

# RFID et sécurité font-elles bon ménage ?

**Gildas Avoine**

Massachusetts Institute of Technology  
Cambridge, MA 02139, USA

[www.avoine.net](http://www.avoine.net)

Introduction à la RFID

Classification des menaces

Faiblesses des contrôles d'accès

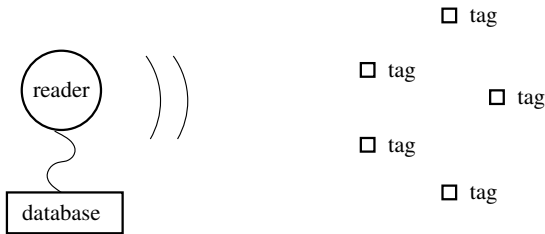
# Introduction à la RFID

# Définition et architecture

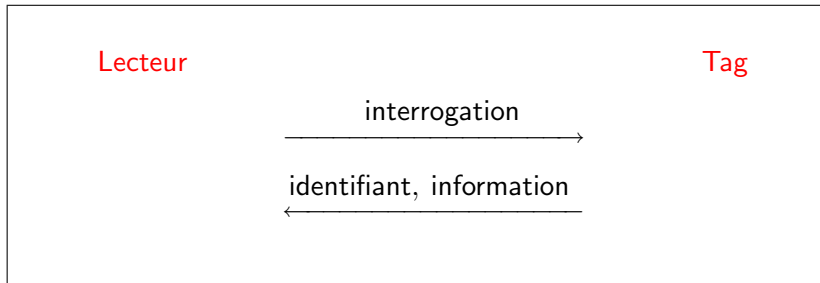
## Definition

## RFID

L'identification par radiofréquence (**RFID**) est une méthode pour identifier à distance des objets ou des sujets en interrogeant des transpondeurs (**tags**) à l'aide d'un lecteur.



# Protocole d'identification



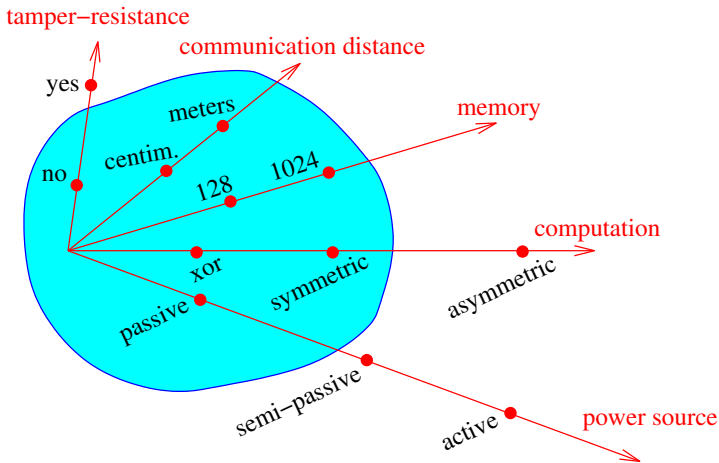
# Tags



# Lecteurs



# Caractéristiques des tags



## Exemples d'applications

- ▷ 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

# Classification des menaces

# Devises personnelles

- ▷ 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**.

# Ce que doit faire l'application

Je veux :

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

# Ce que ne doit pas faire l'application

## Je ne veux pas :

- ▷ Qu'un adversaire puisse perturber mon système.  
⇒ **Dénis de service.**
- ▷ Qu'un adversaire puisse voler de l'information.  
⇒ **Fuite d'information.**
- ▷ Qu'un adversaire puisse tracer les tags.  
⇒ **Traçabilité malveillante.**
- ▷ Qu'un adversaire puisse se faire passer pour un tag légitime.  
⇒ **Usurpation d'identité.**

# Identification vs Authentication

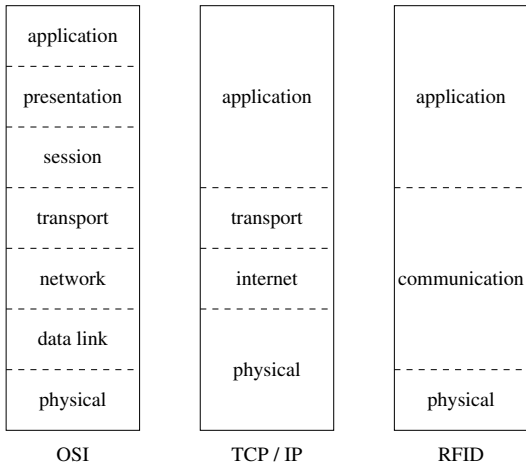
## Identification :

- ▶ Dénis de service, fuite d'information, (traçabilité malveillante).
- ▶ Traçabilité dans les chaînes de production, bibliothèque, marquage du linge dans les blanchisseries, etc.

## Authentication :

- ▶ Denis de service, fuite d'information, usurpation d'identité, (traçabilité malveillante).
- ▶ Abonnement aux transports publics, badge d'accès, clef de démarrage de voitures, etc.

# Dénis de service



## Dénis de service : solutions

- ▶ Se **prémunir** des dénis de service est très difficile quand il y a une interface avec l'extérieur.
- ▶ Attaques **faciles** à mettre en œuvre à moindre coût.
- ▶ **Conséquences** pouvant être importantes : exemple chaîne de production stoppée.
- ▶ Il faut vivre avec et savoir comment **réagir**.

# Fuite d'information

- ▷ Information révélée par le **systeme**.
  - ▶ **libertés individuelles** et **espionnage industriel**.
  - ▶ Problème existant : utiliser les techniques usuelles.
- ▷ Information révélée par le **tag**.
  - ▶ Facilité de **recueillir** l'information.
  - ▶ Passeport électronique, camion sur un parking.
  - ▶ **Éviter de stocker** des informations sur le tag.

# Fuite d'information

▷ Information rév

▶ libertés ind

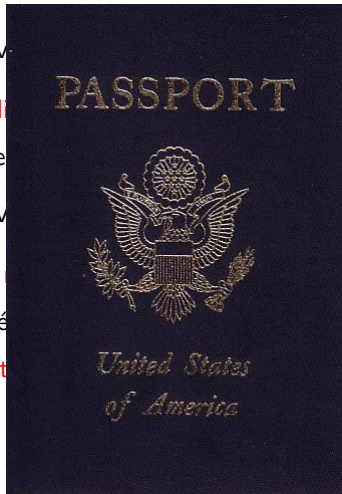
▶ Problème e

▷ Information rév

▶ Facilité de

▶ Passeport é

▶ Éviter de st



iel.

usuelles.

king.

ag.

# Fuite d'information

- ▷ Information
  - ▶ liberté
  - ▶ Problè
- ▷ Information
  - ▶ Facilité
  - ▶ Passep
  - ▶ Éviter



# Fuite d'information

- ▷ Information révélée par le **systeme**.
  - ▶ **libertés individuelles** et **espionnage industriel**.
  - ▶ Problème existant : utiliser les techniques usuelles.
- ▷ Information révélée par le **tag**.
  - ▶ Facilité de **recueillir** l'information.
  - ▶ Passeport électronique, camion sur un parking.
  - ▶ **Éviter de stocker** des informations sur le tag.

## Fuite d'information (Techniques palliatives)

- ▷ Distance de communication adaptée
- ▷ Kill-command
- ▷ Cages de Faraday
- ▷ Blocker tags
- ▷ Antenne amovible
- ▷ Bouton sur le tag
- ▷ Réglementations

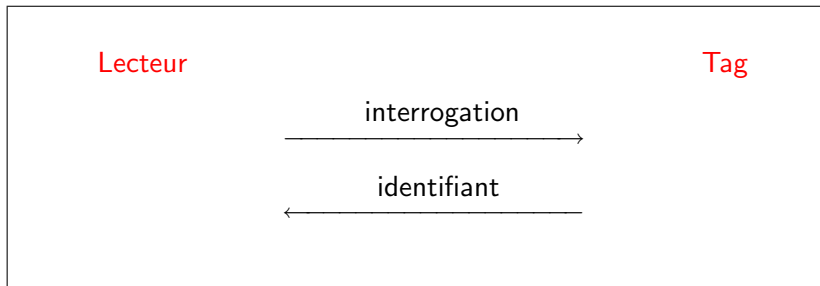
# Fuite d'information (Utiliser la cryptographie)

- ▷ **Chiffrement** du contenu du tag.
- ▷ **Authentification** du lecteur auprès du tag.
- ▷ Problème de la **gestion des clefs**.
- ▷ Les tags ne sont pas **tamper-resistant**.
- ▷ Combiner RFID et **lecture optique**.

# Usurpation d'identité

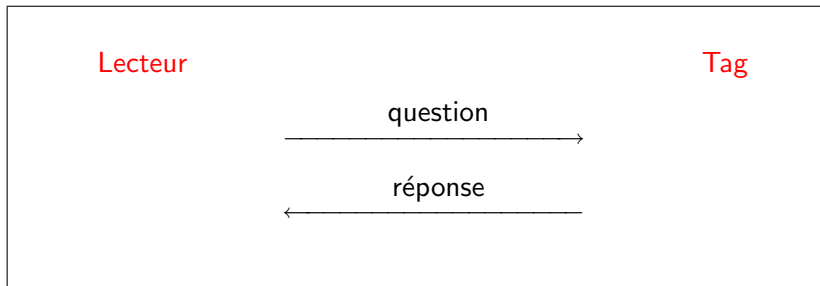


# Usurpation d'identité (Protocole de contrôle d'accès)



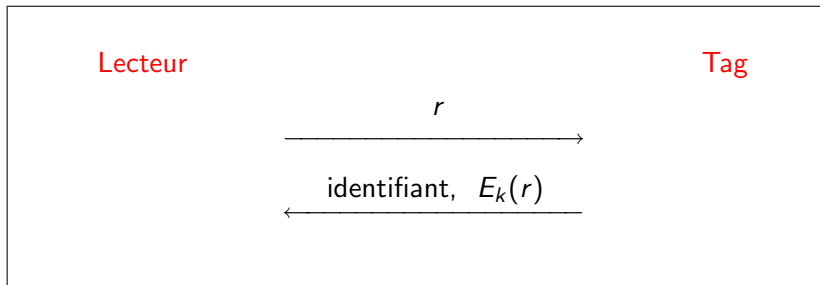
- ▶ Cryptographie **symétrique** uniquement.
- ▶ Ne pas réduire les coûts en utilisant un algorithme **faible**.

# Usurpation d'identité (Protocole de contrôle d'accès)



- ▶ Cryptographie **symétrique** uniquement.
- ▶ Ne pas réduire les coûts en utilisant un algorithme **faible**.

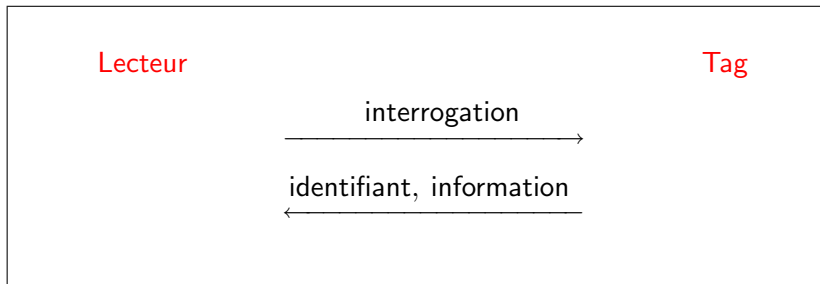
# Usurpation d'identité (Protocole de contrôle d'accès)



- ▶ Cryptographie **symétrique** uniquement.
- ▶ Ne pas réduire les coûts en utilisant un algorithme **faible**.

- ▶ Etant donné un ensemble de communications tags/lecteurs, un **adversaire** ne doit pas être capable de trouver des relations entre ces communications.
- ▶ Tracer des **employés** dans une entreprise, tracer des troupes militaires, etc.

# Traçabilité malveillante (Protocole d'identification)



# Traçabilité malveillante (Réalité ou fiction ?)

- ▶ Possible **techniquement**. En pratique ?
- ▶ Certaines organisations de défense des libertés individuelles s'opposent à la RFID : **Caspian**, **Foebud**.
- ▶ Différences entre RFID et autres **technologies** (vidéo, cartes de paiement, téléphonie mobile, Bluetooth) ?

# Traçabilité malveillante (Réalité ou fiction ?)

▷ Possible tech

▷ Certaines org  
s'opposent à

▷ Différences e

paiement, téléphonie mobile, Bluetooth) ?



individuelles

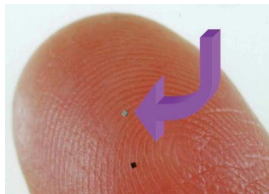
o, cartes de

# Traçabilité malveillante (Réalité ou fiction ?)

- ▶ Possible **techniquement**. En pratique ?
- ▶ Certaines organisations de défense des libertés individuelles s'opposent à la RFID : **Caspian**, **Foebud**.
- ▶ Différences entre RFID et autres **technologies** (vidéo, cartes de paiement, téléphonie mobile, Bluetooth) ?

# Traçabilité malveillante (Particularités de la RFID)

- ▶ 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**.

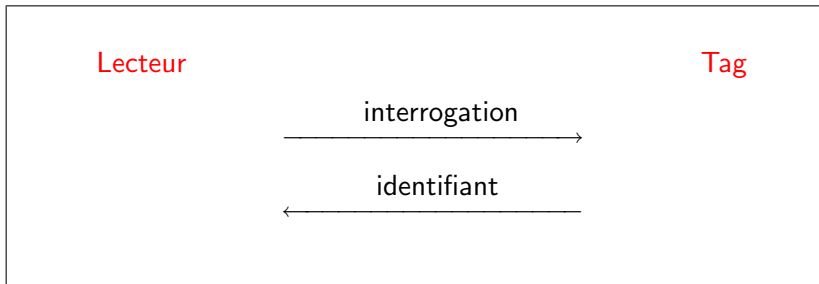


## Traçabilité malveillante (Utiliser la cryptographie)

- ▷ Nouveau **concept** en cryptographie.
- ▷ Protocole tel que l'information renvoyée par le tag est **indistinguable** (par un adversaire) d'une valeur aléatoire.
- ▷ Le lecteur doit essayer **toutes les clefs**.
- ▷ Possible de **réduire les capacités** de l'adversaire.
- ▷ Attaques par **canaux cachés**.

# Faiblesses des contrôles d'accès

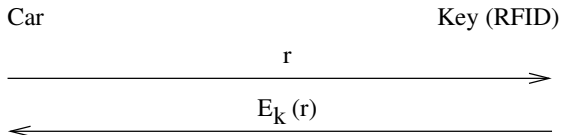
# Contrôle d'accès du MIT



**Agrawal said:** "If you are counting cattle, the cattle are not going to impersonate each other; there is no need for strong encryption. Members of the MIT population are not cattle; we need strong encryption."

# Digital Signature Transponder de Texas Instrument

- ▷ Attaque de Bono *et al.* sur le DST de TI.

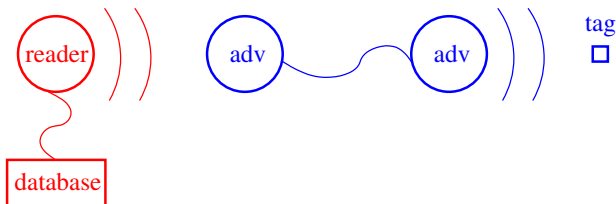


- ▷ L'algorithme de chiffrement n'est pas public.
- ▷ Clef cryptographique de longueur **40 bit**.
- ▷ Cassage en **moins d'une minute** (TMTO).

Recovering the cryptographic key / Impersonating the ignition key / Impersonating the SpeedPass card

# Attaque par relai

- ▶ Le lecteur croit que le tag est dans son champ électromagnétique alors que ce n'est pas le cas. L'adversaire joue le rôle d'une ralonge électrique.



- ▶ La parade consiste à calculer le temps de réponse du tag.

# CONCLUSION

# Conclusion

## Je ne veux pas :

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