Systèmes mobiles

Laboratoire n°3 : Utilisation de données environnementales

Auteurs : Loic Frueh - Koubaa Walid - Muaremi Dejvid
Enseignant : Fabien Dutoit
Assistants : Christophe Greppin, Valentin Minder
Date : 27.11.2018

2.4 Questions Balises NFC

Nous utilisons des tags NFC4 contenant des messages au format **NDEF**, ce format est supporté par la magorité des appareils utilisant la technologie NFC et certaines opperations basique peuvent être effectuée dessus comme la lecture mais aussi l'écriture par conséquent, sans une sécuritée prévue a cet effet, il est très facile de cloner un tag NFC.

Notre implementation Nous avons 10 niveau de sécurité différens pour notre applications, comme proposé dans la données, celui-ci décroit toutes les 6 secondes. Ceci laisse à l'utilisateur 60 secondes pour se loger. À tout moment on peut repasser le NFC tag pour remettre le sécurity niveau maximumm, c'est a dire 10, et réinitialiser le compteur, à 60 secondes.

Nous avons défini 4 états de sécurité pour nos boutons :

- High security, demande au minimum un niveau d'accréditation à 7.
- Medium security, demande au minimum un niveau d'accréditation à 4.
- Low security, demande au minimum un niveau d'accréditation à 1.
- À 0, l'utulisateur n'a plus aucun droit sur les bouttons, il doit repasser le NFC tag.

A partir de l'API Android concernant les tags NFC4, pouvez-vous imaginer une autre approche pour rendre plus compliqué le clonage des tags NFC ?
Une possibilité de se protéger contre la copie d'un tag NFC serait l'utilisation de l'ID unique de celui-ci qui nous permettrait à l'aide d'un service qui les listes d'authentifier et de valider nos tags. Cependant, comme cet id est modifiable, cela ne constitue pas une sécurité parfaite et il faut imaginer d'autres solutions plus complexe.

Est-ce possible sur toutes les plateformes (Android et iOS) ?
Android : Depuis l'API 10 iOS : Depuis iOS 11

Existe-il des limitations ?
Sur android très peu étant donné que la technologie est utilisée depuis l'API 10 et qu'elle a eu le temps d'évolué au fil des versions. Cependant, sur Apple, c'est une technologie naissante et l'accès à celle-ci est très limité par Apple. Actuellement il est surtout possible de detecter un tag NFC et lire les données NDEF, il faut que les données soient bien encodée pour que celà fonctionne, mais l'écriture n'est pas possible. Tout ceci se fait via le framework **Core NFC**

Voyez-vous d'autres possibilités ?
L'idéal serait d'utiliser l'un des cannal sécurisé de la balise NFC. Ceci permet de se proteger contre la plupart

des attaques possible comme par exemple une lecture non autorisée et par conséquent empécher la copie. Pour plus d'informations sur le sujet, voir le site suivant : **NFC secure Channel**

3.2 Questions Codes-barres

Un code-barres, ou code à barres, est la représentation d'une donnée numérique ou alphanumérique sous forme d'un symbole constitué de barres et d'espaces dont l'épaisseur varie en fonction de la symbologie utilisée et des données ainsi codées. Il existe des milliers de codes-barres différents ; ceux-ci sont destinés à une lecture automatisée par un capteur électronique, le lecteur de code-barres. Pour l'impression des codes-barres, les technologies les plus utilisées sont l'impression laser et le transfert thermique.

Grâce aux ressources en libre accès suivantes on peut implementer facilement une activité pouvant lire des codes barres ou des codes QR:

- https://github.com/journeyapps/zxing-android-embedded
- https://github.com/zxing/zxing/wiki/Scanning-Via-Intent

Comparer la technologie à codes-barres et la technologie NFC, du point de vue d'une utilisation dans des applications pour smartphones, dans une optique :

- Professionnelle (Authentification, droits d’accès, stockage d’une clé)

D'un point de vue professionnelle, la technologie des codes barres est relativement limitée pour tout l'aspect sécuritaire. Aucun protocole n'est present afin de garantir l'intergrité des données lues si ce n'est un code correcteur en cas d'erreur (codes de reed-solomon). Les quantitées de données sotckés sur un code barre suffit en general a identifier un element (objet en magasin, livre, appareil..) mais pas assez pour contenir des métadonnées de drotis d'accès,de clées publiques/pirivées).

Le NFC en revanche presente une meilleure utilisation pour les application sur smartphone. Certaines puces NFC permettent l'echange d'informations chiffrées, les rendant donc propisces dans l'optique d'une authentification. De plus la technologie NFC est en géneral plus ergonomique,chose crucial pour une application ou les demande d'authentification sont frequents et ou la rapidité est un facteur primoridial.

- Grand public (Billetterie, contrôle d’accès, e-paiement)

Dans une opitque d'utilisation pour des Billeteries ou un controle d'accès destinés au grand public, les codes barres sont préferables. En effet, le reel soucis est que cette technologie n'est pas disponible sur tout les appareil (les iPhones typiquement qui disposent plutot de la solution Apple avec les iBeacon), rendant donc l'utilisation du NFC mal appropiré car limitées. Il est donc plus interessant d'utiliser les codes barres a une ou deux dimensions (barres ou QR) pour ce type d'utilisation.

- Ludique (Preuves d'achat, publicité, etc.)

Concernant une utilisation plutot ludique, les codes barres sont assez facile à mettre en place, et sur une affiche publicataire par exemple, le code barre sera bien plus visble (pas le cas pour la puce NFC), et un utilisateur saura directement de quoi il s'agit et comment l'utiliser (ou du moins surement plus qu'avec une puce NFC).

Une preuve d'achat est censé etre reuilitsatible par un maximum de client possible, et un meme produit est censé disposer d'un meme code barre. Encore une fois, tout les appareil ne disposent pas de la technologie NFC, rendant sont utilisation non globale. Les codes barres demeurent encore une fois plus interessant ici.

- Financier (Coûts pour le déploiement de la technologie, possibilités de recyclage, etc.)**

L'ajout d'un code barre sur un support pjysique est assez bon marché. La définition et l'impression des codes barres est relativement rapide et aisée, et cela à un cout réduit. A l'inverse la technologie NFC peut etre couteuse (couts de fabrication des puces toujours elevées) sachant qu'en plus de la puce NFC à fournir, il faut aussi l'intégrer au produit (contrairement a code barre et déposer/coller directment).

En ce qui concerne le recyclage, bien évidement les NFC sont reconfigurables/reprogrammables, les rendant donc propisce à de multiples utilisations diverses contrairement aux code barres, à usage unique. Néanmoins l'empreinte carbone de l'une ou l'autre technologie est relative à l'utilsation désirée, on peux malgré tout géneraliser et dire que le NFC offre une meilleure possibilité de recyclage/reutilisation.

4.2 Questions Balises iBeacon

Les iBeacons sont très souvent présentés comme une alternative à NFC. Pouvez-vous commenter cette affirmation en vous basant sur 2-3 exemples de cas d'utilisations (use-cases) concrets (par exemple e-paiement, second facteur d'identification, accéder aux horaires à un arrêt de bus, etc.).

Les e-paiements

Concretement les iBeacons ne sont en fait que des trames bluetooth di□ffusées en broadcast de facon régulière. La communication ne se fait que dans un sens et donc toute authenti□cation, établissement de connexion, ou bien dialogue entre le mobile du client et la balise beacon est tout simplement impossible. En pratique il est assez difficile de concevoir un moyen de payement avec des iBeacons.

Une alternative potentielle serait d'envoyer au client un lien vers une application propre à l'entreprise qui elle se chargera de gerer le paiement.

A l'inverse la technologie NFC permet d'établir une connexion entre un mobile et un tag NFC, connexion suffi□samment sécurisée et authenti□ée, pour effectuer un paiement sans contact.

Donc pour des e-paiement, les iBeacons ne représentent pas une alternative viable au NFC. Leur simple principe de fonctionnement en est la cause, une amélioration et/ou un changement de leur fonctionnement/implémentation semble par ailleurs peu probable.

Le contrôle d'accès

De nos jours, la plupart des PME disposent d'un système pour contrôler l'accès à leurs locaux. Dans ce cas la comparaison entre NFC et iBeacon revient à peu près au même que celle des e-paiement.

- Avec les beacons, une authentification est impossible (voir plus haut). La seule possibilité est donc que l'utilisateur reçoive un iBeacon à l'approche d'une porte. Cet iBeacon devrait contenir un lien (genreré) vers une application permettant à l'utilisateur d'acceder à la porte donnée.
- Avec le NFC en revanche, une authentification directe entre la carte d'accès et la porte est possible. Pas besoin donc de manipulation supplémentaire ou autre. En conclusion, encore une fois les beacons ne représentent pas une alternative viable au NFC.

Les horaires de bus

Une idée serait placer des balises émettant des iBeacons aux arrêts de bus ou devant des oeuvres au musée ou bien devant chaque animal dans un zoo. Ceux-ci permettraient à un utilisateur ou à un visiteur de découvrir un lien sur son téléphone en s'approchant du lieu concerné.

- Dans le cas d'un arrêt de bus, on peutimaginer que l'usager reçoit un lien vers le site internet où se trouvent les horaires pour cet arrêt.
- Dans le cas d'un musée, le lien dirigerait directement la personne vers une page détaillant l'oeuvre à proximité.
- Dans le cas du zoo, à chaque fois qu'un utilisateur s'approche d'une zone contenant un animal, un lien dirrigerait vers une page contenant les informations concernant cet animal (sous forme d'une page wikipédia ou bien paragraphe détaillé d' informations utiles concernant l'animal à proximité).

Dans ces différents cas, les iBeacon s'averent être une alternative très intéressante car ils permettent une meilleure diffusion de l'information sans que l'utilisateur ait besoin d'installer une application spéci□que sur son téléphone.

5.2 Questions Capteurs

On se rend compte que, lorsque l'on essaie la boussole, les animations de mouvement de la flèche ne sont pas fluides. Ce tremblement peut s'expliquer par différent facteurs dont les suivants:

- Premièrement, le capteur de mouvement, soit l'accéléromètre est toujours en train de detecter le mouvement de la planète ce qui va le souvent modifier sa matrice de coordonées même lorsque ceci n'est pas nécessaire et perturbé la vraie détéction de mouvements.
- Ensuite, le magnétomètre qui permet de se positionnner par rapport au pôle nord magnétique, lui est encore plus sensible é l'environnement. Les masses métallique, aimant, ou tout autre élément dégageant un champ magnétique peut facilement le faire changer de trajectoire.
- Enfin, la précision des capteurs d'un téléphone est très mauvaise, selon la gamme du téléphone elle peut être relativement précise ou pratiquement inutilisable. Le temps de raffraichissement de l'écran par rapport au temps de raffraichissement des capteurs va également provoque un tremblement si celui-ci n'est pas un minimum synchronisé.