Sécurité des tags RFID

FABIEN ALLARD, SENSEYOU

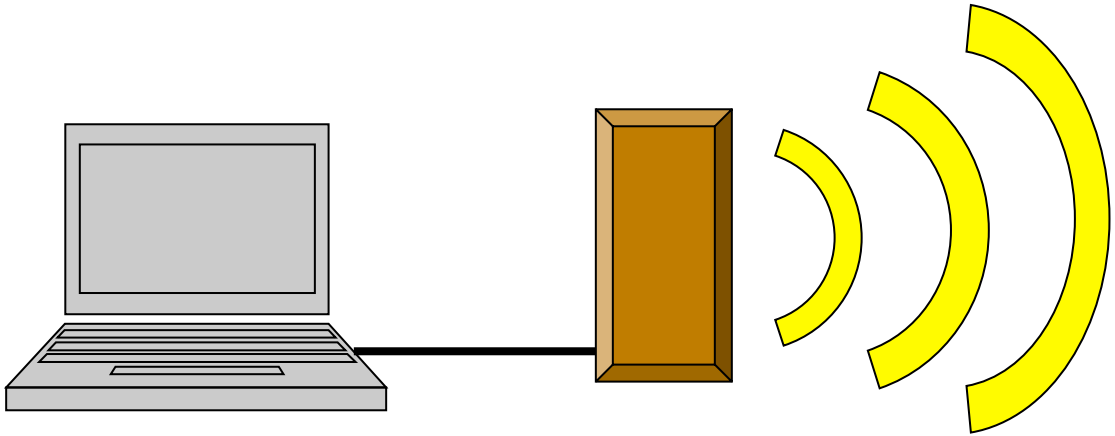
Avant propos

- SenseYou, une start-up issue d'INRIA
  - Expertise en informatique ambiante
  - Spécialiste RFID

- But de la présentation
  - Sensibilisation aux problématiques de sécurité des technologies RFID
  - Présentation de bonnes pratiques
  - Technicité limité

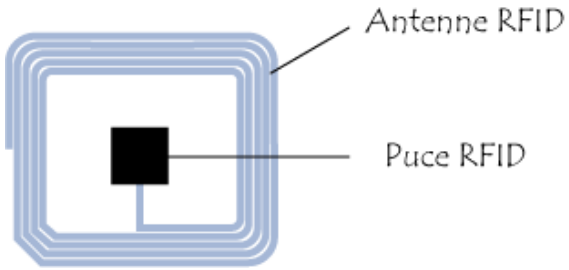
RFID et Objets connectés

Radio Frequency Identification (RFID)



Installation fixe ou mobile avec appareil de lecture

Rattachée à l'appareil de lecture, l'antenne génère les ondes radioélectriques



Le transpondeur réagit aux ondes radioélectriques en entrant dans le secteur du champ d'induction

RFID

- Deux grandes familles
  - Actif (Classe 3 à 5)
  - Passif (Classe 0 à 2)

- Quatres gammes de fréquences en passif
  - LF : 125 et 134,2 KHz
  - HF : 13,56 MHz
  - UHF : 868 à 915 MHz
  - SHF : 2,45 et 5,8 Ghz

Les plus utilisés dans le cadre des objets connectés

RFID

- Tags passifs peu chers
  - Quelques centimes pour des tags UHF
  - Jusqu'à quelques euros pour des tags HF NFC suivant l'inlay
- Tags actifs chers et à durée de vie limité
- Toutes les gammes de fréquences sont sensibles au métal (réflexion)
  - Le rayonnement UHF est aussi absorbé par l'eau

Utilisation dans le cadre des objets connectés

- Les tags RFID sont des mémoires réparties dans l'environnement
- Les lecteurs/antennes déterminent des zones de collecte de ces mémoires
- Chaque collecte engendre un contexte permettant au système d'avoir une réponse appropriée

Quelques exemples de systèmes

- Contrôle d'accès
  - Transport en commun (Pass Navigo, Velib…)
  - Entrée/sortie d'un bâtiment

- Affichage contextuel d'informations
  - Adapter la langue d'un contenu sur un écran commun
  - Publicité interactive
  - Transférer tout ou partie des informations sur un terminal personnel

- Logistique : suivi d'objets et de processus

Pour la suite…

- Se limiter aux deux normes les plus répandues
  - UHF : peu cher et permettant la lecture à quelques mètres
  - HF : plus de sécurités disponibles, norme dans laquelle évolue les tags NFC

- Les tags actifs sont des systèmes embarqués plus « classiques » qui autorisent l'utilisation de plus de sécurités.

Problématiques de sécurité

Types d'attaques

- Destruction
  - Physique (Casse, Shielding…)
  - Impulsion électromagnétique
  - Envoi de commandes type KILL ou LOCK
  - Ecrasement de données

- Clonage
  - Copie sur un tag vierge
  - Emulation d'un tag (Spoofing)

- Ecoute (cf présentation de Mr ALLAIN, Opale Sécurité)

Conséquences des attaques

- Arrêt du service
- Attaque sur les logiciels du système
  - Injection de code en utilisant la mémoire des tags
- Usurpation d'identité
- Mise en place d'un système d'information alternatif
  - Suivi d'objets ou de personnes en dehors du cadre du système

Réponses aux attaques

- Moyens fournis par les normes et/ou les constructeurs
  - Authentification des lecteurs et des tags
  - Cryptage des données et communications
  - Identifiant dynamique

- Destruction des tags après usage

- Protection logicielle
  - Cohérence des données
  - Cryptage
  - Anonymisation des données

UHF

- Sécurités disponibles dans la norme
  - Passwords de 32bits
  - Q protocol : les identifiants ne sont jamais communiqué en entier

- Quelques initiatives des contructeurs
  - PUF (Physical Unclonable Functions)
  - Algorithmes propriétaires pour authentification et cryptage

- Conclusion : Aucune réelle sécurité

HF (NFC)

- Algorithmes disponibles en ISO 14443A
  - 3DES
  - AES 128

- Authentification du tag et du lecteur

- Sécurité suffisante pour des applications standard

Limitations

- Les contraintes de l'application ne laisse pas forcément le choix de la norme
  - Coût
  - Distance de lecture

- Sécurités relatives quelque soit la norme
  - Prendre conscience des limites
  - Anticiper au maximum les failles potentielles

Exemples de défaut de sécurisation

Le passeport RFID en 2006

- La puce RFID contient les informations du passeport et une photo (donnée biométrique)
  - Informations signées numériquement
  - Système BAC : lecture optique d'une zone du passeport pour récupérer la clé secrète d'encryption des données
  - Feuillet métallique pour empêcher la lecture du passeport fermé

Les failles du passeport RFID en 2006

- Détectable à plusieurs centaines de mètres en écoute passive
  - Puce non lisible mais son type permet de déterminer la nationalité du porteur
  - Feuillet métallique inefficace dès que le passeport n'est plus fermé totalement

- Système BAC sensible aux attaque brute force
  - Possibilité de cloner un passeport en quelques heures
  - Corrigé par un système à clé publique (EAC) en 2009

- Source : Rapport des chercheur du réseau d'excellence européen FIDIS (Futur de l'identité dans la société de l'information) de septembre 2006
  - http://www.fidis.net/press-events/press-releases/declaration-de-budapest/#c1301

Exploitations possibles

- Création de faux passeports
  - Pour rappel la décision d'utiliser des passeports RFID vient de l'utilisation de faux passeport dans les attentats de 2001.

- Utiliser un vrai passeport comme détonateur
  - https://www.youtube.com/watch?v=-XXaqraF7pI

Carte bancaire NFC

- Carte bleue avec puce RFID pour paiement sans contact
- Utilisation d'une puce 14443A pour stocker les informations bancaires
- Le protocole EMV (Europay Mastercard Visa) remplace la saisie de code.
- Déploiement en 2012

Les failles des cartes bancaires NFC

- Ensemble des données en clair (Renaud Lifchitz, conférence Hackito Ergo Sum 2012)
  - Nom, prénom, numéro de carte, date d'expiration, listing des 15 dernières opérations
  - « Défaut » corrigé depuis.

- Protocole EMV non adapté : le mode « hors ligne » pour les paiements MasterCard
  - Transactions stockées en clair, permettant un débit maximum de 999 999,99€
  - Sans correctif connu à ce jour.
  - Faille découverte par l'université de New Castle en 2014 http://www.ncl.ac.uk/press.office/press.release/item/contactless-cards-fail-to-recognise-foreign-currency

Conclusion sur ces exemples

- Intégration forcée de technologies RFID dans des systèmes anciens
  - Création de failles de sécurité
  - Ancien protocoles non adaptés

- Erreurs basiques
  - « Oubli » de chiffrer des informations
  - Clé secrète trop facilement accessible et sans gestion de son renouvellement

Conclusion

Conclusion

- Prendre conscience des limites des technologies RFID en terme de sécurité

- Penser au rapport risque/bénéfice avant de déployer de tels système

- Anticiper les failles
  - Conception du système d'information sous-jacent
  - Anticipation des coût

Questions