# Systèmes mobiles – Laboratoire no. 3

Lara Chauffoureaux, Tano Iannetta, Wojciech Myszkorowski

22 décembre 2017

Tout le code source de l'application est joint à ce rapport. Celui-ci est également disponible sur GitHub via le lien suivant :

https://github.com/galahad1/SYM-labo3

# Question NFC

Nous allons calculer les probabilités qui nous sont demandées.

1. Dans le cas d'un vol du mot de passe et de la balise NFC, la probabilité est de $0.01 * 0.04 * 0.1 * 0.001 = 0.000004\%$ de chance que cela se produise.
2. Dans le cas où il le vol concerne soit la balise NFC soit le mot de passe, cela a $(0.01 * 0.04 * 0.1) + (0.01 * 0.001 * 0.1) = 0.0041\%$ de chance de se produire.
3. Dans le cas d'un vol de seulement la balise NFC, la probabilité est de $0.01 * 0.001 * 0.1 = 0.0001\%$ chance de se produire.

Pour calculer les cas où le vol n'a pas lieu. Il faut tout simplement prendre la probabilité inverse $1 - P_1$ par exemple.

Maintenant si on applique les cas précédent à 100 personnes nous avons :

4. Dans le cas où il faut le MDP et le NFC $=> 1 - ((1 - P_1)^{100}) = 0.0039\%$
5. Dans le cas où il faut soit le MDP soit le NFC $=> 1 - ((1 - P_2)^{100}) = 0.4090\%$
6. Dans le cas où il faut juste la balise NFC $=> 1 - ((1 - P_3)^{100}) = 0.0099\%$

On peut voir que l'utilisation de la balise NFC augmente la sécurité. Le risque est très faible dans tous les cas et peut être considéré comme quasiment nul. En effet, cette probabilité calculée précédemment s'applique à chaque collaborateur et peut être considérée comme étant minime. Le fait d'avoir deux facteurs d'authentification est toujours mieux qu'un, cela réduit la probabilité de vol de données.

En revanche, la probabilité de perdre ses clés pour certaines personnes inattentives peut s'avérer très élevée et du coup peut bloquer l'utilisation du téléphone et donc empêcher la personne de pouvoir faire son travail. La possibilité de choisir la façon de s'authentifier (mot de passe **ou** NFC) peut sembler plus "user-friendly" pour l'utilisateur. Mais le risque est supérieur et n'apporte donc rien au niveau sécurité. A notre avis, cette possibilité ne devrait pas être disponible pour les utilisateurs.

Le contrôle par le serveur peut être une bonne idée, mais doit être bien géré car si on intercepte le trafic et qu'on récupère le hash alors la situation est critique car une personne malicieuse n'a qu'à envoyer un hash récupérer et elle pourra s'authentifier. Au final cette option n'ajoute pas vraiment une sécurité supplémentaire pour l'entreprise. Un bonne optique serait de pouvoir bloquer les comptes lorsqu'un employé dit avoir perdu un des éléments critiques (mot de passe, NFC ou téléphone). Un sms ou un email envoyer par l'utilisateur permettrai de notifier l'entreprise de l'incident.

L'authentification à double facteur est clairement recommandée pour une entreprise comme UBIQOMP SA. La mise en place de stockage à distance pour les éléments tels que mot de

passe est aussi recommandée. Mais il faut savoir que cette opération peut s'avérer couteuse en ressources et argent. Une perte de connexion deviendrai aussi un inconvénient majeur. Une autre réalité est le fait d'avoir à savoir ou se trouve la balise NFC. La perte d'un élément comme le NFC peut survenir plus souvent en réalité qu'en théorie pour une bonne partie des employés.

# Question codes barre

### Utilisation professionnelle (Authentification, droits d'accès, clés de chiffrage) :

Dans ce cadre, la technologie NFC est à préférer.

Certaines puces NFC permettent l'échange d'informations chiffrées, rendant l'utilisation du NFC préférable dans l'optique d'une authentification. La technologie NFC est aussi plus ergonomique, ce qui est crucial dans un environnement où l'authentification est fréquente et où la rapidité est un facteur important.

### Utilisation grand public (Billetterie, contrôle d'accès, e-paiement) :

Pour le grand public il est préférable d'utiliser les codes barres. En effet, pour le NFC, certains mobiles (iPhone) n'utilisent pas cette technologie. C'est donc une grande partie des utilisateurs potentiels qui ne pourront pas profiter de l'application. Il est donc plus avisé d'utiliser les codes barres dont la technologie est plus répandue parmi les mobiles.

### Utilisation ludique (Preuves d'achat, publicité, etc.) :

Il est plus facile de déployer des codes barres, par exemple sur des affiches pour de la publicité que des puces NFC. Le code barre sera aussi plus voyant, et l'utilisateur saura directement à quoi cela correspond.

Comme dit plus haut, tous les utilisateur ne disposent pas du NFC. Une preuve d'achat se doit être utilisable par le plus d'utilisateurs possible. Et donc, il est important d'utiliser les codes barres plutôt que le NFC.

### Utilisation de un cadre financier (Coûts pour le déploiement de la technologie, possibilités de recyclage, etc.) :

L'ajout d'un code barres à des supports est bon marché. Il nécessite peut-être un travail de conception supplémentaire mais l'impression a un coût minime. A contrario, intégrer la technologie NFC peut être coûteuse étant donné les coûts de production et les efforts nécessaires pour intégrer une puce NFC.

D'un point de vue recyclage, le NFC est re-programmable pour une autre utilisation. Le code barre ne l'est pas !

# Question beacon

Pour répondre à cette question, nous avons choisi d'analyser 3 cas d'utilisations différents.

### Les e-paiements

Dans le cas du e-paiement, chacune des deux solutions doit être analysée avec soin :

- Les beacons ne sont en fait que des trames bluetooth diffusées en broadcast de manière régulière. La communication ne se fait que dans un sens et donc toute authentification, établissement de connexion, ou dialogue entre le mobile du client et la balise beacon est tout simplement impossible.
  Il est donc impossible de vraiment payer avec des beacons. Une alternative imaginable est d'envoyer au client un lien vers une application propre à l'entreprise qui elle permettra le paiement.
- A contrario, le NFC permet d'établir une connexion entre un mobile et un tag NFC. Cette connexion, une fois suffisamment sécurisée et authentifiée, peut permettre la réalisation d'un paiement sans contact.
  Aujourd'hui en Suisse, les NFC sont utilisés dans la plupart des cartes de banque afin de permettre le paiement sans contact.

Donc dans le cas des e-paiement, les beacons ne représentent pas une alternative viable au NFC. Leur principe de fonctionnement en est la cause, une amélioration et/ou un changement de ce paradigme semblent donc très peu probables.

### Contrôle d'accès

Aujourd'hui, la plupart des grandes entreprises disposent d'un système pour contrôler l'accès à leurs bâtiments. Dans ce cas la comparaison entre NFC et beacons revient à peu près au même que dans le cas des e-paiement traité précédemment.

- Avec les beacons, une authentification est impossible. La seule possibilité est donc que l'utilisateur reçoive un beacon à l'approche d'une porte. Ce beacon devrait contenir un lien vers une application permettant à l'utilisateur de s'authentifier pour la porte donnée.
- Avec le NFC par contre, une authentification directe entre la carte et la borne est possible. Pas besoin donc de manipulation supplémentaire ou autre.

Comme précédemment, dans ce scénario d'utilisation les beacons ne représentent pas une alternative valable au NFC.

### Horaires de bus

Voilà un cas d'utilisation permettant d'illustrer un cas où les beacons proposent une réelle alternative aux méthodes existante :

Aux arrêts de bus ou devant des oeuvres au musée, il serait possible de placer des balises émettant des beacons. Ceux-ci permettraient à un utilisateur ou à un visiteur de découvrir un lien sur son téléphone en approchant du lieu concerné. Dans le cas d'un arrêt de bus, on peut imaginer que l'usager reçoit un lien vers le site internet où se trouvent les horaires applicable pour cet arrêt. Pareil au musée, le lien dirigerait directement l'intéressé vers une page détaillant l'oeuvre concernée.

Dans ce cas, les beacons sont une alternative très intéressante car ils permettent une diffusion large de l'information sans que l'utilisateur ait besoin d'installer une application spécifique sur son téléphone.

Pour résumé, les beacons sont très à la mode actuellement mais leurs cas d'utilisation demandent des conditions très spécifiques. Contrairement au NFC ils ne permettent aucun dialogue et donc aucune authentification entre les deux acteurs. De plus, les balises beacons coutent sensiblement plus cher que les tags NFC (environ 1 CHF par NFC tag contre 20 CHF pour une bonne balise beacon [1]). Pour conclure, nous dirions donc qu'à part dans certains cas très spécifiques l'utilisation des beacons n'est pas une alternative aux autres technologies existantes.

## Question capteurs

Notre flèche tremble car les capteurs sont "trop" sensibles. En effet, le bruit n'est pas ignoré, il en résulte donc un faible tremblement dû aux perturbations environnementales.

Pour remédier à ce problème on pourrait, avant d'afficher la flèche, ne pas considérer les variations trop faibles. Il serait possible de faire un régulateur afin d'assouplir le résultat et donc d'ignorer le bruit.

1. Ces prix dépendent bien sûr de la qualité voulue et de la quantité commandée