Laboratoire n°3 : Utilisation de données environnementales

Question 1 : 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 (on négligera dans le calcul la probabilité de l'intersection des deux ensembles), ou encore le cas où seule la balise est nécessaire ? En d'autres termes, si l'on envoie cent collaborateurs en déplacement, quel est le risque encouru de vol de données sensibles ? Mettre vos conclusions en rapport avec l'inconfort subjectif de chaque solution.

La probabilité moyenne globale que des données soient perdues, dans le cas où il faut la balise ET le mot de passe est de 0.01 * 0.04 * 0.001 * 0.1 = 0.00000004
La probabilité moyenne globale que des données soient perdues, dans le cas où il faut la balise OU le mot de passe est de 1 – (1 – (0.01 * 0.001 * 0.1)) * (1 – (0.04 * 0.01)) = 0.0004009996
La probabilité moyenne globale que des données soient perdues, dans le cas où seule la balise est nécessaire est de 0.01 * 0.01 * 0.1 = 0.000001

On observe donc que la probabilité la plus faible est la perte de données dans le cas où il faut utiliser la balise ET le mot de passe. Ce qui est du que l'authentification à deux facteurs offre plus de sécurité.

Question 2 : Peut-on améliorer la situation en introduisant un contrôle des informations d'authentification par un serveur éloigné (transmission d'un hash SHA256 du mot de passe et de la balise NFC) ? Si oui, à quelles conditions ? Quels inconvénients ?

Réponse : Non car si les credentials ont été volés, l'attaquant arriverait tout de même à se connecter avec ces credentials.

Question3 : 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.

La société UBIQOMP peut améliorer en utilisant un serveur d'authentification comme mentionné ci-dessous mais utilisant un chiffrement sûr pour la transmission des informations car un attaquant qui écoute la communication pourrait les réutiliser pour s'authentifier si ce n'est pas le cas. En plus on pourrait rajouter une deuxième couche d'authentification en rejouant un code renvoyé par le serveur également chiffré par SMS à l'utilisateur qui se connecte ou par mail. Les inconvénients pour les utilisateurs sont les utilisateurs c'est qu'il y aura encore une deuxième couche d'authentification.

Question 4 : 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)**

  NFC est à favoriser pour une utilisation professionnel étant donnée qu'il permet une authentification à 2 facteurs. De plus, la clé de chiffrement n'est pas visible d'un simple coup d'oeil. Le tag NFC peut contenir des droits d'accès et on peut ajouter des niveaux de sécurité dans le temps (inactivité pendant un lapse de temps, rescan du tag nécessaire pour accéder à la ressource).

La technologie de code barre est voué à être remplacer par NFC. Une authentification par 2 facteurs est également possible bien que moins pratique. Par leur facilité de création et destructions, les codes barres peuvent être utilisés comme clé de chiffrement et/ou comme droit d'accès à usage unique.

- **Grand public (Billetterie, contrôle d'accès, e-paiement)**
  La technologie à code barre est la plus pratique car elle permet de scanner facilement un billet ou un e-ticket pour voir s'il est encore valide. Ainsi, on pourrait acheter un e-ticket facilement sur internet et le sauvegarder dans le téléphone ce qui est instantané par contre avec le NFC il faudrait recevoir dans un deuxième temps un tag contenant l'information du billet ce qui n'est pas très pratique.
- **Ludique (Preuves d'achat, publicité, etc.)**
  La technologie à code barre est la plus pratique. Par exemple dans le cas d'une publicité sur internet on peut consulter les informations directement avec le téléphone en lisant le code barre.
- **Financier (Coûts pour le déploiement de la technologie, possibilités de recyclage, etc.)**
  Une fois un QR code généré l'information contenu est figé, impossible de la remplacer à moins de générer un autre QR code entier. Le support sur lequel il se trouve peut-être recyclé (sticker, feuilles, etc). Le coût de déploiement est relativement bas, par contre si les données changent et entrainent un nouveau QR code, alors les coûts augmentent pour maintenir la solution à jour.
  Un tag NFC a un coût contrairement au QR code. Cependant une fois en possession du tag, on peut facilement le réécrire et donc le recycler pour une autre utilisation. Le coût initial de déploiement est donc plus élevé que le QR code.

Question 5 : 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.).

L'avantage majeure des iBeacons est sa portée d'émission. En effet elle atteint une grande distance par rapport au NFC. Ainsi elle est plus adaptée pour accéder aux horaires. Le NFC peut ne pas etre disponible sur certains téléphone alors que les iBeacons utilise le bluetooth qui est disponible sur la majorité des téléphones.
En outre les informations transmises pas les iBeacons peuvent être lus par plusieurs personnes en même temps alors que le NFC limite son utilisation pour une seule personne. Ainsi dans le cas d'une consultation d'horaire à un arrêt de bus par une, les iBeacons conviendront mieux.
Aussi dans le cas d'un second facteur d'identification, les iBeacons peuvent très bien être utilisé à la place du NFC.

Question 6 : Une fois la manipulation effectuée, vous constaterez que les animations de la flèche ne sont pas fluides, il va y avoir un tremblement plus ou moins important même si le téléphone ne bouge pas. Veuillez expliquer quelle est la cause la plus probable de ce tremblement et donner une manière (sans forcément l'implémenter) d'y remédier.

En utilisant le debugger, on découvre un nombre important d'events générés par les capteurs. L'image est générée plusieurs fois par secondes. De plus les valeurs du capteur ne sont pas homogènes, ce qui peut entrainer des sauts plus ou moins important. Une solution serait d'analyser

les données qui sont reçues des capteurs et d'effectuer une moyenne. De cette façon, on évite des valeurs atypiques qui entraine des sauts d'image.