L’attaque par impulsions électromagnétiques des réseaux ferroviaires | Le Net Expert Informatique

L’attaque par impulsions électromagnétiques des réseaux ferroviaires

De nouveaux capteurs pour faire face aux attaques EM dans le secteur ferroviaire

Virginie Deniau, coordinatrice du projet SECRET, discute des dispositifs mis au point par son équipe afin d'identifier les attaques par impulsions électromagnétiques (EM) et permettre aux opérateurs de passer à un mode sûr.
Il y a onze ans, l'attentat du métro de Madrid a prouvé que le système de sécurité ferroviaire européen n'était pas assez efficace. Mais aujourd'hui où l'équipement ferroviaire (comme dans la plupart des autres industries) est de plus en plus normalisé et connecté, entre autres, un autre type d'attaque plus insidieuse est devenue plus probable: les attaques par impulsions électromagnétiques (EM). Un projet financé par l'UE a mis au point des technologies de détection permettant au secteur de faire face à cette nouvelle menace.
Saviez-vous que bientôt il y aura autant d'appareils connectés que d'êtres humains sur Terre? Cinq milliards de ces appareils sont actuellement opérationnels et ce nombre devrait atteindre les 25 milliards d'ici 2020. Évidemment, chaque nouveau type d'appareil connecté nous rapproche de l'aube des villes intelligentes et de leurs bénéfices attendus. Mais d'un autre côté, comme le montrent les récentes actualités, les pirates informatiques et autres passionnés par la technologie animés de mauvaises intentions représentent une menace croissante pour la sécurité.
Dans le secteur ferroviaire européen par exemple, l'homogénéisation des technologies de réseau et l'utilisation accrue des communications sans fil a rendu très probable le scénario d'une attaque EM. Les brouilleurs de communication sont faciles à utiliser et aisément accessibles à tous grâce à Internet, autrement dit les communications pourraient éventuellement être brouillées, pour notamment provoquer des retards, un blocage ou une déviation des trains.
Pour permettre au secteur de faire face à cette nouvelle menace, le projet SECRET (SECurity of Railways against Electromagnetic aTtacks) a développé un ensemble de sondes de détection capables d'identifier des attaques EM lorsqu'elles surviennent, afin que les opérateurs des équipements ferroviaires puissent passer le réseau à un « mode sûr » inviolable par le type spécifique de l'attaque EM utilisé.
Virginie Deniau, coordinatrice de SECRET, discute la probabilité du scénario d'attaque par impulsions EM, des dispositifs mis au point par son équipe et de la façon dont le secteur aura bientôt besoin de s'adapter à cette nouvelle réalité.

Quelles sont les chances d'un scénario d'attaque EM?
La définition d'une attaque par impulsions EM évolue parallèlement à la multitude des applications de technologies de communication sans fil. Par le passé, les attaques EM découlaient de la production d'interférences à haute tension (Electromagnetic pulse ou micro-ondes haute tension) intentionnelles capables de perturber ou d'endommager l'équipement électronique. Aujourd'hui, ces équipements peuvent être enclenchés par une commande ou une information transmise par des liens sans fil, autrement dit, il est désormais plus facile de perturber les informations transmises et d'endommager l'équipement. Ces attaques nécessitent un signal moins puissant qui peut être généré par des appareils mobiles et autres dispositifs discrets.
Ainsi, d'un point de vue technologique, la probabilité d'une attaque augmente proportionnellement à la vulnérabilité des infrastructures. Il est cependant difficile d'établir une nette probabilité car aujourd'hui il est impossible de faire la distinction entre un défaut technique et une attaque EM. Les attaques EM par un signal de puissance relativement « faible » impliquent des perturbations mais aucun dégât permanent.

Vous avez mentionné les dispositifs mobiles. Cela signifie-t-il que n'importe qui est capable d'effectuer de telles attaques?
La connaissance de la cible est essentielle si l'on veut définir les moyens nécessaires pour effectuer une attaque EM. De nos jours, les brouilleurs de communications publiques peuvent être facilement achetés mais leur puissance et action sont restreintes.
Maintenant, si nous prenons en compte les services de communication professionnels ou de sécurité, il faut des dispositifs spécifiques pour ce genre d'attaques. Ces appareils sont habituellement limités au marché professionnel ou doivent être conçus à partir de zéro. Mais cela nécessite un certain niveau d'aptitudes et de connaissances.
Néanmoins, lorsque ces applications professionnelles sont soutenues par des services publics sans fil, elles peuvent être perturbées par des brouilleurs communs. Cela peut donc poser de nombreux problèmes, et la sécurité et l'importance des services sans fil doivent être sérieusement prises en compte.

SECRET se concentre sur la sécurité ferroviaire. Quelles pourraient-être les conséquences des attaques EM dans ce secteur?
Le principal risque direct est la perturbation du trafic ferroviaire. Il serait possible d'empêcher le départ des trains, de forcer les arrêts de train mais cela provoquerait d'importantes pertes financières et des situations ingérables. Cependant, il est difficile d'évaluer précisément les risques en cascade qui dépendent des caractéristiques de chaque réseau ferroviaire (exploitation, infrastructure, applications, etc.).

Pouvez-vous nous en dire davantage sur les outils que vous avez développés?
La vision de SECRET est que si on est capable de détecter une attaque EM avec certitude, nous pouvons alors tenter de passer à un mode de sécurité ferroviaire parfaitement adapté à la situation et permettant aux opérateurs de regagner le contrôle. Le défi consiste donc à développer des solutions de détection rapide et fiable. C'est dans cet esprit que de nombreuses solutions ont été étudiées dans le cadre de SECRET. Certaines pourraient être mises en œuvre au sein des terminaux de communication et d'autres nécessiteraient des dispositifs dédiés mais offrent l'avantage de suivre divers canaux de communication.
À des fins de résistance, nos capteurs ont été couplés à un terminal d'acquisition et de décision chargé d'analyser les résultats de ces capteurs de détection et de commander une plateforme de télécommunications reconfigurable. D'après les résultats sortants des capteurs, le terminal de décision dirige les messages à transmettre vers le canal de communication le plus résistant à l'attaque EM. Manifestement, cette approche nécessite le déploiement de nombreux réseaux de communication.

Quand prévoyez-vous la commercialisation de la technologie de SECRET?
En raison de la mobilité et du large spectre d'environnements ferroviaires électromagnétiques, la fiabilité et l'absence totale de défauts des solutions de détection est difficile à démontrer à bord d'un train. Néanmoins, lorsque le train est immobile, les technologies de SECRET peuvent être vraiment efficaces. Nous pouvons donc envisager une commercialisation relativement rapide à l'aide de ces technologies afin de protéger les gares et autres infrastructures cruciales.
Parallèlement, les technologies de SECRET peuvent contribuer à l'évolution des normes de télécommunications employées dans les infrastructures critiques. Au lieu d'améliorer la performance en termes de vitesse de données, les normes peuvent évoluer pour fournir des informations en temps réel quant à la qualité des services ou de la présence des signaux brouilleurs (intentionnels ou non-intentionnels). Elles pourraient ensuite fournir un diagnostic pertinent et activer le processus d'intervention adéquat.

Les voies ferrées européennes font déjà l'objet d'une pression économique et sécuritaire importante. Pensez-vous que le secteur peut soutenir les coûts supplémentaires qu'impliquerait la mise en œuvre de solutions de SECRET?

Je pense qu'avec cette menace croissante, il sera nécessaire de garantir la résilience du réseau ferroviaire contre de telles attaques. Habituellement, les systèmes de communication sans fil ne représentent qu'un faible pourcentage du budget d'un projet ferroviaire. Or, ces systèmes sont essentiels dans les plans opérationnels et de sécurité. Les attaques à impulsions EM peuvent avoir des conséquences considérables en termes de coût, et avec un déploiement trop simple, elles peuvent également faire l'objet d'actions malveillantes. Ainsi, une solution contre les attaques EM devrait être envisageant en trouvant un équilibre entre les risques, les impacts et les investissements.

Quels sont vos projets maintenant que le projet touche à sa fin?
Nous aimerions tester notre analyse d'attaques EM avec d'autres types d'attaques telles que les attaques physiques ou les cyber-attaques. En effet, les attaques de brouillage peuvent facilement entraîner d'autres actions malveillantes afin d'empêcher les transmissions vidéo ou d'alarme. Par conséquent, les analyses de risques doivent prendre en compte le risque d'une combinaison d'attaques physiques et de brouillage. Nous pensons également que l'architecture de détection pour les attaques EM proposées dans SECRET devrait être associée à d'autres outils de surveillance de l'infrastructure afin d'obtenir une meilleure vue de ce qui se passe sur le réseau en temps réel.

Pour plus d'informations voir: projet SECRET
