# Compteur électrique intelligent: quand le hacking mène au black-out général

17/10/2014 à 10h31 Mis à jour le 17/10/2014 à 20h26

Éteindre l'électricité chez son voisin, envoyer des faux rapports de consommation, provoquer une panne générale… Certains compteurs intelligents sont facilement piratables, comme viennent de le montrer deux chercheurs en sécurité.

La belle promesse des « smarts cities » - ou villes intelligentes - ne serait-elle qu'une illusion? A l'occasion de la conférence Black Hat Europe 2014, deux hackers espagnols ont montré que l'interconnexion des infrastructures urbaines cachent aussi d'énormes risques. Javier Vazquez Vidal et Alberto Garcia Illera ont, en effet, décortiqué l'un des nombreux compteurs électriques intelligents déployés dans leur pays natal, histoire de voir son niveau de sécurité. A première vue, l'engin semble solide. Les communications entrantes et sortantes sont toutes chiffrées en AES 128 bits. Et quand on essaye de regarder sous le capot, un dispositif de protection le bloque automatiquement, nécessitant l'intervention d'un technicien. Donc tout va bien ?

Grosse erreur ! Les deux compères se sont plongés dans les entrailles électroniques de l'appareil pendant plusieurs mois et ont analysé son fonctionnement par rétro-ingénierie. Ce qu'ils ont découvert n'est pas très glorieux. Ainsi, le mode bloqué peut être contourné sans grande difficulté, car il est possible de modifier directement certaines parties du firmware. La clé de chiffrement AES est stockée dans le processeur et peut être lue au moment de la mise en route. Et en plus, il s'avère que cette clé est la même pour tous les appareils !

MM. Vidal et Illera décortiquent le firmware d'un compteur intelligent. - MM. Vidal et Illera décortiquent le firmware d'un compteur intelligent.

Mais ce n'est pas tout. Une fois que l'on a le contrôle d'un appareil, il est possible de détourner ses fonctionnalités. Par exemple: envoyer des faux rapports de consommation pour diminuer sa note d'électricité. Comme les compteurs fonctionnent en réseau, on peut également couper l'électricité chez son voisin. Il suffit d'envoyer la bonne commande. Autre possibilité: faire passer son compteur pour celui de quelqu'un d'autres en changeant l'identifiant (spoofing).

On peut aussi rajouter des fonctionnalités, en modifiant le firmware, ou simplement siphonner les données des autres compteurs pour se constituer une petite base de données. Ca peut toujours servir. « Théoriquement, on peut même imaginer la création d'un ver qui infecte les compteurs de proche en proche puis génère un black-out général dans une quartier ou une ville », souligne Javier Vidal. On est plus très loin du scénario catastrophe.

Un modèle ausculté par les deux hackers. - Un modèle ausculté par les deux hackers.

Les deux hackers ont pris contact, de manière indirecte, avec le fabricant du compteur intelligent, pour l'informer des vulnérabilités trouvés. Pour l'instant, il n'y a que peu de réaction. Compte tenu de la très mauvaise conception de l'appareil, ils estiment que le tir ne sera pas facile à corriger. MM. Vidal et Illera n'ont pas révélé le nom du fabricant, mais, d'après les images montrées, il est très probable que le modèle ausculté est celui de la société Meters And More, qui fournit les compteurs intelligents d'Endesa. Espérons qu'EDF aura fait un meilleur choix avec Linky, le compteur communicant qui devrait équiper tous les foyers français d'ici 2021.