

# L'environnement radio, de plus en plus difficile à protéger

*Renaud Lifchitz*

*Depuis quelques années, on assiste à une véritable explosion des usages du sans-fil, notamment à travers la mouvance du « tout connecté » et de « l'internet des objets ». Il devient, dès lors, de plus en plus difficile de protéger notre environnement. Quelles sont les voies pour y remédier ?*

L'omniprésence des technologies radio dans notre environnement quotidien se fait de plus en plus ressentir, chaque objet de notre environnement est voué à devenir communicant pour devenir intelligent et ainsi nous faciliter la vie. Mais cela soulève en réalité pas mal de questions.

Il est difficile d'être exhaustif quand il s'agit de recenser ces usages, tant ils sont nombreux, qu'ils soient grand public ou professionnels: contrôle d'accès (badges sans contact), ouverture de portes (garage, voiture...) et interphones, alarmes sans fil, capteurs domotiques, drones, cartes sans contact (cartes bancaires NFC, cartes Velib', Autolib, Navigo...), réseaux cellulaires (GSM, téléphonie domestique DECT), bureautique sans fil (souris, clavier, casque), dispositifs médicaux (pacemakers, pompes à insuline...), dispositifs de navigation ou guidage (GPS), radiopilotage horaire (GSM NITZ, DCF77...), talkies-walkies, radios personnelles, radio professionnelle (PMR)...

Beaucoup de protocoles radio ont été conçus il y a plus de dix ans, alors que les besoins en sécurité étaient considérés comme moindre et que la radio était un environnement vierge considéré comme sûr, tous comme l'étaient les premiers réseaux filaires ou le réseau Internet à ses débuts. Certains protocoles radio disposent de fonctions de sécurité plus ou moins avancées (par exemple Bluetooth 4.0 et ZigBee), mais en pratique rares sont les dispositifs à utiliser, qui plus est correctement, ces fonctions.

On trouve 3 principales familles d'attaques sur les protocoles radio: brouillage, écoute passive, et spoofing (usurpation). Le brouillage peut être volontaire (émission de bruit à l'aide d'un amplificateur par un attaquant) ou involontaire (interférences ou obstacles physiques). Il est généralement difficile de s'en protéger à part en circonscrivant physiquement le périmètre physique d'usage du protocole radio. L'écoute passive va toucher tous les protocoles non suffisamment chiffrés, à l'heure actuelle une majorité des protocoles radio. Elle va permettre à un attaquant de prendre connaissance des données ou commandes envoyées par radio entre l'émetteur et le récepteur. Enfin, le spoofing va consister à émettre du trafic à la place de l'émetteur légitime, soit en rejoignant du trafic écouté passivement (si par exemple il est chiffré), soit en le modifiant (valeurs, données, commandes), de façon à atteindre l'intégrité ou la disponibilité du système distant.

Auparavant, il était très difficile d'auditer ou attaquer un protocole radio, faute d'outil suffisamment agile. En effet, pour chaque protocole radio il fallait utiliser des périphé-

riques matériels spécifiques, dont beaucoup sont bridés pour éviter l'écoute passive ou l'injection arbitraire de trafic. Ces dernières années, ces obstacles ont été levés avec l'avènement de la radio logicielle. Il s'agit de périphériques génériques d'acquisition et/ou d'émission brute de signal radio, tout le reste (modulation/démodulation, codage/décodage) se faisant de manière logicielle, donc ils sont reprogrammables à volonté, ce qui change la donne. Certains périphériques fonctionnent sur de larges bandes, quasiment de 0 à 6 GHz, et permettent d'étudier la quasi-totalité des fréquences civiles et militaires, et ce, avec un unique matériel, éventuellement agrémenté de différentes antennes sélectives par bandes de fréquences retenues. Leur utilisation est de plus en plus aisée grâce à des filtres et blocs prédéfinis que l'on peut assembler graphiquement pour les programmer (citons par exemple le framework open source GNU Radio Companion).

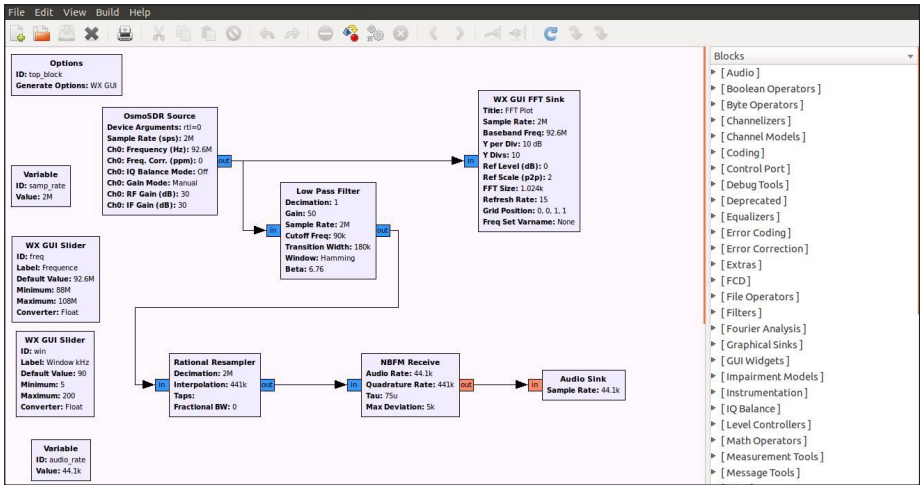


Figure 1 - Création d'un récepteur FM en radio logicielle avec GNU Radio Companion

Des périphériques connaissent un certain succès actuellement, les clés USB de réception TV TNT basés sur le chipset Realtek RTL2832U (cf. <http://sdr.osmocom.org/trac/wiki/tt1-sdr>). Très accessibles, autour de 20 euros, elles permettent en réalité de capter les fréquences de 50 MHz à 2200 MHz environ, ce qui en font des outils d'audit déjà très accessibles et très puissants. Avec ce type de matériel, il est possible d'analyser le protocole GSM, de capter la TV TNT et la radio FM, l'essentiel des capteurs et télécommandes radio, les talkies-walkies, ou encore les protocoles de géolocalisation et de diagnostic d'avaries sur les avions (ADS-B et ACARS). Les auditeurs les plus agueris s'orienteront vers d'autres équipements, les HackRF ou USRP, qui ont des capacités d'émission et des bandes passantes plus larges. Ceci en fait des outils d'audit et d'attaque redoutables.

Parmi les technologies récentes particulièrement vulnérables, nous pouvons citer les systèmes domotiques (caméras, capteurs, prises commandées à distance), les cartes bancaires sans contact, les systèmes d'alarme, les pacemakers, et les bips de garages ou de voitures. L'essentiel de ces systèmes à l'heure actuelle est démuné de fonctions de sécurité et permet l'écoute passive et le rejeu de façon assez simple. Pour ces raisons, le vol de voitures aux États-Unis est d'ailleurs devenu un véritable sport.

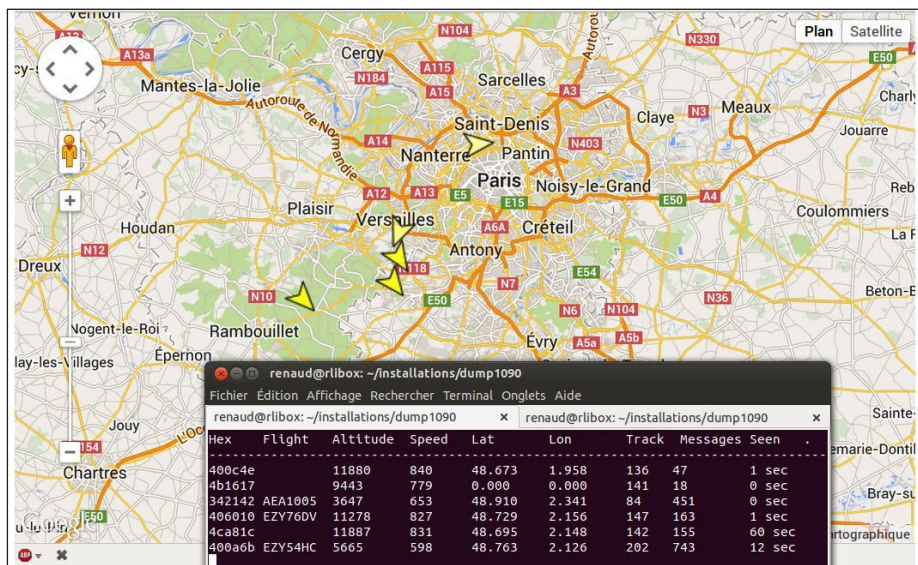


Figure 2 - Réception de trames ADS-B et géolocalisation d'avions

Ce constat est préoccupant et il est désormais urgent que les industriels cessent d'utiliser des protocoles connus comme étant vulnérables pour des fonctions critiques (paiement, sécurité de biens et bâtiments, sécurité et santé de la personne). Il appartient aux consortiums qui conçoivent les protocoles radio d'élargir leurs consultations aux professionnels de la sécurité lors de la conception de ces protocoles, et de ne plus considérer les réseaux sans fil comme des réseaux de confiance. La sécurité ne doit pas être non plus confiée aux développeurs d'applications sans fil, qui ne sont pas dans l'immense majorité des experts sécurité et ne maîtrisent pas la théorie derrière une bonne authentification ou un bon chiffrement. C'est véritablement dans les couches basses d'un protocole que doivent être implémentées les fonctions de sécurité, qui devraient pouvoir être utilisées de manière transparente par défaut par les développeurs. Ces aspects sont bien trop souvent négligés dans la conception des protocoles. De plus, beaucoup d'industriels succombent à la pression du « time to market », au détriment de la confiance du consommateur et de leur image de marque future. Les acteurs du secteur sans-fil doivent faire des progrès, les recettes existent et sont connues.

Les fonctions de sécurité qui devraient être présentes dans tous les protocoles radio sont un chiffrement de qualité satisfaisante, un mécanisme anti-rejeu, une authentification de l'émetteur, et un mécanisme d'authenticité et intégrité (signature électronique). Une plus grande disponibilité (QoS) peut aussi être atteinte à l'aide des concepts issus de la radio cognitive, notamment le choix intelligent de canaux radio, à l'épreuve du brouillage. À partir de là, nous pourrions avoir confiance en ces protocoles radio promis à un bel avenir.

Cet article a fait l'objet de présentations par l'auteur aux JSSI et aux GS DAYS 2014 (cf. <https://speakerdeck.com/rlifchitz/lenvironnement-radio-de-plus-en-plus-difficile-a-protger>).