Comment ouvrir 4 millions de chambres d'hôtel en quelques lignes de code

Nous avons consacré un billet à la (merveilleuse) histoire du libre circuit imprimé Arduino.

Puis, tout récemment, nous avons mis en exergue une conférence TED de l'un de ses créateurs qui s'enthousiasmait de la diversité et originalité des projets dérivés d'Arduino.

Il aurait pu ajouter celui-ci…

PS : Alors, Ritz ou Carlton cet été pour les vacances ?

Un hacker « black hat » peut ouvrir 4 millions de chambres d'hôtel grâce à un microcontrolleur Arduino

Black Hat hacker gains access to 4 million hotel rooms with Arduino microcontroller

Sebastian Anthony – 25 juillet 2012 – ExtremeTech
(Traduction Framalang : esperolinuxien, ZeHiro, Martin)

Mauvaise nouvelle: Pour moins de 50$ de matériel et un petit peu de programmation, un hacker peut ouvrir, instantanément et sans laisser de trace, des millions de chambres d'hôtel protégées par une carte-clé.

Ce hack a été présenté par Cody Brocious, un développeur de chez Mozilla, à la « Black Hat Security Conference » de Los Angeles. 4 millions de chambres d'hôtel sécurisées par les serrures programmables à carte vendues par Onity sont menacées. Selon Bocious, que l'on devrait réprimander pour ne pas avoir divulgué le hack à Onity avant de le rendre public, il n'y a pas de correction facile par une mise à jour du firmware. Si les hôtels veulent sécuriser les chambres de leurs clients, chaque serrure devra être changée.

Le hack est entièrement détaillé sur le site internet de Borcious, mais en quelques mots : à la base de chaque serrure Onity se trouve un petit port alimentation DC (simplement identique à celui de votre vieux téléphone Nokia). Ce port est utilisé pour recharger la batterie de la serrure, et pour programmer cette dernière avec le « sitecode » de l'hôtel – une clé 32-bit identifiant celui-ci. En connectant un microcontrolleur Arduino dans le port DC, Brocious a trouvé qu'il pouvait simplement extraire cette clé 32-bit de la mémoire de la serrure. Aucune authentification n'est requise – et la clé est enregistrée à la même place dans chaque serrure Onity.

Le meilleur : en introduisant ce code 32-bit dans la serrure… elle s'ouvre ! D'après Brocious, 200 millisecondes sont simplement nécessaires pour lire le "sitecode" et ouvrir la serrure. « Je le branche, l'allume, et la serrure s'ouvre » confie Brocious. Sa mise en œuvre actuelle ne fonctionne pas avec toutes les serrures, et il ne compte pas mener plus loin ses investigations, mais ses documents de recherche prouvent de manière très claire que les serrures Onity,

assez ironiquement, ne disposent même pas de la sécurité la plus élémentaire.

J'aimerais pouvoir dire que Brocious a consacré des mois à ce hack, pratiquant une rétro-ingénierie minutieuse du protocole des serrures Onity, mais la vérité est bien plus triste. « Avec cette simplicité enfantine, je ne serais pas surpris si un millier d'autres personnes avait trouvé la même vulnérabilité et l'avais vendue à d'autres gouvernements » déclare Brocious, dans une interview accordée à Forbes. « Un stagiaire à la NSA pourrait trouver cela en cinq minutes. »

C'est de cette manière qu'il justifie la divulgation au public de la vulnérabilité : si les agences de sécurité et les milices privées ont déjà accès à des millions de chambres d'hôtel, alors de cette manière Brocious contraint Onity a corriger son erreur. Informer le public signifie aussi que nous pouvons trouver d'autres méthodes pour sécuriser nos chambres – avec des chaînes ou des verrous blindés à l'intérieur des chambres par exemple.

Concernant la justification d'Onity pour un tel manquement à la sécurité, personne ne sait. Généralement, tant que les affaires roulent, sécuriser un système est une dépense inutile – jusqu'à ce que celui-ci soit hacké. Ce genre de vulnérabilité n'a rien d'extraordinaire venant d'une entreprise traditionnelle – en général, une entreprise n'embauche un spécialiste de la sécurité qu'après avoir connu un hack surmédiatisé. Pour une entreprise dont le rôle est de sécuriser le sommeil de millions de personnes chaque nuit, Onity aurait pu faire preuve d'un peu plus de précautions.

Crédit photo : Cory Doctorow (Creative Commons By-Sa)