SYM laboratoire 3 janvier 2017

Groupe

- Amine Tayaa
- Simon Baehler
- Thibault Schowing

Fonctionnement de l'application

Le but de cette application n'était pas d'implémenter un système réellement sécurisé mais d'appliquer certaines technologies à Android.

Informations de login

A des fins de test et d'utilisation facilitée, le nom d'utilisateur et le mot de passe sont **"a"** tout simplement. Cela évite de perdre du temps pour tester l'application. Dans un cas réel une politique de mot de passe devrait être mise en place.

Fonctionnement général

Avec accord du professeur, les détails comme la sauvegarde lors des changements de contexte n'est pas implémentée. Il est donc nécessaire de ne pas incliner le téléphone durant l'utilisation de l'application.

Questions

Question 1

Sachant que les collaborateurs de l'entreprise UBIQOMP SA se déplacent en véhiculant des informations extrêmement précieuses dans leurs dispositifs informatiques mobiles (munis de dispositifs de lecture NFC), et qu'ils sont amenés à se rendre dans des zones à risque, un expert a fait les estimations suivantes :

- La probabilité de vol d'un mobile par une personne malintentionnée et capable d'utiliser les données à des fins préjudiciables pour la société est de 1%
- La probabilité que le mot de passe puisse être découvert, soit par analyse des traces de doigts sur l'écran, soit par observation en cours d'utilisation est de 5%
- La probabilité de vol du porte-clés est de 0.1%
- Environ 10% des criminels susceptibles d'accéder aux données du mobile sait que le porte-clés donne accès au mobile

Quelle est la probabilité moyenne globale que des données soient perdues, dans le cas où il faut la balise ET le mot de passe, ainsi que dans le cas où il faut la balise OU le mot de passe, ou encore le cas où seule la balise est nécessaire ? En d'autres termes, si l'on envoie cent collaborateurs dans la géographie, quel est le risque encouru de vol de données sensibles ? Mettre vos conclusions en rapport avec l'inconfort subjectif de chaque solution.

Peut-on améliorer la situation en introduisant un contrôle des informations d'authentification par un serveur éloigné (transmission d'un "hash" genre MD5 du mot de passe et de la balise NFC) ? Si oui, à quelles conditions ? Quels inconvénients ? Proposer une stratégie permettant à la société UBIQOMP

SA d'améliorer grandement son bilan sécuritaire, en détailler les inconvénients pour les utilisateurs et pour la société.

Réponse :

Par vol de données sensibles ici on entendra donc "vol de données avec préjudice pour la société". Pour résumer nous avons les valeurs suivantes :

- Vol à des fins préjudiciables : 0.01
- Mot de passe découvert : 0.05
- Vol du porte-clés : 0.001
- Sait que le porte-clés donne l'accès : 0.1

La probabilité que le vol de données ait lieu alors que la balise ET le mot de passe sont nécessaires est de **0.01 x 0.001 x 0.1 x 0.05** soit 0.00000005 c'est-à-dire **0.000005 %.**

La probabilité que le vol de données ait lieu alors que la balise seule est nécessaire est de **0.01 x 0.001 x 0.1** soit 0.000001 c'est-à-dire **0.0001 %**.

La probabilité que le vol de données ait lieu alors que la balise OU le mot de passe sont nécessaires est de **1 - (1 - 0.01 x 0.001 x 0.1) x (1 - 0.01 x 0.05)** soit 0.0005009995 c'est-à-dire **0.05009995%.**

On s'aperçoit qu'avec la balise ET le mot de passe, la probabilité de perdre les données est plus basse. En revanche, le confort d'utilisation avec une balise ET un mot de passe est fortement réduit. Les utilisateurs seront vite lassés de devoir s'authentifier plusieurs fois afin d'avoir accès à leurs données. Ce genre d'authentification n'est pas user-friendly.

Pour améliorer la sécurité il faut prendre en compte plusieurs points. Si les données sont en locale sur le terminal, il faut absolument les chiffrer. La manière la plus ergonomique serait d'utiliser un hash entre nom d'utilisateur et mot de passe (déjà haché) qui pourrait être utilisé comme clé de chiffrement/déchiffrement des données locales. Lorsque l'on parle de hash, on parle bien sûr d'un algorithme sûr comme Sha256 ou Sha512 et non MD5. Mais même dans ce cas, si le terminal est volé les données sont en possession du voleur.

L'utilisation d'un serveur distant pour vérifier les données de connexion, par exemple en vérifiant ID et mot de passe (hash) ainsi que position géographique, peut apporter une étape de sécurité en plus. Il faudra ensuite que ce serveur transmette une autre partie de la clé de déchiffrement au terminal afin qu'il puisse déchiffrer les données. On pourrait aussi utiliser un système d'authentification comme Google qui envoie un code au terminal comme complément d'authentification.

Dans une certaine mesure, stocker les données sur un serveur distant et les transmettre quand nécessaire peut être une solution sûre mais la disponibilité du réseau devient alors cruciale tout comme pour l'étape de vérification. Il est donc à l'entreprise, selon son contexte, de choisir entre un mode locale ou distant de transmission / vérification des données.

La meilleure option de sécurité est d'utiliser premièrement le tag NFC ET le mot de passe. Les différents chiffres ci-dessus ne laissent pas de doute. L'ergonomie diminue avec l'accumulation de moyens d'identification mais c'est un compromis nécessaire.

Question 2

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, clés de chiffrage)
- Ludique (preuves d'achat, identité électronique pour gaming, etc...)
- Grand public (ticketing, access control, e-paiement)
- Financier (coûts impliqués par le déploiement de la technologie, possibilités de recyclage, etc...)

Réponse :

Cette question est relativement délicate due au fait que la technologie évolue, il faut savoir que le code barre existe depuis 1952. Il ne faut donc pas se le cacher, même si cette technologie est toujours très utilisée dans les supermarchés, elle devrait être enclin à disparaitre comme la téléphonie traditionnelle l'est actuellement par la téléphonie mobile. Mais le problème réside dans le fait que le code barre est ancré dans notre vie de tous les jours. NFC devra passer outre plusieurs barrières qui sont les suivantes :

- Prix du tag NFC
- Les produits devront être redesigné pour NFC

Professionnelle

Déjà mis en place et plus dure à fabriquer soi-même, les tag NFC se prêtent mieux à un usage professionnel. Le NFC a aussi un niveau de sécurité supérieur au QR code suivant son utilisation.

Ludique

Le lecteur par QR code devrait être le meilleur, car il est facile à mettre en place du moment que nous possédons une imprimante. Cette technologie est visuelle et relativement intuitive d'utilisation. Même si son utilisation est à la baisse, il est quand même connu des personne ayant un smartphone.

Exemple : pour Festigeek on pourrait mettre un QR code sur nos affiches qui redirige vers le site avec les informations en rapport avec l'affiche, ce qui serait difficile à mettre en œuvre avec du NFC, et aussi moins intuitif, on n'est pas forcément au courant qu'un tag NFC se trouve derrière l'affiche. Pour le cas d'identité électronique pour gaming, ou même le cas d'identité numérique, on peut prendre le cas de Snapchat ou chaque utilisateur à un code bar qui lui est propre et peut le partager facilement sur une vidéo Youtube ou sur son Facebook.

Grand public

Dans le cadre d'un e-paiement l'utilisation d'un QR code pourrait être approprié. Comme pour les utilisations ludiques la facilité d'accès et d'utilisation du QR code est un plus. Pour le cas du ticketing, un QR code est optimal, car nous pouvons imprimer notre ticket chez nous et le faire scanner à l'entrée du concert. Cela vaut aussi pour les boarding cards.

Financier

Le QR code ne peut pas être recyclé mais le support sur lequel il se trouve peut l'être. L'information du QR code est donc fixe. On a donc une dualité entre le faible cout de production (on peut en faire un avec un crayon papier sur le mur de la cuisine si on veut) mais l'impossibilité de les recycler, alors qu'un Tag NFC peut être réécrit afin d'en changer son contenu mais sa fabrication nécessite des composants électroniques. Afin de réduire les couts, on peut par exemple imaginer que la position du Tags sur des affiche est normalisée, et alors on pourrait mettre le Tag non pas sur chaque affiche mais dans le support de celles-ci et le poseur d'affiche aurait simplement à reprogrammer les Tags lors qu'il change les affiches. Le cout financier est alors toujours supérieur au QR code (il faut investir dans un tag alors que l'affiche est de toute manière imprimée) mais une réutilisation est quand-même possible.

Question 3

Les Beacons sont basés sur l'utilisation de Bluetooth Low Energy (BLE), tandis que NFC utilise des ondes radios courtes ce qui fait une courte distance (10 cm maximum) alors que les iBeacons peuvent aller jusqu'à 50 m. NFC supporte le chiffrement ce qui augmente sa sécurité en plus de la petite distance entre les périphériques. Les iBeacons sont pratiques pour la consultation des horaires d'un arrêt de bus, par exemple, car il fonctionne de façon ONE TO MANY ce qui permet de plusieurs personnes de consulter les horaires en même temps, par contre pour le NFC qui fonction de façon ONE TO ONE, ce qui ne permet qu'à une seule personne à la fois de consulter les horaires du bus. Par exemple, pour les paiements sans contact, on privilégiera le NFC car il est plus sécurisé et on sait que la transaction est faite entre deux et seulement deux périphériques physiquement proches.

Une excellente comparaison des deux technologies peut être consultée à l'URL suivant :
http://www.getelastic.com/mobile-commerce-ibeacon-vs-nfc-infographics/