

# Le GSM-R est-il une cible de choix pour les hackers ?

Le déploiement du GSM-R, standard de communication sans fil dédié à l'industrie ferroviaire, pose des problèmes de sécurité, a déclaré un spécialiste du secteur, **Stefan Katzenbeisser**, lors de la 28ème édition du Chaos Communication Congress ([28C3](#) « *Behind Enemy Lines* ») organisée à Berlin du 27 au 30 décembre 2011.

## Le GSM-R et la problématique du chiffrement

M. Katzenbeisser est professeur en informatique et ingénierie de la sécurité à l'université technique de Darmstadt, en Allemagne. « *Le principal problème que je vois concerne le processus de changement des clés de chiffrement. Ce sera un gros souci à l'avenir : comment gérer ces clés en toute sécurité ?* », a-t-il déclaré à l'agence *Reuters*.

Les clés de chiffrement seraient chargées sur un support physique, une clé USB par exemple, avant d'être transmises aux personnes autorisées, et ce, avec le risque qu'un pirate informatique s'en empare et mène une attaque par déni de service. Ces incidents entraîneraient des retards et d'autres soucis logistiques qui ne seraient pas sans conséquences sur l'équilibre budgétaire des sociétés concernées.

Ce risque reste limitée, selon la société Network Rail chargée de déployer le GSM-R sur l'ensemble du réseau ferré anglais d'ici la fin 2014. « *Le GSM-R est un système robuste et sûr* », a déclaré un porte-parole de Network Rail à la BBC.

## Le successeur du réseau de télécommunications analogiques (RST)

La gestion du trafic ferroviaire a longtemps été contrôlée par des réseaux de télécommunications analogiques (Radio Sol-Train ou RST). A la fin du 20ème siècle, plus de 35 systèmes différents étaient utilisés à travers l'Europe. Le GSM-R est une version du GSM (2G) davantage sécurisée utilisant les spécifications EIRENE – MORANE, censées garantir une communication sans coupure jusqu'à une vitesse de déplacement du train de 500 km/h.

La technologie a été lancée à l'initiative d'un groupe d'industriels pour doter le rail européen d'un standard numérique unique de communication, interopérable avec les solutions utilisées par différents opérateurs.

Support du Système européen unifié de sécurité, signalisation et supervision des transports ferroviaires (*European Rail Traffic Management System* ou ERTMS), le GSM-R permet notamment d'effectuer des appels point à point, de passer des appels propriétaires et/ou groupés (fonctionnalité *Advanced Speech Call Items* ou ASCI), de joindre un conducteur (fonctionnalité d'adressage fonctionnel) ou un contrôleur de zone en fonction de sa localisation géographique et, enfin, d'assurer le contrôle des appels au sein de groupes d'utilisateurs ferroviaires.

Progressivement déployée, la technologie GSM-R est d'ores et déjà utilisée dans certaines régions d'Europe, d'Afrique et d'Asie. En France, l'opérateur ferroviaire RFF (Réseau ferré de France) gère ce déploiement et sa maintenance pour le compte de la SNCF.