un modem est par définition, à la fois, un modulateur et un démodulateur. Le récepteur, quant à lui, ne fait que démodulateur. En revanche, les générateurs de signaux font généralement office de modulateur. Le générateur de signaux peut donc être employé pour moduler le signal utile directement à la bonne fréquence (cela permet de s'affranchir de la phase de transposition) et avec la puissance désirée.

Enfin, les numériseurs font généralement CAN et CNA. Ils peuvent donc être employés pour générer un signal issu du PC. Ce signal pourra ensuite être traité par le générateur HF.

3.2.4.3.1 Utilisation des fonctions de modulation.

La logique opportuniste de notre attaquant et la recherche d'un coût réduit limitent les solutions de chaîne d'émission. On peut cependant utiliser les capacités de certains matériels électroniques de laboratoire. Le coût d'acquisition des matériels peut être limité (cf 3.2.1.1). Des générateurs et synthétiseurs possèdent des fonctions de modulation qui peuvent être exploitées pour moduler le signal. Certains de ces équipements peuvent délivrer des signaux jusqu'à 15 dBm (30 mW environ). Il ne reste qu'à mettre une antenne adaptée au besoin (cf 3.2.4.1.2.1). Un amplificateur peut être adjoint si le niveau nécessaire du signal à l'émission doit être supérieur à 15 dBm (niveau maximum fourni par notre générateur).

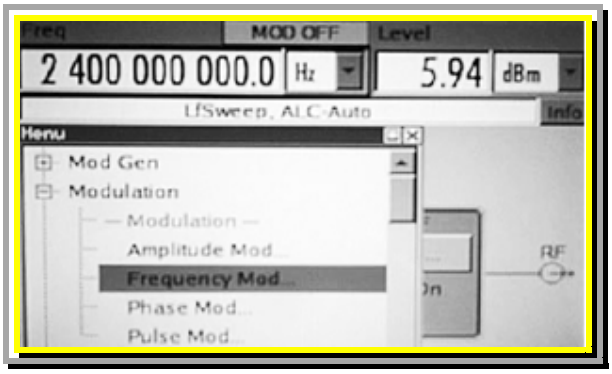


FIGURE 34 : réglage de la modulation sur un générateur de laboratoire.

3.2.4.3.2 Estimation du coût d'une attaque en intégrité.

L'attaque en intégrité dont on parle ici n'est pas un DoS comme évoqué dans le paragraphe précédent. Il s'agit ici d'une attaque élaborée dont le but est de modifier intelligemment le contenu de la communication sans fil.

Dans un premier temps, l'attaquant doit réaliser un ensemble d'action comparable à celui présenté brièvement pour l'attaque en confidentialité (§3.2.4.1.3). L'estimation de coût réalisée ci-après ne tient pas compte des coûts induits par cette première partie de l'attaque. Il s'agit uniquement d'essayer de quantifier l'effort spécifique à l'injection de données différentes. Nous sommes alors dans le schéma d'une attaque dite « man the middle ».

On part du principe que l'attaquant réussit l'attaque en confidentialité. Il doit donc modifier les bits reçus et les réinjecter dans la communication. Un effort important peut lui être demandé si le protocole de communication utilise des fonctions d'authentification des données transportées. Dans le cas contraire, il peut réaliser un émetteur tel que celui décrit au paragraphe précédent. Force est d'insister encore une fois sur l'importance de l'antenne pour gagner en distance et en qualité entre l'émetteur « pirate » et le récepteur « légitime » de l'application sans fil. En se situant non loin du récepteur « légitime », l'attaquant se trouve dans une situation comparable du point de vue de la qualité de réception. Par contre, il se place dans une situation beaucoup plus confortable que l'émetteur « légitime » car il subit moins la dégradation du signal liée à la distance et aux perturbations entre l'émetteur et le récepteur légitime. Il faut, au niveau du récepteur légitime, que le signal issu de l'émetteur de l'attaquant soit légèrement supérieur au signal issu de l'émetteur légitime.

Il faut enfin préciser que l'utilisation de la fonction de contrôle automatique de fréquence (AFC) présente sur de nombreux récepteurs, permettra à l'attaquant de se substituer à l'émetteur « légitime ». Il peut légèrement faire glisser sa fréquence d'émission. Le récepteur va rester callé sur le signal de l'attaquant, empêchant par ce moyen, l'émetteur légitime de rétablir la liaison, y compris en augmentant fortement sa puissance d'émission.

Profil	***Coût***	***Temps***	***Moyen***
Technicien	10^3 euros	De l'ordre de quelques semaines	Synthétiseur. Logiciels dédiés.

3.3) Conclusion sur l'opportunité générée par l'emploi de ce moyen.

La quantification des actions élémentaires décrites dans les paragraphes précédents montre que la réalisation d'une attaque sur un réseau sans fil est accessible à un technicien passionné, dans le cadre de ses activités privées, pour un budget qui peut être limité à quelques milliers d'euros lorsque les protocoles sont standards. Comme précisé dans le chapitre 3.2.4.1,

l'attaquant devra encore réaliser les moyens logiciels nécessaires pour traiter les données obtenues par les actions décrites précédemment (UC figure 25).

On peut donc tenter de comparer les applications sans fil et celles avec fil en fonction du niveau de difficulté d'accès physique au système cible, de la capacité d'élongation possible et de la difficulté technique liée à la réalisation des moyens décrits par les figures 6 et 7. Le tableau suivant en propose une synthèse.

	Sans fil	***Filaire***
Accès physique pour la connexion	Sans impact.	Obligatoire.
Distance	Dans le périmètre de sensibilité.	Sur site pour connexion. Dans le périmètre de sensibilité pour les SPC.
Complexité technique	Liée aux technologies radios et électroniques mises en œuvre.	Liée aux technologies mécaniques et électroniques mises en œuvre.

Il faut préciser que la distance, dans le cadre d'une application sans fil, va être fortement conditionnée par :

- différents éléments de contexte (météo, topologie géographique, bruit environnant).
- Les caractéristiques physiques de la technologie employée.
- La pertinence de la chaine E/R réalisée par l'attaquant.

On pourrait aussi parler des vulnérabilités de l'application et celles liées à son paramétrage. Cependant, elles se situent essentiellement au niveau de la composante logicielle (UC figures 6 & 7). Par conséquent, elles ne sont pas spécifiques aux applications sans fil.

On peut se rendre compte que l'emploi de moyens peu couteux, s'ils sont bien choisis, intégrés et utilisés peut permettre à un attaquant de s'éloigner significativement du système cible. Celui-ci pourra assurer plus facilement sa propre sécurité et sa furtivité. En effet, le risque n'est pas le même entre rentrer physiquement dans les locaux d'une entreprise (légitimement ou non) et se connecter via une liaison radio depuis un lieu non protégé et distant géographiquement du système attaqué. Le tableau suivant nous permet de donner un ordre d'idée entre différents niveaux de moyens utilisés par l'attaquant et l'élongation[1] envisageable en fonction de plusieurs types d'application sans fil.

Dans le tableau suivant, nous considérons de l'ordre de :

- 10^2 euros, quelques jours et sans difficulté technique majeure l'item « solution à coût faible ».

[1] Augmentation de la distance entre l'émetteur et le récepteur tout en assurant encore une qualité suffisante au signal capturé pour être traité (démodulation, dés encapsulation, accès aux données utiles…).

- 10^4 euros, le temps en mois et un niveau de difficulté pouvant être résolu par un ingénieur confirmé en ce qui concerne l'item « solution à coût plus élevé ».

	Capacité native des solutions sans fil	***Utilisation par l'attaquant de solution à faible coût***	***Utilisation de solution à coût plus élevé***
Type RFID	De l'ordre de la dizaine de millimètres	En mètre	En dizaine de mètres
Type Bluetooth	De l'ordre du mètre	De l'ordre de la centaine de mètres	De l'ordre du kilomètre
Type Wi-Fi	Plusieurs dizaines de mètres en local	De l'ordre du kilomètre	De l'ordre de plusieurs kilomètres.

Cette capacité à pouvoir réaliser ses actions à une distance élevée constitue un atout pour l'attaquant par rapport à une liaison filaire.

4 Conclusions.

L'analyse de la menace permet de caractériser les outils et savoir-faire que doit maîtriser un attaquant opportuniste. L'analyse, suivant les actions élémentaires de découverte, d'élévation de droit permet de lister les solutions envisageables et de commencer à quantifier le coût d'un scénario pour atteindre un objectif sur un système cible.

La comparaison du modèle générique d'une application utilisant une liaison sans fil et son modèle correspondant pour une application « filaire » permet de montrer le principal avantage pour l'attaquant opportuniste. Celui-ci se traduit par une diminution importante de la contrainte d'accès (élongation, sécurité) au support physique quand la liaison est radio. Dans les deux cas la difficulté technique et le coût de l'attaque sont comparables. Dans tous les cas (filaire et radio), la réussite de son action pourra être bloquée par :

- le choix d'une solution bien implémentée.
- La configuration ad hoc des équipements en imposant systématiquement la personnalisation de tous les paramètres de sécurité. Les modes usines sont souvent très permissifs et n'utilisent pas les mécanismes de sécurité pourtant proposés par les équipements.

Il conviendra d'utiliser un moyen adapté pour sa réelle plus value technique et non par simple effet de mode technologique. On peut donc conclure en précisant que pour la sécurité des

applications sans fil ou non, le problème de sécurité est à considérer dans sa globalité, « de bout en bout », et qu'il ne faut pas se limiter au seul média de transmission.

Geolocalisation and privacy

Sébastien Gambs

INRIA - Université Rennes 1
Centre de Rennes - Bretagne Atlantique
Campus de Beaulieu – 35041 Rennes Cedex France
sebastien.gambs@irisa.fr

A geolocalised system (such as a cell phone or a GPS-equipped vehicle) usually belongs to an individual and as such its location reveals the location of its owner, which is a direct threat against his privacy. For instance, the spatio-temporal data of an individual can be used to infer the location of his home and workplace, to trace his movements and habits, to learn information about his center of interests or even to detect a change from his usual behaviour. Moreover, if an adversary has some auxiliary knowledge, he can use it in combination with the location information to infer additional knowledge. For example, if the adversary has access to the social network of an individual, he can determine when the person is visiting a given friend. Geo-privacy (sometimes called "locational privacy") seeks to prevent an unauthorized entity from learning the current, past and future location of an individual. To protect the privacy of users, a sanitization process, which adds uncertainty to the data and removes some sensible information, can be performed but at the cost of a decrease of utility due to the quality degradation of the data. Other approaches based on cryptography can also be used to compute the output of a global task which depends of the local information of individuals (for instance real-time computation of a traffic map) while keeping their individual locations private. During this talk, I will give an overview of the principles of geo-privacy, and introduces some possible inference attacks on geolocalised data as well as possible counter-measures. I will also discuss the trade-off that exists sometimes between the level of privacy desired and the resulting utility for applications depending on the spatio-temporal data of individuals.

Compromising electromagnetic emanations of wireless communications

Martin Vuagnoux

LASEC / EPFL
martin.vuagnoux@epfl.ch

Martin Vuagnoux est actuellement en dernière année de thèse au laboratoire de sécurité et de cryptographie (LASEC) de l'EPFL sous la supervision du professeur Serge Vaudenay. Il a au préalable travaillé pendant 6 ans dans le domaine de la sécurité informatique comme auditeur (Ethical Hacking). Ses domaines de recherche portent sur l'analyse et la détection automatisée de vulnérabilités software, la cryptanalyse de protocole, l'ingénierie inverse de protocoles inconnus dans les systèmes embarqués, RFID, etc. ainsi que l'analyse d'émanations électromagnétiques compromettantes des appareils électroniques.

RFID : la protection des données à caractère personnel dans l' « Internet des objets »

Marie Barel

Orange Consulting, 114, rue Marcadet 75018 PARIS, France
marie.barel@orange-ftgroup.com

Résumé Quel rapport entre l'« Internet des objets » (IoT) et l'atteinte à la vie privée ? Si ce lien n'est pas encore toujours évident pour l'usager, le consommateur ou le client, Michel Alberganti, journaliste, le résume quant à lui en dénonçant ces « mille milliards de mouchards » dans un essai sur l'impact des RFID sur la vie quotidienne. Une analyse juridique permet quant à elle de caractériser l'applicabilité des textes généraux sur la protection des données à caractère personnel et de commencer à dessiner le cadre d'emploi des *tags* RFID, susceptible de contenir les risques de dérives ainsi décriés à propos de ces technologies. . . du présent.
Domaine : juridique / *Couverture géographique* : France

1 Introduction

Si la technologie RFID et les principes électromagnétiques qui la supportent ne sont pas nouveaux [1], les progrès de la miniaturisation des composants et les économies d'échelle réalisées dans la production de certaines classes de marqueurs [2] ont permis un très fort développement et une multiplication sans précédent des applications RFID.

Suivant un avis communément partagé par l'ensemble des parties prenantes (politiques, industriels, usagers/consommateurs, . . .), la problématique dominante « affectant » les technologies RFID et qui représente encore aujourd'hui un frein à son déploiement massif, au-delà des questions liées à la sécurité ou leur acceptabilité sociale, réside dans leur potentiel d'atteinte à la vie privée et la protection des données. En effet, si les technologies RFID relève de ce qu'on appelle aussi « l'Internet des objets », l'examen de la notion de donnée à caractère personnel conduit à conclure que ces technologies relèvent bien du domaine d'application de la réglementation en matière de protection des données à caractère personnel (Directive 95-46 / loi française de 1978 dite loi « Informatique et Libertés »).

Dès lors il conviendra de s'interroger sur les contraintes et les recommandations juridiques liées à leur déploiement, ce qui nécessitera préalablement d'en rappeler également les principales caractéristiques de fonctionnement.

1. Elle était déjà utilisée par la RAF, lors de la seconde guerre mondiale, pour distinguer les avions alliés des avions ennemis. . .

2. Pour indication, le prix des *tags* de classe 1 (classification selon le standard EPG Global – cf infra, section 4.1) est de l'ordre de 0,15 centimes d'euros l'unité.

2 Notion de données à caractère personnel au regard des technologies RFID

La définition des données à caractère personnel (ci-après « DACP ») figurant dans la directive 95/46/CE (ci-après « la Directive sur la protection des données » ou « la Directive ») [1] est ainsi rédigée [3] :

*« **Données à caractère personnel** : toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ».*

Ce libellé reflète, comme dans la Convention 108 [4], la volonté constante [5] du législateur européen d'adopter la définition la plus globale possible et appelle une interprétation large permettant de « *couvrir toutes les informations qui peuvent être reliées à une personne physique* ».

À cet égard, l'avis du Groupe de travail « Article 29 » adopté le 20 juin 2007 sur le concept de données à caractère personnel [3] permet en particulier de faire ressortir les éléments d'appréciation suivants :

i – quant à l'expression « toute information » : elle englobe à la fois des données « objectives » (cas d'une particularité physique par exemple) et « subjectives » (appréciations, avis, ...), qu'elles relèvent des données dites « sensibles » au sens de l'article 8 de la Directive précitée (race, opinion politique, etc.) ou qu'il s'agisse d'informations plus générales touchant non seulement sa vie privée et familiale mais également son comportement économique ou social, ses habitudes et pratiques professionnelles et toutes ses activités quelles qu'elles soient [6].

De plus, s'agissant du format des informations ou du support utilisé pour celles-ci, on relève que le concept de données à caractère personnel englobe les informations disponibles

3. La nouvelle mouture de la loi française [2], telle que modifiée par la loi du 6 août 2004, adopte une rédaction sensiblement similaire : « Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. »

4. Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Conseil de l'Europe – 28 janvier 1981) : `http://conventions.coe.int/Treaty/FR/Treaties/Html/108.htm`

5. Volonté exprimée tout au long du processus législatif. Voir par exemple : COM(90) 314 final, 13.9.1990, p. 19 (commentaire relatif à l'article 2) ; COM(92) 422 final, 28.10.1992, p. 10 (commentaire relatif à l'article 2) ; Position commune (CE) nž 1/95 arrêtée par le Conseil le 20 février 1995, JO C 93 du 13.4.1995, p. 20.

6. Cette interprétation va aussi dans le sens de celle adoptée par la Cour européenne des droits de l'homme en matière de « vie privée » : *« [...]le terme « vie privée » ne doit pas être interprété de façon restrictive. En particulier, le respect de la vie privée englobe le droit pour l'individu de nouer et développer des relations avec ses semblables ; de surcroît, aucune raison de principe ne permet d'exclure les activités professionnelles ou commerciales de la notion de « vie privée » (arrêts* Niemietz/Allemagne *du 16 décembre 1992, série A nř 251-B, pp. 33-34, ğ 29 et Halford précité, pp. 1015-1016, ğ 42). Cette interprétation extensive concorde aussi avec celle de la Convention 108 précitée.*

sous n'importe quelle forme, qu'elles soient alphabétiques, numériques, graphiques, photographiques ou acoustiques.

La relation ou le lien existant avec la personne **« concernée »** par les données faisant l'objet d'un traitement réside dans la présence d'un élément :

- soit de « contenu » : informations ayant trait à une personne particulière
- soit de « finalité » : les données sont utilisées (ou susceptibles de l'être) afin d'évaluer, de traiter ou d'influer sur le statut ou le comportement d'une personne (physique) ;
- soit de « résultat » : l'utilisation des données est susceptible d'avoir un impact sur des droits et intérêts d'une personne (traitement différencié par rapport à d'autres personnes à la suite du traitement de ces données).

ii – Une personne est considérée comme **identifiée** lorsque, au sein d'un groupe de personnes, elle se « distingue », directement ou par le phénomène de « combinaisons uniques », de tous les autres membres de ce groupe. Ensuite, la personne physique est **identifiable** lorsque, même sans avoir encore été identifiée, il est possible de le faire.

L'identification se fait normalement au moyen d'informations que l'on peut appeler « identifiants » et dont le croisement permet de rapprocher les données d'une personne physique. Cependant, pour déterminer si une personne est identifiable, les législateurs français (article 2 de la loi de 1978) et européen (considérant 26 de la Directive) précisent en outre qu'il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut (raisonnablement) avoir accès le responsable du traitement ou toute autre personne. À cet égard, la simple possibilité hypothétique de distinguer une personne n'est pas suffisante et il faut considérer un ensemble de facteurs tels que le coûts engendrés, la finalité visée, l'intérêt escompté, ... On tiendra également compte du caractère évolutif de ce critère (moyens d'identification) et donc de la nécessité de tenir compte de l'état d'avancement des technologies au moment du traitement et d'éventuels changements pendant la période de conservation.

En définitive, concernant l'applicabilité des textes généraux relatifs à la protection des données à caractère personnel en matière de technologies RFID, on relèvera la position commune à la fois de :

- l'autorité nationale de contrôle, la CNIL : [4] et [5] - Extraits : *« Dès lors que les dispositifs RFID utilisés donnent lieu à l'identification directe ou indirecte d'une personne physique, la loi informatique et libertés s'applique. »*
  « La Commission considère que les RFIDs sont des données personnelles au sens de la loi Informatique et Libertés comme à celui de la directive 95/46. »
- le Contrôleur européen de la protection des données (CEPD) [6] - Extrait : *« Le cadre législatif général en matière de protection des données, tel qu'il est défini dans la directive 95/46/CE, s'applique à la technologie RFID pour autant que les données traitées par les systèmes RFID relèvent de la définition des données à caractère personnel. »*
- la Commission européenne [7] - Extraits : *« La protection des données à caractère personnel est couverte par la directive générale sur la protection des données indépendamment des moyens et procédures utilisés pour le traitement des données. La directive*

s'applique donc à toutes les technologies, y compris la RFID. » [08] « Les droits et obligations concernant la protection des données à caractère personnel et la libre circulation de ces données, prévus par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 (. . .) et par la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 (. . .) (directive vie privée et communications électroniques) s'appliquent intégralement à l'utilisation d'applications RFID traitant des données à caractère personnel »(10ème considérant).

Ainsi, l'applicabilité des textes généraux sur la protection des données à caractère personnel (tant au niveau national qu'au niveau européen) emporte application de certains principes directeurs et impose au responsable du traitement un ensemble d'obligations principales que nous allons maintenant détailler.

3 Conséquences de l'applicabilité des textes généraux sur la protection des données à caractère personnel [1][2]

Lors de la définition de nouveaux traitements mettant en IJuvre des technologies RFID, les responsables de traitement [7] doivent ainsi veiller à appliquer les principes de finalité, de proportionnalité et de légitimation qui animent les textes (3.1). De plus, la législation oblige à l'accomplissement de formalités préalables et à apporter des garanties en matière d'information des personnes concernées, de sécurité et de confidentialité des données, ainsi que de suppression ou d'anonymisation des données (3.2).

3.1 Principes directeurs

Les principes directeurs qui constituent l'esprit des différents instruments juridiques sur la protection des données DACP sont les suivants :

finalité : ce principe, incarné aussi par l'article 6, paragraphe 1, point b), de la Directive sur la protection des données, interdit un traitement ultérieur qui est incompatible avec la ou les finalité(s) de la collecte, telle(s) que spécifiée(s) avant la mise en IJuvre du traitement.

proportionnalité : ce principe exige que les données à caractère personnel soient pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées. Ainsi, toute donnée non pertinente ne doit pas être collectée et, si elle a été collectée, doit être éliminée (article 6, paragraphe 1, point c). Ce principe exige aussi, de manière subséquente, que les données soient exactes et mises à jour (on parlera ici de « qualité » des données).

7. Rappelons que le « responsable du traitement » est la personne qui décide de la finalité et des modalités du fichier (c'est-à-dire qui définit par exemple les catégories de données à caractère personnel qui doivent être enregistrées et quelles opérations leur seront appliquées).

légitimation : conformément à l'article 7 de la Directive (dans le même sens, l'article 7 de la loi française), les données à caractère personnel ne peuvent être traitées que si ce traitement se fonde sur l'un des motifs légitimant le traitement des données.

Ces motifs juridiques légitimant le traitement de données sont :

(i) La personne concernée a indubitablement donné son consentement ;

(ii) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ;

(iii) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

(iv) le traitement est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ;

(v) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ;

(vi) le traitement est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection de la vie privée de la personne.

Sur ce dernier point, l'avis du Groupe de travail « Article 29 » [9], comme de celui de la Commission [7] ou du Contrôleur européen de la protection des données [6], est de considérer que, dans la plupart des scénarios actuellement identifiés où est utilisée la technologie RFID, le consentement des personnes est le seul motif légal que pourront invoquer les responsables de traitement pour légitimer la collecte d'informations par radio-identification.

3.2 Obligations du responsable de traitement

L'accomplissement de formalités préalables auprès de l'autorité nationale de contrôle compétente (la CNIL, en France) – formalités allant de la déclaration normale ou simplifiée à la demande d'autorisation ou d'avis – constitue un premier pan des obligations qui s'appliquent au responsable de traitement, mais aussi seulement la « partie visible de l'iceberg ».

Bien qu'elles soient encore trop souvent négligées [8], trois autres obligations principales s'imposent au responsable du traitement :

i Information auprès des personnes concernées (article 32, I de la loi de 1978) Pour garantir un traitement loyal par rapport à la personne concernée, les responsables de traitement doivent fournir les informations suivantes aux personnes concernées :
– l'identité du responsable du traitement,
– la ou les finalités du traitement

8. Comme l'illustre les motifs d'avertissement ou de sanctions prononcées par la CNIL (voir ses Rapports annuels) ou bien encore la longue série des incidents de sécurité portant sur des données à caractère personnel, qui sont relayés régulièrement par les médias...

- l'existence de droits (en particulier le droit d'accès aux données)
- le caractère obligatoire ou facultatif des réponses
- les conséquences éventuelles d'un défaut de réponse et aussi, dans la mesure des circonstances spécifiques dans lesquelles les données sont collectées :
- l'information sur les destinataires des données
- les transferts envisagés hors du territoire de l'Union européenne.

Nous verrons plus loin, dans le cadre de la section 4 à suivre, que la Commission européenne recommande [8] en outre de compléter les informations de base ainsi définies par des informations spécifiques aux projets relevant de la RFID.

ii Sécurité et confidentialité des données (article 34 de la loi de 1978) Tout responsable de traitement de données à caractère personnel doit adopter (et faire appliquer [9]) des mesures de sécurité, physique et logique, adaptées à la nature des données et aux risques présentés par le traitement. Le non-respect de l'obligation de sécurité est sanctionné de 5 ans d'emprisonnement et de 300 000 € d'amende (art. 226-17 du code pénal).

De plus, seules les personnes autorisées doivent pouvoir accéder aux données personnelles contenues dans un fichier. Il s'agit :

- des destinataires explicitement désignés (champ 12 du formulaire de déclaration normale à la CNIL) pour en obtenir régulièrement communication,
- des « tiers autorisés » ayant qualité pour les recevoir de façon ponctuelle et motivée (ex. : la police, le fisc).

La communication d'informations à des personnes non autorisées est punie de 5 ans d'emprisonnement et de 300 000 € d'amende. La divulgation d'informations commise par imprudence ou négligence est punie de 3 ans d'emprisonnement et de 100 000 € d'amende (art. 226-22 du code pénal). Du point de vue de la sécurité et de la confidentialité des données, nous soulignerons plus loin (cf. 4.2) les choix technologiques qui sont susceptibles de répondre le mieux à ces obligations, en soulevant en particulier le débat autour de la protection offerte par la communication en champ proche ou technologie NFC, qui est considérée par les partisans de la RFID comme la moins intrusive.

iii Suppression des données à l'expiration du délai utile au traitement Découlant du principe de « droit à l'oubli », le responsable de traitement doit définir la durée de conservation utile à chaque catégorie de données figurant dans un traitement DACP. La durée de conservation raisonnable des données sera déterminée en particulier en fonction de la

9. Hypothèse de la sous-traitance (voire la sous-sous-traitance) telle qu'envisagée par l'article 35 de la loi de 1978 :

« Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement. Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la présente loi. Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures. (. . .) ».

finalité et des objectifs du traitement. Enfin, au terme du délai, une procédure devra garantir la destruction des données ou, éventuellement, leur anonymisation.

La conservation des données à caractère personnel au-delà de la durée prévue [10] est puni de cinq ans d'emprisonnement et de 300 000 € d'amende (sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi). S'agissant des projets RFID, les auteurs parlent ainsi de « droit au silence des puces » (*right to silence of the chips*) et c'est surtout les moyens permettant la destruction sinon la désactivation des étiquettes (*tags*) dans le cadre de la vente au détail, qui fait débat et a justifié là aussi (comme en matière de droit à l'information) l'adoption de recommandations spécifiques [8] par la Commission européenne. Parmi les mesures techniques envisagées [10], on peut relever les propositions de commande de destruction (*kill order solution*) permettant de désactiver l'étiquette ou de bit de contrôle (*privacy bit*) pouvant être placé par le porteur lui-même en position éteinte (libre lecture des données) ou activé (refus de lecture).

4 État des recommandations d'implémentation des technologies RFID

Face à des conditions environnementales variées et des usages tout aussi diversifiés, force est de relever dans un premier temps la diversité des technologies RFID et le très large panel de *tags* disponibles sur la marché (4.1). Dès lors, suivant les caractéristiques de fonctionnement de la technologie retenue, on répondra de manière plus ou moins satisfaisante aux recommandations de la Commission européenne sur l'implémentation des principes de vie privée, de protection des données et de sécurité de l'information dans les applications supportées par la RFID (4.2).

4.1 Préalable : de la diversité des technologies RFID

Sous le vocable de radio-identification (plus souvent désignée sous le sigle RFID pour *Radio Frequency Identification* en anglais), on trouve différentes technologies permettant de mémoriser et récupérer des données à distance en utilisant des marqueurs – composés d'une micro puce (également dénommée « étiquette » ou « tag ») et d'une antenne – qui dialoguent par ondes radio avec un lecteur. D'une manière générale, les marqueurs peuvent prendre la forme tantôt d'étiquettes autoadhésives qui peuvent être collées ou incorporées dans des objets en remplacement notamment des codes barres (cas d'application existants : inventaires chez Wal-Mart, suivis industriels en chaîne de montage, gestion des fonds documentaires en bibliothèque, gestion des parcs de Vélib' à Paris et de Vélo'v à Lyon, ...), tantôt de puces RFID intégrées souvent dans des cartes sans contact pour identifier des personnes (cas d'application existants : passeports biométriques français, cartes de transport –

10. Par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés...

ex. Navigo à Paris et Badgéo à Strasbourg –, épreuves sportives telles que le Marathon de Paris ou le Tour de France de cyclisme permettant ainsi le chronométrage individuel lors du passage des lignes de départ et d'arrivée, ...).

Suivant qu'elles disposent ou non d'une alimentation autonome, les radio- étiquettes sont dites passives, actives ou semi-actives ; dans ce dernier cas, les « BAP » (pour *battery-assisted passive tags*) sont équipées comme les étiquettes actives d'une batterie, mais elles ne l'utilisent pas pour émettre des signaux et agissent en fait comme des étiquettes passives au niveau communication [11]. De plus, les radio-étiquettes diffèrent également au plan technique par différentes caractéristiques :

- leur potentiel de distance de lecture et de communication : de quelques centimètres à plusieurs centaines de mètres ;
- leurs capacités de lecture/écriture, de calcul et de stockage (plus grande dans les cas des tags actifs) ;
- la classe des fréquences qu'elles utilisent : des marqueurs utilisant les micro-ondes aux versions basse fréquence (125 à 135 kHz), haute fréquence (HF / 13,56 MHz) et UHF – Ultra Haute Fréquence (chaque classe étant soumise à une réglementation différente [12]) ;
- leur sensibilité aux obstacles ;
- les techniques d'anticollision qu'elles appliquent (méthode fréquentielle, spatiale, temporelle, systématique, ...).

Ainsi, comme le souligne Gildas Avoine dans un article sur la RFID et la sécurité [11], il n'existe en définitive *« pas beaucoup de points communs entre un tag à 15 centimes d'euros, qui ne contient qu'une simple mémoire d'une centaine de bits, et un tag à plusieurs euros, qui peut éventuellement posséder sa propre source d'énergie, contenir plusieurs kilobits de mémoire réinscriptible et effectuer des calculs cryptographiques ».*

Si l'on s'en réfère au standard EPCglobal, on peut distinguer quatre classes de *tags*. Les classes 1 et 2, qui sont les plus répandues à ce jour (elles sont aussi les moins coûteuses), correspondent à des *tags* passifs qui, dès lors qu'ils sont dépourvus de batterie, doivent se trouver dans le champ du lecteur pour s'activer (la distance de communication varie ici de quelques centimètres en HF à quelques mètres en UHF). Dans la classe 1, les *tags* sont dotés d'une mémoire limitée (typiquement 128 bits) contenant un identifiant unique et accessible en lecture seulement ; de plus, lorsqu'ils sont interrogés par un lecteur, ces *tags* envoient simplement leur identifiant. Dans la classe 2, il est possible d'implémenter quelques

11. Exemple d'application des étiquettes semi-actives : envoi de produits sous température dirigée, permettant d'enregistrer la température de la marchandise à intervalles réguliers lors du transport.

12. Les basses et hautes fréquences sont normalisées au niveau mondial. Pour les très hautes fréquences (UHF), l'Europe, l'Asie et les États-Unis se distinguent par des puissances d'émission, des fréquences (915 MHz aux États-Unis, de 865 MHz à 868 MHz dans l'Union européenne) et des réglementations différentes. Lien utile sur la réglementation en France et en Europe de l'UHF : `http://www.gs1.fr/gs1_fr/standards_gs1__1/epc_rfid/les_standards_epc`

fonctions supplémentaires tel qu'un algorithme cryptographique symétrique et de disposer de quelques centaines de bits de mémoire réinscriptible.

Les radio-étiquettes de la classe 3 sont quant à elles semi passives, et la classe 4 correspond enfin à des *tags* actifs qui ont la capacité d'initier eux-mêmes des échanges avec un lecteur (voir de communiquer entre eux) et pour lesquels les distances de communication offertes sont les plus importantes.

L'exercice de catégorisation conduit en dernier lieu à citer le projet LEGAL-IST [10] de même que le Groupe de travail Article 29 [9], qui distinguent quant à eux trois grandes catégories de *tags* suivant la nature des informations qui peuvent être révélées au sujet d'une personne et également, de la façon dont cette information est accédée. Ainsi la taxonomie des étiquettes RFID posée dans le cadre de ces travaux est la suivante :

1. *tags* ne contenant qu'un numéro d'objet (cas des marchandises dans le cadre de la vente au détail, qui sont identifiées par un code électronique unique – *Global Trade Identification Number* – et un numéro de série). Ces *tags* passifs, à première vue inoffensifs, sont l'application la plus répandue à ce jour et permettent l'identification d'objets dans une base de données de produits. Toutefois, dès lors que l'information relative à l'objet peut être liée à son acquéreur dans le cadre en particulier de la procédure d'achat et que cette donnée est conservée dans une base de données Clients, cette méthodologie peut permettre en particulier de créer des profils de consommation ;
2. *tags* contenant un numéro d'identification (ex. nř de dossier) qui révèle l'identité d'une personne après rapprochement de l'information contenue dans le tag avec une base de données *« backend »*, qui contient les données concernant l'identité de la personne ;
3. *tags* sur lesquels des données à caractère personnel sont directement stockées (il s'agit généralement de *tags* actifs, contenant des informations telles que le nom du porteur, son âge, sa nationalité, etc.).

Toutefois, quelle que soit la catégorie concernée, force est de souligner que la Commission européenne, dans sa Recommandation du 12 mai 2009, traite uniformément tous les *tags* RFID *traitant des données à caractère personnel.*

4.2 Recommandation de la Commission européenne en date du 12 mai 2009

Après un long processus de consultation [13] (`http://www.rfidconsultation.eu/`), la Commission européenne a adopté le 12 mai 2009 une « Recommandation sur l'implémen-

13. Notamment une série d'ateliers suivis d'une première consultation publique de mars à octobre 2006, qui ont permis de construire un consensus sur les problématiques clés en matière de développement des technologies RFID lesquelles ont été synthétisées dans la communication adoptée en mars 2007 [7] ; mise en place le 28 juin 2007 d'un groupe d'experts sur l'identification par radiofréquence (également connu en anglais sous le nom *« RFID stakeholders group »*) ayant entre autres pour mission de conseiller la Commission sur les éléments à insérer dans l'instrument juridique présenté ici, et qui a fait l'objet d'une consultation publique de février à juin 2008.

tation des principes de vie privée, de protection des données et de sécurité de l'information dans les applications supportées par la RFID » [8] (ci-après « la Recommandation »).

Parmi les préconisations émises, on relève deux séries de recommandations, les unes à la charge des exploitants d'application RFID, les autres en direction des États membres (en coopération avec les entreprises et les parties intéressées de la société civile).

Recommandations en direction des « exploitants d'application RFID » Tout d'abord, par « exploitant RFID », la Recommandation entend la personne physique ou morale, l'organisme public, l'agence ou tout autre organe qui, seul ou avec d'autres, définit la finalité et les modalités de l'exploitation d'une application, y compris les responsables du traitement des données à caractère personnel utilisant une application RFID.

Ensuite, il est important de souligner que la première série des recommandations à la charge des exploitants vient en complément des obligations préexistantes en vertu de la Directive de 1995 (ou de la loi nationale de 1978 transposant la Directive).

Ces recommandations particulières en direction des exploitants d'application RFID sont les suivantes :

Point 5 de la Recommandation : évaluations d'impact sur la protection des données et de la vie privée

a) Réaliser une évaluation des incidences de la mise en œuvre de l'application sur la protection des données à caractère personnel et le respect de la vie privée, y compris des possibilités d'utiliser l'application pour suivre une personne.

Le niveau de détail de l'évaluation doit être approprié aux risques que l'application peut présenter pour la vie privée et permettra en particulier d'identifier les risques de profilage ou de divulgation d'informations relatives au porteur du tag, voire de traçabilité malveillante des personnes. *b) Prendre les mesures techniques et organisationnelles appropriées pour assurer la protection des données à caractère personnel et le respect de la vie privée. c) Désigner une personne ou un groupe de personnes chargées de réexaminer les évaluations et l'adéquation constante des mesures techniques et organisationnelles pour assurer la protection des données à caractère personnel et le respect de la vie privée.*

Dans la plupart des cas, on constate sur le terrain que les mesures prises pour assurer la sécurité et la confidentialité des données DACP découlent directement de la protection globale des SI (sans analyse de risque préalable ou mise à jour portant sur le nouveau fichier ou traitement DACP ou ses évolutions) et donc qu'elles ne reflètent pas des mesures spécifiques prises en considération des risques propres de l'application ou du traitement.

S'agissant de la sécurité des applications RFID, rappelons - comme indiqué déjà plus haut - que les partisans de la RFID présentent souvent la technologie NFC comme étant la moins intrusive, leur principal argument étant que, cette technologie n'étant utilisable que sur des distances de quelques centimètres, elle suppose une démarche volontaire de l'utilisateur et ne peut donc que difficilement être utilisée à l'insu de ce dernier. Pour les détracteurs de la RFID, ces seules caractéristiques ne suffisent pas à apporter les garanties nécessaires et des possibilités d'attaque ont déjà été avancées.

En définitive, au-delà de la prise en considération des caractéristiques de fonctionnement des *tags*, les groupes d'experts mandatés par la Commission européenne recommandent en général de préférer un numéro de dossier ou une référence stockée dans le tag qui renvoie aux données nominatives du porteur (usager, client ou consommateur) stockées dans une base de données "backend", avec téléchargement sécurisé sur les lecteurs. En cas de nécessité de stocker des informations nominatives dans le tag, il conviendrait alors d'utiliser un moyen de chiffrement de ces données (tag avec crypto processeur) et de prévoir une authentification du lecteur.

d) mettre l'évaluation à la disposition de l'autorité compétente au moins six semaines avant le déploiement de l'application.

Sans préjuger du régime de formalités préalables à accomplir, la présente recommandation semble suggérer la mise en place d'une procédure d'information particulière en matière de traitements DACP utilisant les technologies RFID, qui devrait intervenir en amont de la mise en IJuvre des applications. Pour autant, il ne s'agit pas de la mise en place d'une nouvelle forme d'autorisation ou de demande d'avis puisqu'il s'agit d'une simple « mise à disposition » auprès de l'autorité nationale de contrôle.

Point 6 de la Recommandation : sécurité de l'information

Concernant les applications présentant un risque pour la sécurité de l'information ayant des conséquences pour le grand public, les exploitants doivent :

Démontrer que le niveau de sécurité de l'information et de protection de la vie privée est approprié aux risques évalués.

S'agissant des moyens à mettre en IJuvre pour conduire cette mesure, la Recommandation n'est pas vraiment prescriptive et indique que les exploitants peuvent soit élaborer de nouveaux systèmes soit appliquer des systèmes existants, comme la certification ou l'autoévaluation par l'exploitant.

Ainsi, parmi les démarches qui peuvent être utilisées, la démarche « PIA » pour *Privacy Impact Assessment*, développée par l'ICO (Information Commissionner Office, qui est l'autorité nationale de contrôle britannique), fait partie des méthodologies de référence recensées par les groupes d'experts. [Documentation disponible sur : `http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html`].

Points 7 et 8 de la Recommandation : Information et transparence concernant l'utilisation de la RFID

Élaborer et rendre publique, pour chacune de leurs applications, une politique d'information concise, précise et aisément compréhensible.

Cette politique d'information doit au moins indiquer :

- a) l'identité et l'adresse des exploitants ;
- b) l'objet de l'application ;
- c) les données qui doivent être traitées par l'application, en particulier s'il s'agit de données à caractère personnel et si la localisation des étiquettes fera l'objet d'un suivi ;
- d) un résumé de l'évaluation d'impact sur la protection des données et de la vie privée ;

– e) les risques probables que l'utilisation d'étiquettes dans l'application peut présenter pour la vie privée, et les mesures que les personnes peuvent prendre pour limiter ces risques (ex. privacy bit ou commande kill – cf. supra, section 3.2 in fine).

Prendre des mesures pour informer les personnes de la présence de lecteurs, au moyen d'un signe européen commun (ex. pictogramme) élaboré par des organismes européens de normalisation avec l'aide des parties concernées.

Le signe doit indiquer l'identité de l'exploitant et un point de contact auquel les personnes peuvent se procurer la politique d'information concernant l'application.

Points 9 à 14 de la Recommandation : applications RFID utilisées dans le commerce de détail

Les recommandations spécifiques à ce secteur portent, en résumé, sur :

– les mesures d'information de la présence d'étiquettes ;
– l'évaluation des risques pour la vie privée ou la protection des données à caractère personnel ;
– et surtout, les mesures pour :la désactivation ou le retrait, au point de vente, des étiquettes (sauf le consentement éclairé des consommateurs).

Recommandations en direction des États membres Une deuxième série de préconisations s'adressent non plus aux exploitants d'applications RFID mais aux États membres eux-mêmes, ainsi qu'aux industriels et entreprises du secteur et à toutes les parties intéressées de la société civile.

Point 4 : évaluations d'impact sur la protection des données et de la vie privée

Les États membres doivent veiller à ce que les entreprises, en collaboration avec les parties intéressées de la société civile, élaborent un cadre d'évaluation de l'impact sur la protection des données et de la vie privée.

Ce cadre doit être soumis pour approbation au groupe de travail « Article 29 » sur la protection des données dans un délai de douze mois à compter de la publication de la Recommandation au Journal officiel de l'Union européenne.

[Nous ne disposons pas, au jour de la rédaction du présent article, d'informations concernant l'état de prise en compte de cette mesure à l'échelon national.]

Point 6 : sécurité de l'information

Les États membres doivent aider la Commission à déterminer quelles applications pourraient présenter un risque pour la sécurité de l'information ayant des conséquences pour le grand public.

En effet, le spectre de « Big Brother » [14], des étiquettes « dormantes » et des capteurs furtifs plane toujours sur les applications RFID dont la Commission, en préambule de sa Recommandation, rappelle que : *« la technologie RFID permet de traiter des données, y*

14. La littérature regorge à cet égard d'exemples de dérives potentielles des applications RFID : ex. suivi abusif de personnes ayant emprunté certains types de livres révélant des centres d'intérêt politique, philosophique, religieux, syndical ou bien encore des orientations sexuelles de l'individu...

compris des données à caractère personnel, sur de courtes distances sans contact physique ni interaction visible entre le lecteur et l'étiquette de sorte que cette interaction peut se produire sans que la personne concernée s'en rende compte » (considérant 4) ; dès lors, « étant donné que la RFID peut être utilisée partout et qu'elle est pratiquement invisible[15]*, son déploiement exige d'accorder une attention particulière aux questions relatives à la protection des données et de la vie privée (. . .) »* (considérant 6).

Points 15 et 16 de la Recommandation : actions de sensibilisation

Des actions sensibilisation doivent être mises en IJuvre par les États membres à destination à la fois des pouvoirs publics et des entreprises d'une part et du grand public d'autre part.

La typologie des actions à mettre en IJuvre est définie comme suit :

- actions visant les pouvoirs publics et des entreprises (en particulier les PME) : les *informer des avantages et des risques potentiels liés à l'utilisation de la technologie RFID et les y sensibiliser, en accordant une attention particulière aux questions de sécurité de l'information et de respect de la vie privée ;*
- actions visant le grand public :
  - *recenser et fournir des exemples de bonne pratique dans la mise en œuvre d'applications RFID pour informer et sensibiliser le grand public ;*
  - *Préalablement à une plus large adoption de la technologie RFID, prendre les mesures appropriées, par exemple lancer des projets pilotes à grande échelle, pour sensibiliser davantage le public à cette technologie et aux avantages, risques et conséquences de son utilisation.*

Ces actions d'information et sensibilisation du grand public doivent notamment concourir à un consentement libre et éclairé tel qu'exigé en l'état actuel de la législation en matière de légitimation des traitements. De plus, par la communication d'informations, l'objectif selon le Groupe de travail Article 29, est bien que *« la personne concernée (soit) en état de comprendre les effets de l'application de radio-identification »* [9].

Enfin notons, au niveau de la France, que Christian Estrosi, ministre en charge de l'Industrie, a annoncé en septembre 2009 un plan de plusieurs millions d'euros pour financer 13 projets technologiques innovants en relation avec les solutions RFID / sans contact[16], action qui vient ainsi en réponse aux présentes recommandations. . .

Point 17 : recherche et développement (*privacy by design*)

Il s'agit ici de *promouvoir et favoriser l'intégration du principe de « sécurité et respect de la vie privée assurés dès la conception » à un stade précoce de développement des applications RFID.*

De plus, le soutien en faveur du développement de ces technologies (en anglais, « PET » pour *Privacy Enhancing Technologies*) vient par ailleurs en complément des efforts de la

15. Comme le rappelle la CNIL dans son 29ème rapport annuel (édition 2009), « certains prototypes sont quasi-invisibles (0,15 millimètre de côté et 7,5 micromètres d'épaisseur). »

16. Pour connaître ces 13 projets pilotes soutenus par l'État : `http://www.techniques-ingenieur.fr/article/article_6296/rfid---nfc---les-13-projets-soutenus-par-l-etat.html`

Commission pour favoriser la labellisation des produits, telle que récemment encore reconnue et insérée dans la loi de 1978 modifiée (article 11, 3, c de la loi [17] issue de la loi modificative nř2004-801 du 6 août 2004).

5 Conclusion : vers un cadre d'emploi des applications RFID

Alors que la RFID est en phase initiale de mise en œuvre, un cadre d'emploi des applications RFID se dessine progressivement au travers à la fois des groupes d'experts qui conseillent les institutions sur les éléments à insérer dans des instruments juridiques spécifiques et aussi des organismes européens de normalisation (OEN) mandatés par la Commission : CEN, CENELEC, ETSI. Dès juillet 2009, celle-ci a en outre mis en place un groupe de travail [18] chargé de l'implémentation de sa Recommandation du 12 mai, et dont les objectifs sont clairement désignés dans une Communication du 18 juin [12]. Enfin, la CNIL, en France, a institué elle aussi un groupe de travail chargé notamment de réfléchir aux évolutions nécessaires pour prendre en compte les enjeux de l'IoT et les spécificités des objets communicants (les résultats de ce groupe de travail n'ont pas été rendus publics à ce jour) ...

Références

1. Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données : `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fr:HTML`

2. Loi nř 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés (texte consolidé) : `http://www.cnil.fr/index.php?id=301`

3. Groupe de travail « Article 29 » sur la Protection des données – Avis 4/2007 du 20 juin 2007 sur le concept de données à caractère personnel [WP136] : `http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_fr.pdf`

4. CNIL, 28ème Rapport d'activité 2007 : `http://lesrapports.ladocumentationfrancaise.fr/BRP/084000197/0000.pdf`

5. Communiqué de la CNIL du 18.8.2006 portant sur la radio-identification : `http://www.cnil.fr/index.php?id=1063`

6. Avis (2008 /C101/01) du Contrôleur Européen de la Protection des Données sur la communication de la Commission intitulée « L'identification par radiofréquence (RFID) en

17. *« (La Commission) délivre un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel, après qu'elles les a reconnus conformes aux dispositions de la présente loi. »*

18. Plus d'informations sur : `http://ec.europa.eu/information_society/policy/rfid/documents/participateinworkgroup.pdf`

Europe : vers un cadre politique »– JOCE du 23 avril 2008 : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:101:0001:01:FR:HTML

7. Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions sur « l'identification par radiofréquence (RFID) en Europe : vers un cadre politique »- COM (2007) 96 Final (document du 15.3.2007) : http://ec.europa.eu/information_society/policy/rfid/doc/rfid_fr.pdf

8. Recommandation de la Commission européenne (2009/387/CE) du 12 mai 2009 sur la 1a mise en IJuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:FR:PDF

9. Groupe de travail « Article 29 » sur la Protection des données – Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification) [WP105] – Document du 19.1.2005 : http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_fr.pdf 10. Report on legal issues of RFID technology, LEGAL-IST Project – IST-2-004252-SSA / 16/05/2006 : http://www.rfidconsultation.eu/docs/ficheiros/Legal_issues_of_RFID_technology_LEGAL_IST.pdf

11.RFID et sécurité font-elles bon ménage ?, Gildas Avoine – actes de la conférence du SSTIC06 : http://actes.sstic.org/SSTIC06/RFID_et_securite/SSTIC06-article-Avoine-RFID_et_securite.pdf

12. Communication de la Commission européenne du 18 juin 2009 : Internet des objets, un plan d'action pour l'Europe – COM(2009) 278 final http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf