Etiquetes RFID i privadesa

La lluita contra el Big Brother: tecnologia, percepció social i legislació sobre privadesa en la societat de la informació

Jordi Castellà-Roca

Universitat Rovira i Virgili,
Dept. Enginyeria Informàtica i Matemàtiques,
Av. Països Catalans, 26, E-43007 Tarragona, Catalunya
E-mail: jordi.castella@urv.cat

26 de juny de 2007

Índex

1. Introducció
2. Elements d'un sistema RFID
3. Aplicacions
4. Breu història
5. Privadesa
6. Conclusions

Introducció

RFID: què és?

- Radio-Frequency IDentification (RFID) - Identificació per ràdio freqüència.
- El terme RFID és emprat normalment per descriure qualsevol tecnologia que empra senyals de ràdio per identificar un objecte concret.
- RFID fa referència a qualsevol tecnologia que transmet un número identificatiu específic mitjançant ràdio.

Introducció

AIDC: què és?

- Automatic Identification and Data Collection (AIDC)
- Identificació automàtica i recollida de dades.
- Exemples: codis de barres, banda magnètica, RFID.

EPC: què és?

El sistema Electronic Product Code (EPC) és un conjunt d'estàndards i tecnologies desenvolupades al centre Auto-ID del MIT que permeten gestionar (identificar/seguir) el material en una cadena de subministrament.

Elements d'un sistema RFID

- Etiqueta RFID
- Lector RFID
- Antena adequada per la freqüència de ràdio desitjada.
- Xarxa d'ordinadors (opcional).

Elements d'un sistema RFID

Figura: Antena RFID 9610 fabricada per Alien Technology

Figura: Lector RFID 8780 fabricat per Alien Technology

Figura: Etiqueta RFID fabricada per Alien Technology

Etiqueta RFID

Cada etiqueta té les parts següents:

- Antena
- Xip de silici
  - Receptor de ràdio
  - Modulador de ràdio per respondre al lector de RFID
  - Lògica de control
  - Memòria
  - Sistema d'energia

Classificació segons el sistema d'energia

- Etiqueta activa: l'etiqueta disposa d'una bateria
  - Avantatges: rang de lectura (915MHz - 31 m), fiabilitat
  - Desavantatges: mida, preu alt, temps de vida
- Etiqueta passiva: l'energia sobté a partir del senyal de ràdio freqüència del lector de RFID
  - Avantatges: mida reduïda, baix cost, llarg temps de vida
  - Desavantatges: rang de lectura, fiabilitat
- Etiqueta semi-passiva: tenen una bateria (idem actives), però empren l'energia del lector per enviar la resposta
  - Avantatges: fiabilitat, temps de vida més gran que una etiqueta activa
  - Desavantatges: rang de lectura (idem passives)

Exemples de diferents mides d'etiquetes RFID

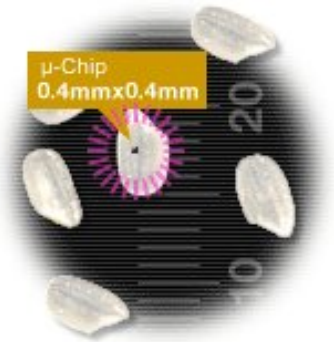

Figura: Etiqueta RFID de Hitachi mu-chip 0.4mm

Figura: Etiqueta RFID Verichip (implantable)

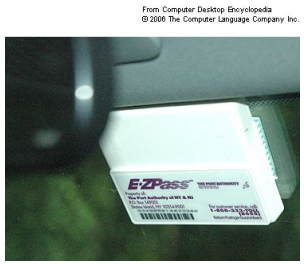

Figura: E-ZPass (permet pagar el peatge)

Modes de comunicació

- Promiscus: es comuniquen amb qualsevol lector.
  - Són els que estan més desplegats.
  - Tenen un baix cost.
  - La gestió d'aquests sistemes és més senzilla.
- Segurs: només responen si el lector envia la contrasenya correcta.
  - Les contrasenyes s'han de distribuir abans d'utilitzar les etiquetes.
  - La gestió de les contrasenyes dificulta el seu desplegament.

Identificació

- Les etiquetes més senzilles només tenen un número de sèrie.
- La longitud del número de sèrie pot anar de 64 a 96 bits per la primera generació de EPC i de 96 a 256 bits la segona generació de EPC.
- El número de sèrie pot ser programat per fabricant o per l'usuari final.
- En la majoria d'etiquetes la memòria on es guarda el número de sèrie només es pot gravar un cop.
- En les etiquetes més avançades el número de sèrie es pot gravar diversos cops.

Kill-off

- Algunes etiquetes es destrueixen quan reben un codi.
- Aquest codi rep el nom de Kill-off.
- Un cop s'envia aquest codi l'etiqueta deixa de respondre.

Interferències

- Les etiquetes RFID poden generar interferències les unes amb les altres.
- En alguns casos això no és un problema perquè només hi ha una etiqueta RFID (p.e. porta de l'aparcament).
- En els casos on llegir moltes etiquetes és essencial s'empren protocols anticol·lisió.
- Els protocols anticol·lisió reben el nom de *singulation protocol*.

Lector RFID

- Envia un pols d'energia de ràdio a l'etiqueta i escolta la resposta.
- L'etiqueta detecta l'energia i respon amb el seu número de sèrie i opcionalment amb altra informació.
- El pols d'energia pot actuar com un interruptor (encendre-apagar), o pot incloure comandes per l'etiqueta (llegir o escriure a la memòria, una contrasenya, etc...).

Lector RFID

- Lector monomode: només llegeixen un tipus concret d'etiquetes.
- Lector multimode: poden llegir diferents tipus d'etiquestes (tendència actual).

Antena RFID

L'energia de ràdio es mesura en funció de la freqüència a la que oscil·la i la potència.

Banda	**Freqüència lliure**	**Longitud d'ona**	**Usos**
LF	125-134.2 KHz	2400 m	Etiquetatge d'animals
HF	13.56 MHz	22 m	Accés sense claus
UHF	865.5-867.6 MHz (EU) 915 MHz (U.S.) 950-956 MHz (Japó)	32.8 cm	Targes intel·ligents Logística Gestió d'articles
ISM	2.4GHz	12.5 cm	Gestió d'articles

La xarxa

- El lector envia el número que ha obtingut de l'etiqueta a l'ordinador.
- Sistema de control d'accés: l'ordinador busca si el número està autoritzat.
- Sistema de pagament: el lector envia el número de sèrie de l'etiqueta i la resposta a un repte. Si tot és correcte es carrega l'import al client
- EPC: una BD conté la informació específica per cada número de sèrie de l'etiqueta.

Factors que dificulten la lectura de les etiquetes RFID

- L'aigua, els plàstics, les llaunes, o la gent poden afectar la correcta lectura d'un RFID, o fins i tot impossibilitar-la completament.
- En les bandes HF i UHF les barreres més importants són l'aigua i el metall.
- No es pot llegir una etiqueta dins d'una llauna.
- El paper d'alumini és suficient per impedir la lectura de les etiquetes RFID amb una potència més baixa.

Aplicacions

- Fabricació
- Distribució i inventari
- Venda al detall
- Rastreig de documents
- Seguretat
- Subministre d'aliments
- Assitència sanitària

Fabricació

- Comprovar que la caixa d'un producte conté tots els ítems.
- Rastrejar una producte al llarg d'un procés productiu i registrar cada eina que hi ha fet una operació.

Distribució i inventari

- Mantenir un inventari de forma acurada.
  - Elimina la necessitat del recompte físic.
  - Assegura la disponibilitat d'un producte.
- Operation Iraqi Freedom: identificar les unitats de l'interior dels contenidors de càrrega.
- Tots els enviaments marítims al Department of Defense (DoD) dels USA han d'estar etiquetats amb RFID.

Venda al detall

- AIDC és molt útil per mantenir un nivell adequat d'estoc en la distribució de bens, i especialment en el cas de bens peribles.
- Reduir els robatoris.
- Reduir les pèrdues.

Rastreig de documents

- Radiografia d'un pacient en un Hospital.
- Prova criminal d'un judici.
- Inventari de fitxers en oficines d'advocats.

Seguretat

- Accés a l'aparcament.
- Accés a àrees protegides.
- Rastreig de persones dins d'una àrea.
- Passaports, visats.
- Evitar la importació d'armes químiques o biològiques.

Subministre d'aliments

- Control dels aliments: malaltia de les vaques boges, hepatitis, etc...
- Els RFID permeten mantenir l'historial dels animals i dels aliments.
- UK: és obligatori poder rastrejar un paquet de carn d'un supermercat fins l'animal. S'ha de poder consultar l'historial de l'animal i la seva alimentació.

Assistència sanitària

- La informació mèdica del pacient pot ser vital per salvar-li la vida.
- Una targeta intel·ligent (Smart-Card) pot guardar aquesta informació.
- Identificació dels pacients.
- Enregistrament dels medicaments subministrats als pacients.
- Manteniment de l'estoc dels medicaments, equipament, etc...

Aplicacions Futures

- RFID amb sensors
- Autenticitat dels fàrmacs
- Autenticitat dels productes
- Articles intel·ligents

Sensors

- Els RFID poden mesurar la temperatura, la humitat, els impactes, i altes condicions ambientals.
- Permeten monitoritzar de forma remota un producte.
- Algunes etiquetes (semi-passives) poden mantenir un registre de les mesures.
- Exemples:
  - Monitoritzar l'emmagatzematge de menjar refrigerat.
  - Monitoritzar el procés d'enduriment d'una estructura de formigó.

Autenticitat farmacèutica

- La falsificació de medicaments és un problema actual.
- Les conseqüències poden ser greus.
- Els RFID permetrien demostrar el pedigrí dels productes farmacèutics.
- Cada paquet podria ser rastrejat.
- Qualsevol anomalia en el procés podria ser detectada.

Autenticitat dels productes

- Falsificació dels productes.
- La indústria deslocalitza la producció de béns a països amb poca cultura de la propietat intel·lectual.
- La falsificació afecta tota la cadena de consum, des del fabricant fins al consumidor.

Articles intel·ligents

- Informació de la garantia.
- Forn Microones que cuina els aliments a partir de la informació del RFID del producte.
- Rentadora que segons les peces de roba selecciona el programa de rentat més adient.
- Un armari dels medicaments intelligent que recorda al pacient que ha de prendre una medicació.
- També podria avisar d'una medicació erronea o al metge que el pacient no segueix la medicació.

Breu Història

- 1939 (UK) Segona Guerra Mundial - IFF (Identification Friend or Foe).
- 1940-1950
  - Millora del radar.
  - Invenció del RFID: (UK) Harry Stockman, "Çommunication by Means of Reflected Power", Proceedings of the IRE, pp1196-1204, October 1948.
- 1950-1960. Primeres exploracions de la tecnologia RFID, experiments de laboratori.
- 1960-1970.
  - Desenvolupament de la teoria de RFID.
  - Inici de les aplicacions en proves de camp.

Breu Història

- 1970-1980
  - Explosió del desenvolupament de RFIDs.
  - Acceleració dels test de RFIDs.
  - Adopció primerenca de les implementacions de RFID.
- 1980-1990 Les aplicacions comercials dels RFID són adoptades àmpliament.
- 1990-2000
  - Es defineixen els estàndards de RFID.
  - Els RFID estan àmpliament desplegats.
  - Els RFID esdevenen una part de la nostra vida diària.

Breu Història

- 2002 (USA) Gillette realitza la compra de 500 milions d'etiquetes RFID.
- 2003 (USA) Wal-Mart sol·licita als seus 100 principals proveïdors la utilització d'etiquetes RFID en els seus productes.

Privadesa

Tres significats bàsics per privadesa:

- Aïllament: és el dret de restar amagats de la percepció dels altres.
- Soledat: és el dret d'estar sol.
- Autodeterminació: és el dret de controlar la nostra informació personal.

Amenaces: revelació d'informació

- Si portem articles o documents equipats amb etiquetes RFID (promíscues) qualsevol persona amb un lector de RFID podria obtenir la informació dels RFID sense la nostra autorització (passaport, diners, medicaments, etc..).
- La proximitat necessària per llegir l'etiqueta no ofereix una protecció suficient.

Amenaces: vigilància

- Si sabem que una persona porta una determinada etiqueta RFID i disposem de lectors de RFID podríem veure com es mou per l'espai. Podem saber on és físicament.
- Podem vincular una etiqueta RFID amb una persona sense la necessitat de saber a quin article fa referència.

Amenaces: perfil

- Si es vincula un RFID a una persona també s'hi poden vincular més etiquetes RFID.
- A mesura que agreguem més etiquetes anem creant un perfil de la persona.
- La possibilitat de saber per on es desplaça afegeix més informació al seu perfil.
- Aquesta valuosa informació es pot vendre a un tercer.

Amenaces: les xarxes de recollida d'informació

- Una xarxa de sensors i Internet poden facilitar la compartició de dades que facilitin la creació de perfils.
- La creació d'una xarxa de lectors de RFID per la recollida de dades pot ser possible si es porta a terme per diferents institucions que col·laborin.
- Els incentius per la col·laboració poden ser polítics o econòmics.

Amenaces: vinculació amb una persona concreta

- El perfil es pot vincular a una persona concreta en el moment que una de les etiquetes es pot vincular a una persona.
- El venedor d'un article pot vincular una etiqueta RFID amb una targeta de crèdit o directament amb el nom del comprador.

Amenaces: resum

Si tenim la situació següent:

- L'etiqueta no és desactivada després de la compra (kill-off).
- L'etiqueta és promíscua o la seguretat no és suficient.
- La vinculació entre l'etiqueta i la persona es revela.

Es poden donar les amenaces següents:

- Perfil personal
- Vigilància
- Actuació: un espai equipat amb un lector de RFID pot detectar la nostra presència i reaccionar.
  - Deternir-nos/Multar-nos, p.e. hem anat massa ràpid de casa a la botiga.
  - Oferir-nos publicitat en funció del nostre perfil (Minority Report).

Propostes tècniques pel problema de privadesa dels RFID

- Primeres mesures:
  - Facilitar la supressió de l'etiqueta RFID.
  - Kill-off al punt de venda.
- Perdem alguns dels beneficis al no poder utilitzar les etiquetes.
- En algunes etiquetes no podem utilitzar aquestes mesures.

Propostes tècniques pel problema de privadesa dels RFID

- Les etiquetes de baix cost actualment no poden realitzar operacions criptogràfiques.
- Es treballa en el desenvolupament d'algorismes criptogràfics per la seva utilització en RFIDs.

Algunes propostes:

- Bloquejador d'etiquetes (Blocker Tags)
- Bloqueig suau (Soft Blocking)
- Mesura de la relació Senyal-Soroll (Signal-to-Noise Measurement)
- Etiquetes amb pseudònims (Tags with Pseudonyms)

Bloquejador d'etiquetes (Blocker Tags)

- Les etiquetes RFID dels articles tenen un bit que indica si l'article és públic (no comprat) o privat (comprat).
- El bloquejador d'etiquetes és un dispositiu que quan un lector intenta llegir una etiqueta privada emet un senyal de jam.
- El lector de RFID rep un gran nombre de respostes, i això el col·lapsa.
- En un entorn sense bloquejador la informació dels RFID es pot utilizar.

Bloqueig suau (Soft Blocking)

- El bloqueig es fa al lector de RFID o en una aplicació de software.
- El lector només retorna la informació de les etiquetes públiques.

Mesura de la relació Senyal-Soroll (Signal-to-Noise Measurement)

- La mesura de la relació senyal-soroll dóna una indicació de la distància entre l'etiqueta i el lector.
- L'etiqueta només respon al lector en funció de la seva distància.

Etiquetes amb pseudònims (Tags with Pseudonyms)

- L'etiqueta RFID disposa de diferents números de sèrie.
- Cada cop que respon utilitza un número de sèrie diferent.
- Per evitar que un atacant conegui tots els pseudònims en un breu espai de temps es poden introduir retards.
- En versions més complexes el lector pot actualitzar els números de sèrie de l'etiqueta.

Criptografia

- Autenticació de l'etiqueta RFID amb algorismes criptogràfics (repte-resposta).
- Cada resposta de l'etiqueta és diferent.
- Només el lector autoritzat pot accedir a la informació.
- El fet de trencar una etiqueta no dóna accés a la resta d'etiquetes.
- Els protocols criptogràfics actuals més eficients es basen en funcions de resum (hash).
- La gestió i els cost de les etiquetes que implementen protocols criptogràfics dificulten la seva implantació.

Conclusions

- La tecnologia RFID cada cop s'imposa més a les nostres vides.
- La utilització de la tecnologia RFID sense mesures per evitar-ho pot suposar una greu vulneració de la nostra privadesa.
- Existeixen solucions tecnològiques que poden minimitzar aquests perills.

Moltes gràcies per la seva atenció.

Etiquetes RFID i privadesa

La lluita contra el Big Brother: tecnologia, percepció social i legislació sobre privadesa en la societat de la informació

Jordi Castellà-Roca

Universitat Rovira i Virgili,
Dept. Enginyeria Informàtica i Matemàtiques,
Av. Països Catalans, 26, E-43007 Tarragona, Catalunya
E-mail: jordi.castella@urv.cat

26 de juny de 2007