Sym_Lab3

Par Jean-Luc Blanc, Kylian Bourcoud & Paul Reeve

Questions

NFC credentials

Voici les credentials pour valider le 1er facteur d'authentification pour le login de la partie NFC:

- username: `hello`
- password: `world`

2.4.1

L'API Android ne propose aucun mécanisme de base pour sécuriser un NFC et
compliquer son clonage car NDEF n'est de base pas un format sécurisé.

2.4.2

Elle serait moins préférable qu'un NFC et celà pour plusieurs raisons:

1. L'autonomie. Une IBeacon fonctionne avec une batterie alors que le NFC fonctionne avec l'électricité que lui donne le téléphone. On a alors un risque que le IBEacon tombe à cours de batterie
2. Le Broadcast. Une IBeacon émet ses datas en broadcast ce qui fait
   que n'importe quel appareil peut récupérer ses datas. Un attaquant se trouvant simplement à proximité physique du IBeacon peut du coup récupérer l'UUID
   et mettre cet UUID sur une autre IBeacon (du spoofing en somme)
3. La Passivité. Une IBeacon émet ses données en boucle contrairement
   à une puce NFC qui exige une action de l'utilisateur. Pour un processus d'authentification il faut mieux utiliser des facteurs d'authentification qui requiert une utilisation active (où l'utilisateur doit faire une action)

QR Code

3.2

1. Il est possible de stocker un maximum d'environ 3 KB dans un QR Code (exactement 2953 bytes). Oui il est possible de travailler avec des QR Codes complexes, il faut cependant prêter attention au fait que le nombre de modules ne soit pas trop élevé afin de permettre à la caméra de bien les distinguer. Sans quoi on se retrouvera avec seulement des fragments du QR Code qui seront transcrits.
2. Les QR Codes dynamiques encodent un lien menant vers un certain contenu, il est donc possible de modifier le contenu sans pour autant modifier le lien.
   Avantages : Le contenu peut évoluer sans avoir à changer le QR Code. Un lien est plus court et donc plus facile à scanner qu'un contenu entier. Facilite la fonctionnalité de payements.
   Inconvénients : Une connexion à internet est nécessaire, on dépend donc d'un accès soit à un WI-FI soit au réseau, ce qui n'est pas toujours le cas dans le monde du mobile. On ne

décode plus le contenu mais on accède à ce dernier soit via une application tierce (site internet) soit en le téléchargeant.

iBeacon

4.2

Les IBeacon émettent plus loin, les rendants bien plus vulnérable à des attaques contrairement au NFC qui lui émets à des distances de l'ordre du centimètre.
Par exemple, lors d'un paiement en caisse, un attaquant pourrait lire les communications si elles ne sont pas chiffrés ou créer un autre réseau, attirer le client sur son réseau au lieu du réseau prévu à cet effet afin dévier les paiements sur un autre compte bancaire. La faible portée du NFC garanti un plus grande sécurité: le client est sûre de se connecter au bon terminal de communication et un attaquant devra se rapprocher énormément pour pouvoir lire les communication.
La facilitation d'utilisation, est un autre point qui les différencie, pour se connecter à un réseau ibeacon, un utilisateur doit savoir que le réseau existe et se connecter à celui-ci via bluetooth, alors que pour nfc il suffit juste de scanner un tag nfc (ou un QR code).
Par exemple, supposons qu'un magasin voudrait afficher leur catalogue, il sera plus aisé de scanner un tag nfc ou un qr code te donnant accès à une page web, que se connecter à un réseau IBeacon afin d'obtenir le même service.
Troisièmement les Ibeacons sont des appareils sur batterie, ils peuvent donc en être à court. Ce n'est pas le cas pour les tags nfc qui sont passif et ne nécéssitent pas de batterir.Un magasin qui voudrait installer un réseau de Ibeacon devra veiller à sa disponibilité alors qu'un tag nfc sera toujours disponible.