

Sensibilisation à la Sécurité en RFID

Gildas Avoine

Massachusetts Institute of Technology

Cambridge, MA 02139, USA

Introduction

- ▶ Faire de la sécurité apporte des **solutions**, pas des **problèmes**.
- ▶ Faire de la sécurité nécessite de connaître son **adversaire**.
- ▶ Faire de la sécurité engendre un **coût**.

Je veux :

- ▷ Que les interlocuteurs puissent communiquer.

Je ne veux pas :

- ▷ Que mon service tombe en panne.
- ▷ Qu'un adversaire puisse écouter les communications.
- ▷ Qu'un adversaire puisse modifier les communications.
- ▷ Qu'un adversaire puisse se faire passer pour quelqu'un d'autre.
- ▷ Qu'un adversaire puisse savoir qui j'appelle.

Analyse de la sécurité en RFID

Quelle sécurité pour quelle application ?

- ▷ Traçabilité dans les chaînes de production
- ▷ Bibliothèque
- ▷ Carte de fidélité
- ▷ Marquage du linge dans les blanchisseries
- ▷ Tatouage animal
- ▷ Passeport
- ▷ Forfait pour les remontées mécaniques
- ▷ Abonnement aux transports publics
- ▷ Badge d'accès
- ▷ Clef de démarrage de voitures

Je veux :

- ▷ Identifier les tags et éventuellement recevoir de l'information.

Je ne veux pas :

- ▷ Que mon service tombe en panne.
⇒ Dénis de service.
- ▷ Qu'un adversaire puisse obtenir de l'information sur les tags.
⇒ Fuite d'information.
- ▷ Qu'un adversaire puisse tracer les tags.
⇒ Traçabilité malveillante.
- ▷ Qu'un adversaire puisse se faire passer pour un tag légitime.
⇒ Authenticité.

Matériel pour faire une attaque



Dénis de service

Définition

Déni de service

L'attaque par déni de service vise à rendre une application informatique incapable de répondre aux requêtes des utilisateurs.

- ▶ Le but peut être de **pertuber** ou d'**anéantir** le service d'un concurrent: défacement de sites web, saturation du système.
- ▶ S'en prémunir passe par l'utilisation d'**outils classiques** (réplication de l'infrastructure, etc.).

- ▷ Destruction de tags, injection de tags, bruiteur.
- ▷ Attaques faciles à mettre en œuvre à moindre coût : magasins, chaînes de production.
- ▷ Se prémunir des dénis de service contre les technologies sans fil est très difficile.
- ▷ Il faut vivre avec et savoir comment réagir.

Fuite d'information

Définition

Fuite d'information

Des informations sur la société ou sur ses clients sont révélées involontairement.

- ▶ **Données relatives à la société** : espionnage industriel
Divulgarion des listes des clients/fournisseurs, offres, informations techniques (sociétés pharmaceutiques, alimentaires, technologiques) ⇒ concurrence déloyale, contrefaçon, etc.
- ▶ **Données relatives aux clients** : respect de la vie privée
Divulgarion d'adresses, salaires, préférences, photos, etc.

Espionnage industriel: Exemple du Concorde



- ▶ **Fléau croissant** : capacités de stockage accrues, base de données connectées à Internet, nouveaux moyens de communication (Mail, Skype).

La taille des disques durs a enflé, et la masse des informations stratégiques embarquées a suivi la même courbe. Bases de données répliquées, correspondance électronique, fichiers divers et variés, une véritable mine d'or pour un pirate. Il n'est pas rare qu'un portable de directeur contienne l'équivalent de 50 kilos de dossiers stratégiques." Samuel Barbaud, Responsable de la Sécurité des Systèmes d'Information de Richemont.

- ▶ Conséquences parfois **désastreuses**.
- ▶ Décideurs **non sensibilisés**.
- ▶ Des mesures simples peuvent **réduire les risques**.

- ▷ Toutes les données sont **informatisées**.
- ▷ La source n'est plus seulement le **système**, mais aussi les **tags**.
- ▷ Facilité de **recueillir** l'information.
- ▷ Une entreprise qui ne considère pas le problème de l'**espionnage industriel** est une entreprise peu ambitieuse.

Espionnage industriel: des tags bien bavards



- ▷ Information révélée par le **ystème**.
 - ▶ Problème existant. Utiliser les techniques usuellles.
- ▷ Information révélée par le **tag**.
 - ▶ Passeport électronique, carte de fidélité.
 - ▶ Éviter de stocker des informations sur le tag.
 - ▶ Apporter des mesures de sécurité supplémentaires.
- ▷ Jouer la **transparence** avec les utilisateurs.

Traçabilité malveillante

Définition

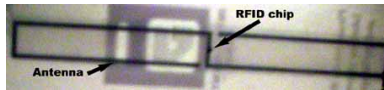
Non-traçabilité

Etant donné un ensemble de communications tags/lecteurs, un adversaire ne doit pas être capable de trouver des relations entre ces communications.

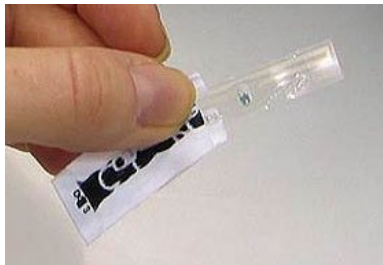
Exemple: Tracer des employés dans une entreprise, tracer des troupes militaires, etc.

Certains organisations de défense des libertés individuelles s'opposent à la RFID : **Caspian**, **Foebud**.

Tags bien cachés : Marks & Spencer



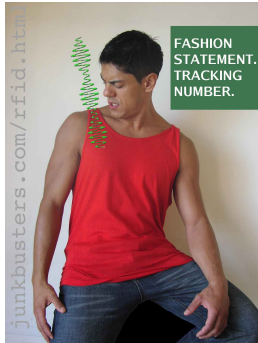
Tags bien cachés : Calvin Klein



Tags bien cachés : Champion



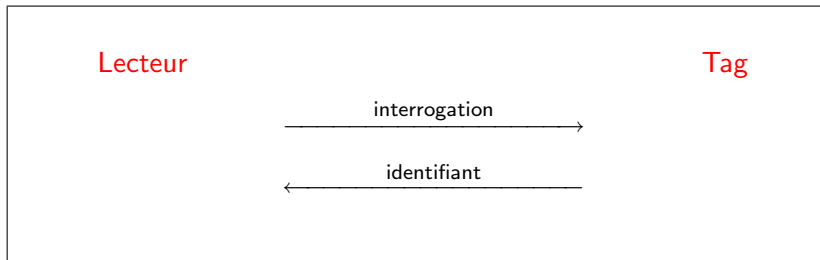
Campagne de boycott contre Benetton



Campagne de boycott



Protocole d'identification



- ▶ Les tags ne peuvent pas être **éteints**.
- ▶ Les tags répondent au lecteur **sans l'accord** de l'utilisateur.
- ▶ La tendance est à augmenter la **distance** de communication.
- ▶ Les tags sont parfois invisibles ou leur **présence ignorée**.

- ▷ Distance de communication adaptée
- ▷ Kill-command
- ▷ Cages de Faraday
- ▷ Blocker tags
- ▷ Réglémentations

Concevoir un protocole tel que seuls les personnes autorisées peuvent **identifier** les tags alors que les adversaires ne peuvent ni les **identifier**, ni les **tracer**.

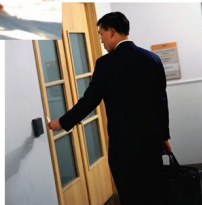
- ▷ Faibles **capacités** des tags.
- ▷ Possible pour **certaines** applications.
- ▷ Engendre un **coût supplémentaire**.
- ▷ Possible de **réduire les capacités** de l'adversaire.

- ▷ Ne pas tomber dans la **paranoïa**.
- ▷ Jouer la **transparence** avec les utilisateurs.
- ▷ Majorité des applications **bien acceptées** (ex. carte Navigo)

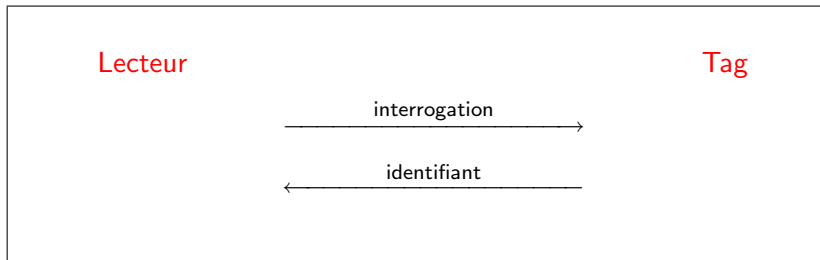
Authenticité

- ▷ Contrôle d'accès
- ▷ Lutte contre la contrefaçon

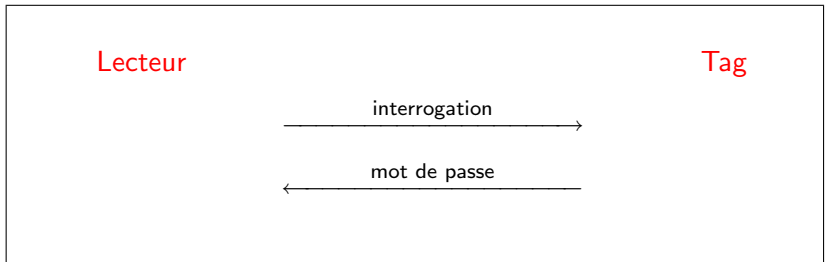
Exemple de contrôles d'accès



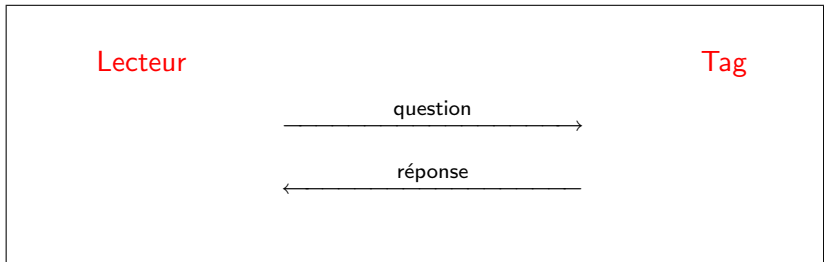
Protocole d'identification



Protocole d'authentification d'Ali Baba



Protocole de contrôle d'accès



- ▶ Ne pas réduire les coûts en utilisant un algorithme **faible**.
- ▶ Utiliser des algorithmes **reconnus** (sécurité par l'obscurité).
- ▶ Exemple de la carte du **MIT**.
- ▶ Exemple du module de **Texas Instrument**.

- ▷ Application **prometteuse**.
- ▷ Quelle est la **réelle** sécurité ? Quel est l'**adversaire** ?
- ▷ Réduire les risques mais les éliminer est **impossible**.
- ▷ La sécurité est essentiellement **physique**.

CONCLUSION

- ▷ Définir les **besoins** en terme de sécurité.
- ▷ Evaluer les **risques** et **conséquences** (concepteur ou utilisateur).
- ▷ **Prix** à payer.
- ▷ Comment **réagir** en cas de problème.
- ▷ **Communication** avec clients / utilisateurs.



RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification.

By Klaus Finkenzeller.



RFID: Applications, Security, and Privacy.

By Simson Garfinkel and Beth Rosenberg (Eds)



Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID.

By Katherine Albrecht and Liz McIntyre

- ▷ <http://www.rfidanalysis.org>
- ▷ <http://www.spychips.com>
- ▷ <http://www.foebud.org>
- ▷ <http://www.rsasecurity.com/rsalabs>
- ▷ <http://lasecwww.epfl.ch/~gavoine/rfid>

Contact

avoine@mit.edu / www.avoine.net