

Sécurité de la RFID : comprendre la technique sans être un technicien

Gildas Avoine

UCL, Louvain-la-Neuve, Belgium

www.avoine.net



Identification par radiofréquence

L'identification par radiofréquence (**RFID**) est une technique qui permet d'identifier à **distance** des objets ou des personnes munis d'un transpondeur (micro-circuit + antenne), appelé **tags**.

Par extension, la RFID permet aussi de **recupérer des données** stockées sur le tag, éventuellement récupérer le **résultat d'un calcul** réalisé par le tag.



Architecture et caractéristiques de la RFID à bas coût



- ▷ **Énergie:** reçue du lecteur (tags passifs).
- ▷ **Communication:** quelques centimètres à mètres.
- ▷ **Calculs:** simple mémoire jusqu'à microprocesseur.
- ▷ **Mémoire:** centaine de bits jusqu'à plusieurs kilo-octets.
- ▷ **Prix:** dizaine de centimes jusqu'à quelques euros.

Quelques exemples d'applications



▷ Qui est la victime ?

- ▷ Le porteur du tag
- ▷ Le propriétaire du système

- ▷ Qui est la victime ?
- ▷ Qui est l'adversaire ?
 - ▷ Un pirate solitaire
 - ▷ Une bande organisée
 - ▷ Un organisme gouvernemental
 - ▷ Le propriétaire du système

- ▷ Qui est la victime ?
- ▷ Qui est l'adversaire ?
- ▷ Comment est réalisée l'attaque ?
 - ▷ Attaque contre le tag
 - ▷ Attaque sur le canal de communication
 - ▷ Attaque sur le système

- ▶ Qui est la victime ?
- ▶ Qui est l'adversaire ?
- ▶ Comment est réalisée l'attaque ?
- ▶ Quel est le but de l'attaque ?
 - ▶ Usurpation d'identité
 - ▶ Fuite d'information
 - ▶ Traçabilité malveillante
 - ▶ Déni de service

Usurpation d'identité

- ▷ Comment se faire passer pour un autre tag
→ Tag **cloné**, **faux** nouveau tag.
- ▷ N'a de sens que dans le cas de l'**authentification**.
- ▷ La **victime** est généralement le système.



- ▶ L'information est révélée par le **tag**.
 - ▶ Facilité d'**obtenir** de l'information (données ou identifiant).
 - ▶ La victime est le porteur du tag : données **personnelles**.
 - ▶ La victime est le système : données sur l'**entreprise**.

- ▶ L'information est révélée par le **tag**.
 - ▶ Facilité d'**obtenir** de l'information (données ou identifiant).
 - ▶ La victime est le porteur du tag : données **personnelles**.
 - ▶ La victime est le système : données sur l'**entreprise**.



- ▶ L'information est révélée par le **tag**.
 - ▶ Facilité d'**obtenir** de l'information (données ou identifiant).
 - ▶ La victime est le porteur du tag : données **personnelles**.
 - ▶ La victime est le système : données sur l'**entreprise**.

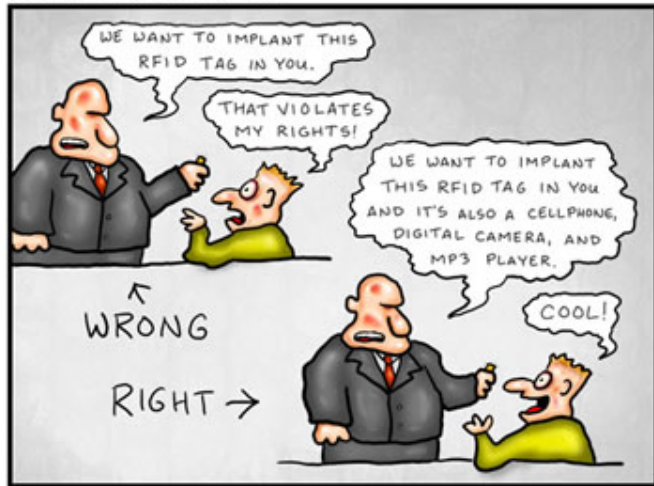


- ▶ L'information est révélée par le **tag**.
 - ▶ Facilité d'**obtenir** de l'information (données ou identifiant).
 - ▶ La victime est le porteur du tag : données **personnelles**.
 - ▶ La victime est le système : données sur l'**entreprise**.
- ▶ L'information est révélée par le **système**.
 - ▶ La victime est le porteur du tag ou le système.
 - ▶ Problème existant mais **amplifié** : plus en plus de données collectées.
 - ▶ Responsable ne prend pas **conscience** du problème, **vol** d'information, fuite **accidentelle**, utilisation **abusive**, etc.

- ▷ L'information renvoyée par le tag permet de le **tracer**.
- ▷ Vrai d'un point de vue purement **technique**.
- ▷ Mise en **pratique** ?
- ▷ Attaque évitée dans certains systèmes (ex: **passeport**)

DOCTOR FUN

16 Jan 2006



Copyright © 2006 David Farley, d-farley@ibiblio.org
<http://ibiblio.org/Dave/drfun.html>

This cartoon is made available on the Internet for personal viewing only. Opinions expressed herein are solely those of the author.

Déni de service (disponibilité)

- ▷ **Perturber** un système RFID: fun, concurrent, etc.
- ▷ **Moyens** peuvent être brouillage électromagnétique, tuer les tags, exploiter un bug, cacher des tags, etc.
- ▷ La **victime** directe est le système.

Conclusion

- ▶ La **victime** n'est pas toujours celle que l'on croit être.
- ▶ Le **pirate** n'est pas toujours celui que l'on croit être.



Magazine **MISC** Numéro 33 (Septembre/Octobre 2007), dossier spécial sur la sécurité de la RFID (Auteurs: A. Juels, K. Albrecht, JJ. Quisquater, M. Girault, S. Lacour, etc.). [<http://www.miscmag.com>]



Site web / Liste de diffusion sur la sécurité de la RFID. [<http://www.avoine.net>]