springcard

YOUR EXPERT IN CONTACTLESS SOLUTIONS

version

technological watch

NFC for protecting smart devices communication

In the previous article, we discussed the security in the Internet of Things (IoT). Today we will explain why using **NFC technology** could be an answer to the need of protecting smart devices communication.

INTERNET OF THINGS FOR YOUR EVERYDAY LIFE

People have responded incredibly well to the smart devices market with **sales skyrocketing in 2014**. Sales of e-wristbands went up by an astonishing 684% in the second trimester, and the entire Internet of Things market continued to grow strongly throughout 2015. However, the numbers fell slightly short of predictions made by analysts.

Today, all the smart devices sold in the top 5 are objects worn on the wrist. But the body is **such a huge field of potential innovations** for this kind of technology. Future will bring us many more products such as connected clothes, shoes, etc. The **expected increase concerning smart devices is absolutely amazing**, especially for a culture obsessed with measuring and quantifying their body every day.

WILL TOMORROW THIEVES BE HACKERS ?

Between gadgets and medical devices, the service provided is very braod. And -certainly in the first cas- the need for data protection is not perceived as urgent. About 11% of French people owned a smart device related to health and wellbeing; the **glycemic reader** remains to be the main product sold on the medical smart market. In this case, its use is regulated and data protection is a real demand since **medical confidentiality is involved**.

Obviously, smart devices don't only concern health and wellbeing fields but also all the aspects of home life. And once again the **expectation of data protection is strong**.

But why would it be interesting to know about someone's heat, intrusing warning system, and opening/closure front door settings ? Because they show evidence of someone is in or not and of the possibility to break into the house. **The slightest security breache in someone's smart-devices-network exposes us and makes us vulnerable to any kind of hostility**.

MARIE-ANTOINETTE AND THE NECESSITY OF AN OUT-OF-BAND CHANNEL

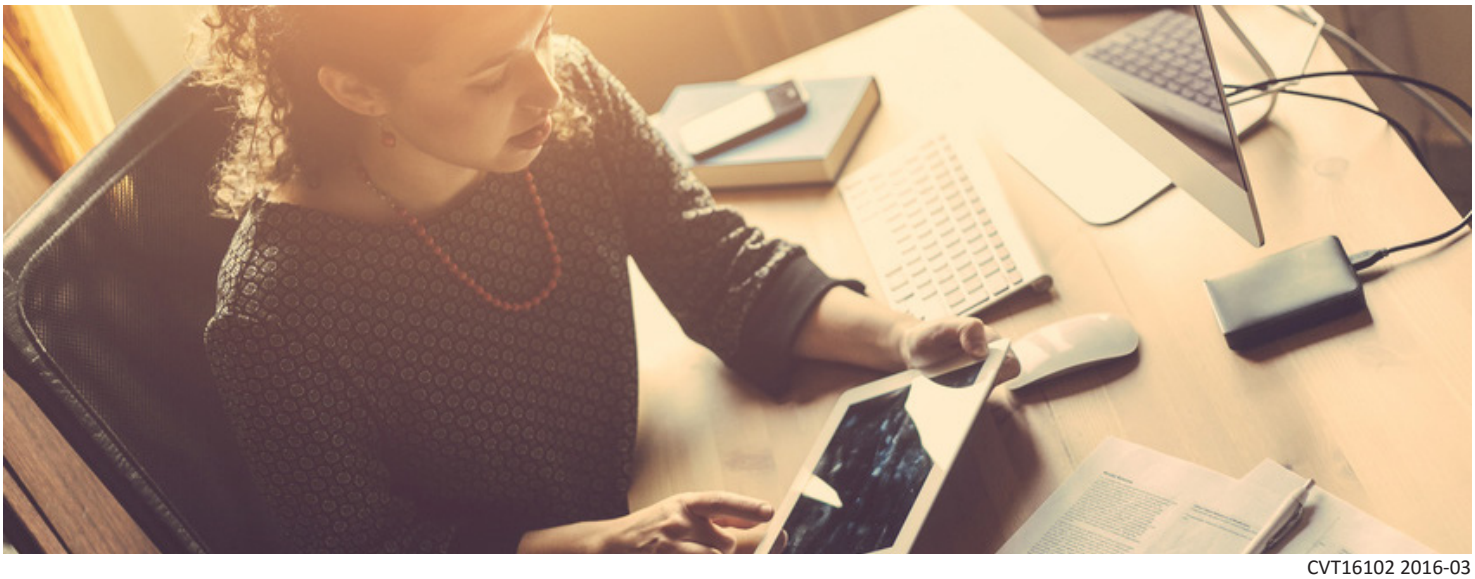
From June 1791 to August 1792, Marie-Antoinette fed the flamme of a passionate correspondance with a young Swedish officer. Their letters were **encrypted** with a complex "poly-alphabetic" code. Two elements are necessary to decrypt the letters - a decrypting table and a **keyword**. The keyword is the only word for which the table is used and it changes with each letter.

Of course, only Marie-Antoinette and the officer were privy to the keyword, and to avoid anyone else stumbling accross it, **the keyword was sent in a different manner to the letters**. To this day, we don't know how they sent the keyword but theories range from it being hidden in hat seams to being smuggled in pieces of furniture.

IS NFC TECHNOLOGY THE BEST TECHNOLOGY FOR PROTECTING SMART DEVICES COMMUNICATION?

NFC (Near Field Communication) is a wireless communication technology which main asset in this case is its **short communication distance** (till 10cm). This would point to NFC technology to be the best way to communicate the equivalent of the **keyword** of Marie-Antoinette'system explained above. And then it would be the security **keystone** of smart-devices-network. A short communication distance means indeed that **nobody can intercept data without being identified**.

It may be so in theory, but in an upcoming article, we will see how pratice turns upside down the theory.



springcard
YOUR EXPERT IN CONTACTLESS SOLUTIONS

version

technological watch

Le NFC pour la protection des objets connectés

Dans l'article précédent, nous avons évoqué les enjeux de la sécurité liée à l'usage des objets connectés (Internet of Things). Dans celui-ci, nous verrons pourquoi le NFC peut être une réponse aux attentes de protection des données des objets connectés.

LES OBJETS CONNECTÉS PRENNENT PLACE DANS LE QUOTIDIEN

Le grand public accueille très favorablement les technologies en lien avec les objets connectés : le marché mondial des bracelets connectés a connu **une augmentation massive de 684 %** au deuxième trimestre 2014 et les ventes mondiales d'objets connectés ont continué à croître fortement en 2015, alors même que les volumes écoulés par les fabricants restent encore loin des estimations ambitieuses avancées par les analystes !

Le top 5 des objets connectés les plus vendus est dominé par des objets qui se portent au poignet. Mais d'autres formes d'**objets connectés en lien avec le corps** vont se développer : vêtements, chaussures, etc. La **croissance attendue** dans ce domaine est forte, et ce d'autant plus dans une société obsédée par l'observation et la mesure du corps.

LES VOLEURS DE DEMAIN SERONT TOUS DES HACKERS ?

Entre simple gadget et appareil médical, le service rendu par l'objet connecté est complètement différent et la nécessité de protéger ses données n'apparaît pas aussi sensible. Environ 11% des Français posséderaient un objet connecté en lien avec **le bien-être et la santé**. Le produit phare du marché médical connecté est le **lecteur de glycémie**. Son utilisation est réglementée et **la sécurité des données est ici un impératif puisque le secret médical est en jeu**.

Les objets connectés ne concernent bien sûr pas seulement les secteurs du bien-être et de la santé, mais aussi toute la sphère de la **vie domestique**. Et là aussi, les attentes en matière de sécurité des données sont fortes.

Mais en quoi un réglages de chauffage, de l'alarme anti-intrusion, de l'ouverture de la porte d'entrée intéresseraient qui que ce soit ? Parce qu'ils sont autant d'indices d'une présence ou d'une absence sur le lieu d'habitation et donc de possibilités d'intrusion. **La moindre faille dans le système de sécurité des objets connectés d'une personne la met à nu et la rend vulnérable**.

MARIE-ANTOINETTE ET LA NÉCESSITÉ D'UN OUT-OF-BAND CHANNEL

De juin 1791 à août 1792, Marie-Antoinette a entretenu une correspondance enflammée avec un jeune officier suédois. Ces échanges mettaient en oeuvre **un code complexe**, dit «poly-alphabétique». Deux éléments sont nécessaires pour le décryptage des missives : une table de déchiffrement et un **mot-clé**. C'est le mot-clé qui permet l'utilisation de la table de déchiffrement et celui-ci change à chaque nouveau courrier.

Pour rester connu des deux seuls protagonistes et empêcher toute personne interceptant les lettres de les décrypter, **le nouveau mot-clé était désigné via un autre canal que la lettre**. Codes cousus dans des doublures de chapeaux, caches dans des secrétaires, etc. : on ne sait toujours pas aujourd'hui comment ils s'y prenaient.

LE NFC, CANAL DE COMMUNICATION SÛR ?

Le NFC (Near Field Communication) est une technologie de communication sans-fil dont **l'atout principal,** dans ce cas précis, **est sa courte portée**, jusqu'à 10 cm. Cela en ferait le vecteur idéal pour communiquer l'équivalent du **mot-clé** dans le système de Marie-Antoinette détaillé ci-dessus, et donc **la clé de voûte du système de sécurité d'un réseau d'objets connectés**. La courte portée empêche en théorie une interception non-visible de données.

Nous verrons toutefois dans un prochain article comment la pratique bouleverse la théorie.