SYM Labo 3 : Rapport

Date : 18.12.2021
Auteurs : Pellissier David, Ruckstuhl Michael et Sauge Ryan

NFC

Question 2.4.1

Dans la manipulation ci-dessus, les tags NFC utilisés contiennent 4 valeurs textuelles codées en UTF-8 dans un format de message NDEF. Une personne malveillante ayant accès au porte- clés peut aisément copier les valeurs stockées dans celui-ci et les répliquer sur une autre puce NFC.

A partir de l'API Android concernant les tags NFC, pouvez-vous imaginer une autre approche pour rendre plus compliqué le clonage des tags NFC ? Existe-il des limitations ? Voyez-vous d'autres possibilités ?

Réponse

1. Authentifier les données de la puce en utilisant son UID, puis vérifier au moment du scan si la signature correspond.
    a. Méthode pas très fiable car l'UID n'est pas toujours en lecture seule : selon le modèle il peut être possible de le modifier et donc contourner la protection
    b. De plus, l'UID peut être prévisible donc il est possible de forger des messages.
    c. Plus d'infos : https://learn.gototags.com/nfc/chip/features/uid
2. Utilisation d'un système de tokenisation
    - le client valide son identité lors de l'ajout d'une carte dans Google Pay (processus d'identification) ;
    - l'appareil mobile du client stocke en toute sécurité ses jetons ;
    - l'application Google Pay transmette les jetons au terminal de paiement lors des transactions en magasin ;
    - Limitation: ce système n'est pas implémentable directement via l'API standard NFC. Il faut une puce spéciale permettant la tokenisation.

Sources :

https://support.google.com/pay/merchants/answer/6345242

https://support.apple.com/fr-fr/HT203027

Question 2.4.2

Est-ce qu'une solution basée sur la vérification de la présence d'un iBeacon sur l'utilisateur, par exemple sous la forme d'un porte-clés serait préférable ? Veuillez en discuter

Premièrement, cette solution n'empêche pas le clonage du contenu de la puce NFC, mais uniquement son utilisation à l'intérieur d'une application spécifique.

Ensuite, le choix de la technologie iBeacon est très mauvais il peut facilement être spoofé par un attaquant.

Donc non cette solution n'est pas préférable pour éviter le clonage de puce NFC.

Codes-barres

Question 3.2.1

Quelle est la quantité maximale de données pouvant être stockée sur un QR-code ? Veuillez expérimenter, avec le générateur conseillé[5] de codes-barres (QR), de générer différentes tailles de QR-codes. Pensez-vous qu'il est envisageable d'utiliser confortablement des QR- codes complexes (par exemple du contenant >500 caractères de texte, une vCard très complète ou encore un certificat Covid) ?

En théorie, le standard QR code indique que la version la plus grande "v40" de QR code peut contenir 177x177 modules, correspondant à entre 23648 à 10208 bits selon le niveau de correction d'erreur (ECC)

Extrait du site officiel: https://www.qrcode.com/en/about/version.html

The figures in the Numeral, Alphanumeric, Binary and Kanji columns indicate the maximum allowable number of respective characters, including those for the data bit number.

When using the Version 1 QR Code with correction level L, for example, the maximum allowable numbers are 152, 25, 17, 10 for the data bit number, numerals, binaries and Kanji respectively.

Version	Modules	ECC Level	Data bits (mixed)	Numeric	Alphanumeric	Binary	Kanji
40	177x177	L	23,648	7,089	4,296	2,953	1,817
		M	18,672	5,596	3,391	2,331	1,435
		Q	13,328	3,993	2,420	1,663	1,024
		H	10,208	3,057	1,852	1,273	784

Cependant, plus le code QR est détaillé, plus il faut une grande surface d'affichage pour afficher le code de manière précise et pour qu'il soit lisible par un capteur photo. La qualité de l'appareil photo peut aussi déterminer la précision de la lecture du code QR si celui-ci est petit.

Question 3.2.2

Il existe de très nombreux services sur Internet permettant de générer des QR-codes dynamiques. Veuillez expliquer ce que sont les QR-codes dynamiques. Quels sont les avantages et respectivement les inconvénients à utiliser ceux-ci en comparaison avec des QR-codes statiques. Vous adapterez votre réponse à une utilisation depuis une plateforme mobile.

Réponse

Les QR-codes dynamiques contiennent une URL redirigeant vers les données affichées sur une page Web.

Avantages :

- Le contenu peut être modifié à volonté
- Le QR code reste petit et donc très lisible, car il ne stocke qu'une URL
- Stockage de données potentiellement illimité (selon les capacités du serveur)
- Depuis le serveur, il est possible d'analyser le trafic venant du QR-code
- Peut être désactivé du côté du serveur

Inconvénients :

- Nécessite une connexion Internet pour accéder aux données
- Les données ont besoin d'être hébergée sur un serveur
- Sensible aux changements de nom de domaine ou d'URL
- Les scanneurs QR n'implémentent pas forcément la redirection automatique

iBeacon

Question 4.2

Les iBeacons sont très souvent présentés comme une alternative à NFC. Vous commenterez 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.).

Réponse

1. **Paiement**
   - Paiement : Utiliser les beacons pour effectuer des paiement PayPal (PayPal Beacon)
     - Sources :
       - https://guide.beaconcrm.org/en/articles/5720169-accepting-payments-through-paypal
       - https://electricnews.fr/paypal-beacon-revolutionne-le-paiement-en-magasin-avec-une-technologie-entierement-sans-contact/
   - Paiement TWINT beacon : https://www.twint.ch/fr/clients-commerciaux/nos-solutions/distributeur-avec-twint/
2. **Supermarché**

Supermarché : Target customers in in real-time

Motivate customers to make a purchase by creating customized push notification using behavioral data and purchase statisti

Source : https://beaconsmind.com

3. **Balise de détresse**

« La localisation dans les bâtiments et dans les zones de construction est pertinente dans les situations d'alarme. Une SOS-Beacon permet une localisation en temps réel dans les bâtiments. Grâce aux balises économiques, un positionnement fiable en intérieur est garanti avec l'application SOS-Mobile (Android et iOS) et le dispositif d'appel d'urgence personnel TRIO. Les balises sont disponibles en différentes versions : Discrètement petite, batterie longue durée, étanche, etc.»

Source : https://www.swissphone.com/fr-ch/produit/sos-beacon/