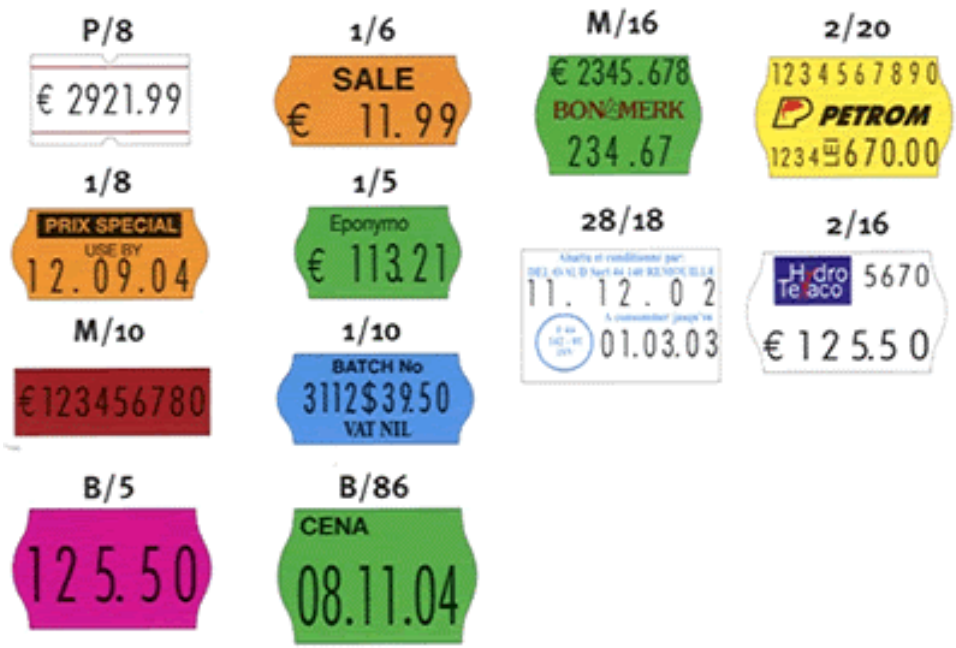
Seguridad en Sistemas RFID

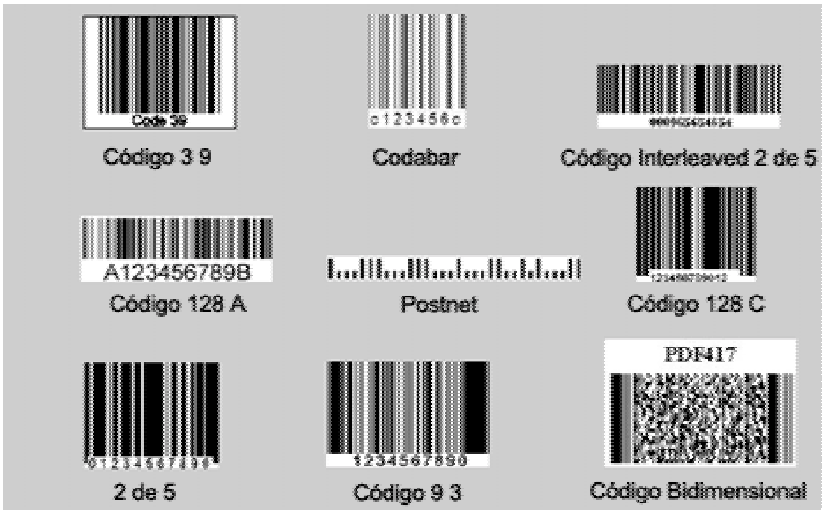
Roberto Gómez Cárdenas
ITESM-CEM
rogomez@itesm.mx
http://webdia.cem.itesm.mx/ac/rogomez

Erase una vez ...

Primero eran las etiquetas ...



Después fue el código barras



Pero ...

Los sistemas RFID

- Radio Frequency Identification Device
- RFID es una tecnología que usa ondas de radio-frecuencia para transferir datos entre un lector y un objeto móvil que debe ser identificado, clasificar, dar seguimiento...
- Son rápidos y no requieren de un contacto físico o “alineación” con respecto al lector/scanner y el objeto “etiquetado”

¿Qué constituye un sistema RFID?

- Una o más etiquetas
- Dos o más antenas
- Uno o más interrogadores
- Una o más computadoras
- Software apropiado

Componentes sistema RFID

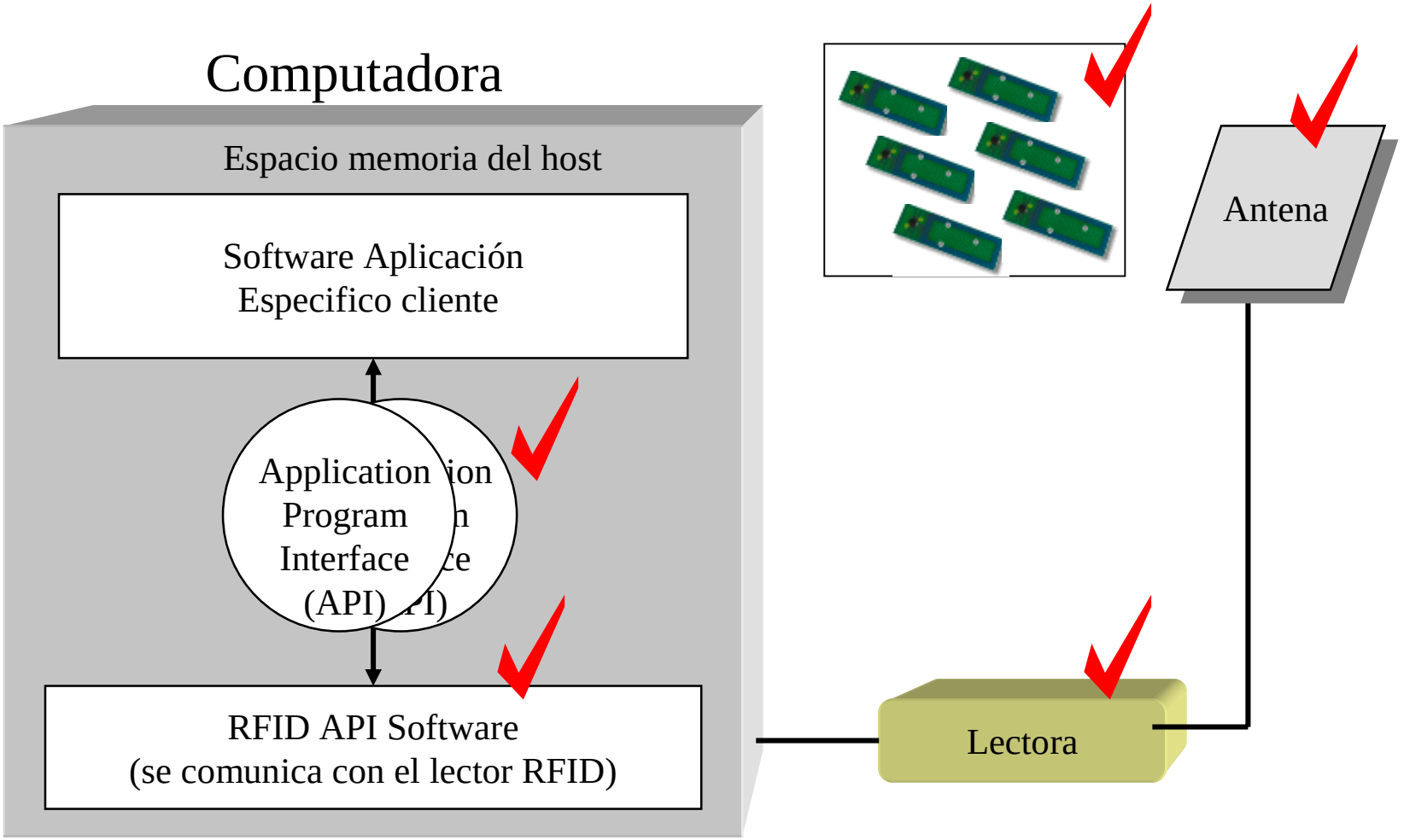
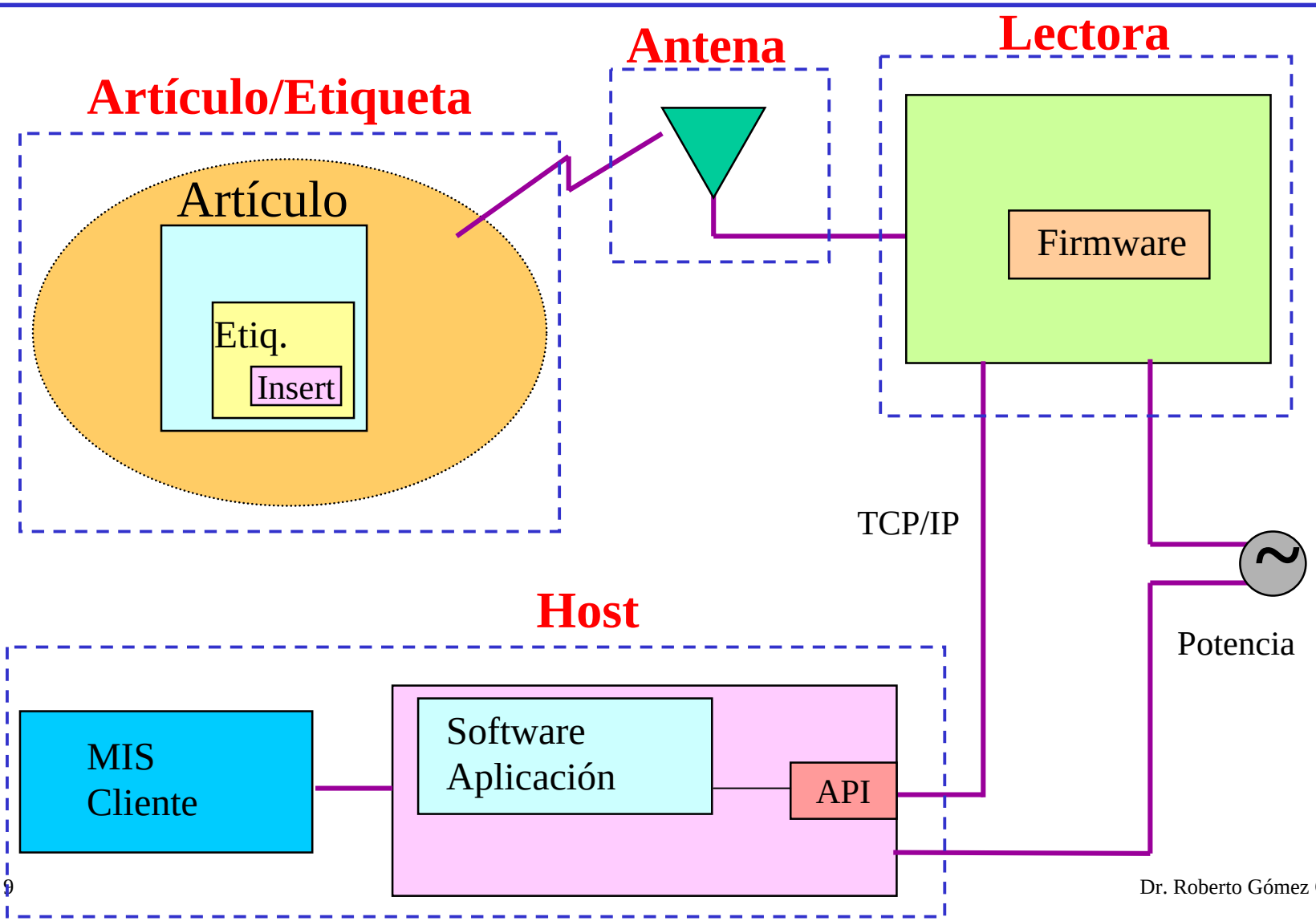


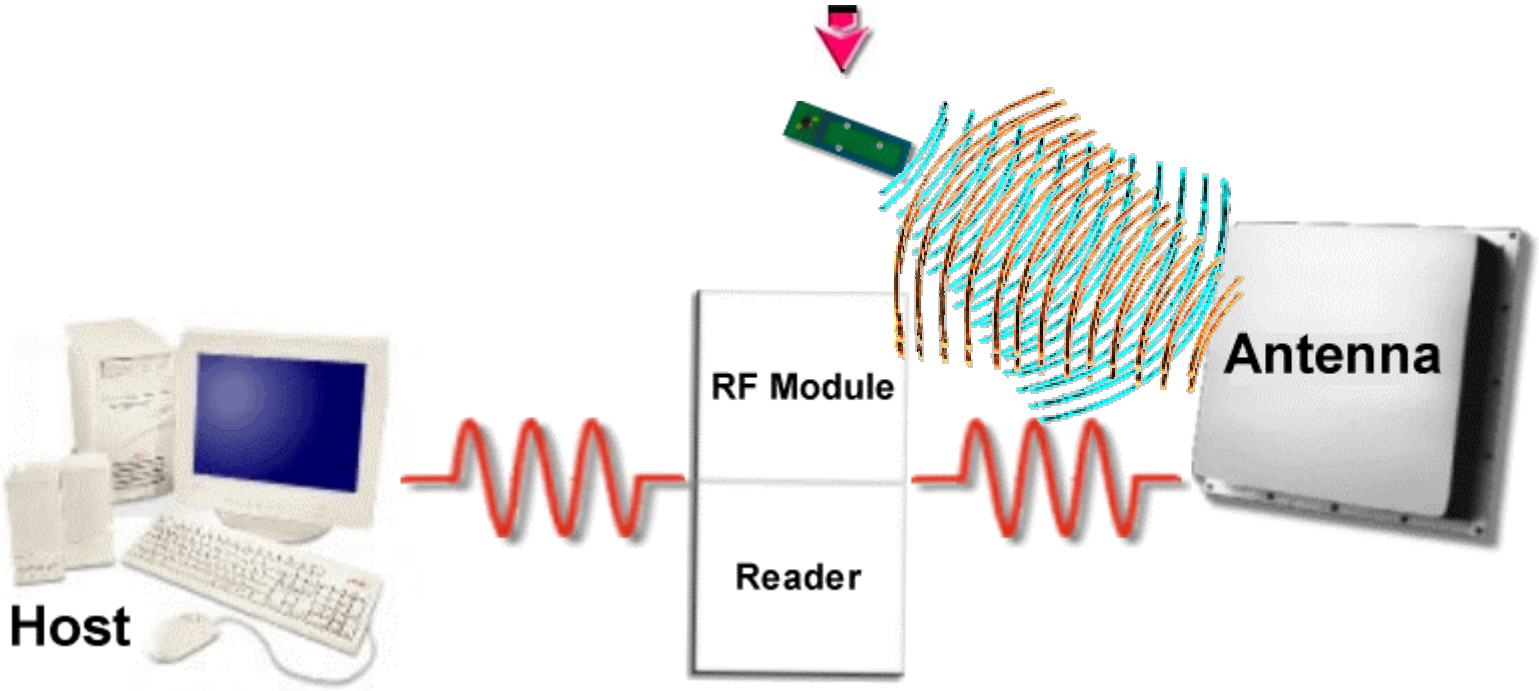
Diagrama bloques componentes



Operación RFID

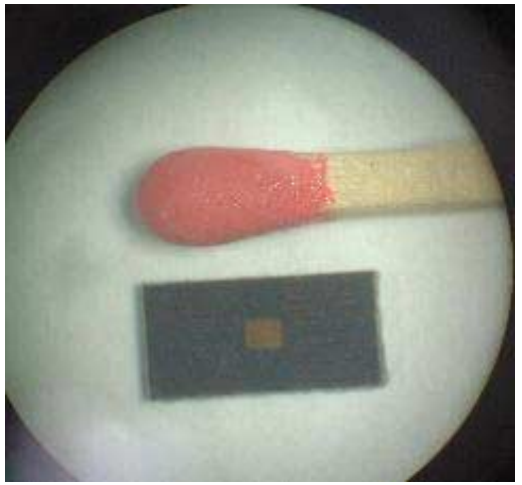
- Secuencia de comunicación
  - Host administra lector
  - Lector y etiqueta se comunican via señal RFID
  - La señal es generada por el lector
  - La señal es enviada a través de las antenas
  - La señal llega a las etiquetas
  - Etiqueta llega y modifica la señal
    - envía de regreso la señal modulada
  - Antenas reciben la señal modulada y la envían al lector
  - Lector decodifica losdatos
    - resultados son enviados al host que contiene la aplicación

Operaciones RFID



Las etiquetas

- Pueden ser de solo lectura o de lectura/escritura
- La memoria de la etiqueta puede ser programada, particionada o bloqueada permanentemente
- Bytes no bloqueados pueden ser re-escritos más de 1000,000 veces

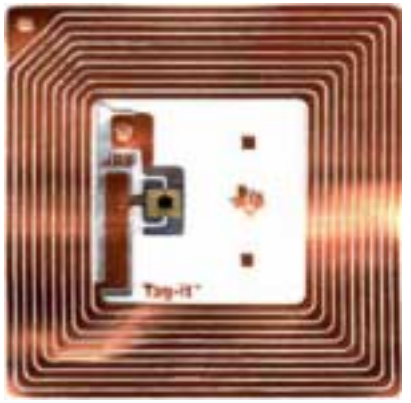


¿Donde pueden usarse?

- Pueden atarse a casi todo
  - vehículos
  - personal y activos de la compañía
  - objetos como aparatos,
  - gente, mascotas
  - objetos electrónicos de alto valor como computadoras, TVs, videograbadroas

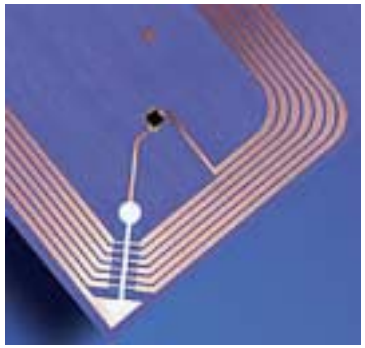
Tipos de etiquetas

- Activas
  - Las etiquetas transmiten señales de radio
  - Batería alimenta memoria, radio y circuitos
  - Alcance de unos 300 pies
- Pasivas
  - Reflejan señales de radio del lector
  - Alimentado por el lector
  - Alcance corto (4 pulgadas a 15 pies)



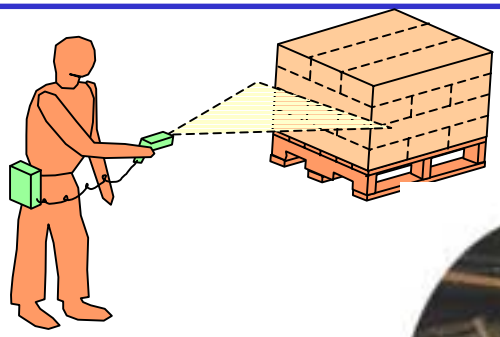
Variedad etiquetas

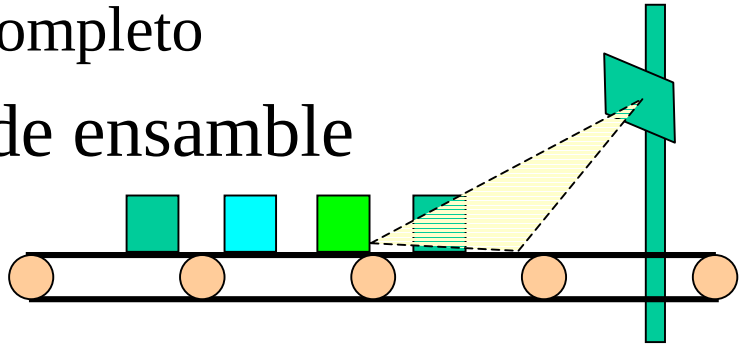
- Memoria
  - tamaño: 16 bits – 512 Kbytes
  - RO, R/W o WORM
  - Tipo: EEPROM, Antifuse, FeRAM
- Anti-colisión
  - habilidad para leer/escribir una o varias etiquetas al mismo tiempo
- Frecuencia
  - 125Khz – 5.8 Ghz
- Dimensiones fisicas
  - uña hasta ladrillo
- Precio (dolares, Alien Technologies)
  - unidad: 25 centavos por unidad
  - 1 billón unidades: 10 centavos por unidad
  - 10 billones unidades: 5 centavos por unidad

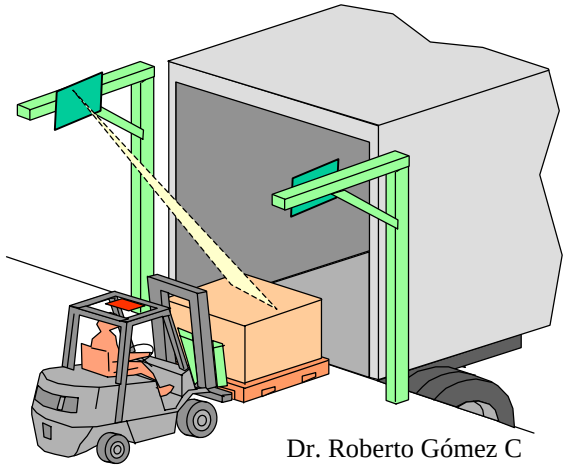


Aplicaciones

- Manejo inventarios
  - ¿qué es?
  - donde ha estado
  - a donde va
- Inspección de materiales
  - esta dentro de la garantía
  - ha sido inspeccionado
  - esta completo
- Líneas de ensamble







Mitos y realidades

- Mito
  - Tamaño RFID es de un pin y puede ser instalada en cualquier producto
  - Pueden ser leídos desde una gran distancia
- Realidad
  - Campos electromagnéticos presentan problemas con metal y otros materiales aislantes
  - Requieren antena, la cual tiene cierto tamaño
  - Distancia máxima: 10 metros

Etiquetas ISO 15693

- Etiqueta cuenta con un identificador único: UID
- UID es necesario para evitar colisiones
- UID es programado de fabrica y no puede ser cambiado
- Memoria etiqueta dividida en dos partes
  - bloque administrativo
    - UID: unique identifier
    - AFI: application family identifier
    - DSFID: data storage format identifier
  - datos usuario
    - almacena hasta 128 bytes de datos de usuario

Bloque administrativo

- Codificación identificador único

Byte							
7	6	5	4	3	2	1	0
E0h	MFR	Serial number					

- Códigos fabricante

MFR-Code	Company
02h	ST Microelectronics
04h	Phillips Semiconductors
05h	Infineon Technologies AG
07h	Texas Instrument
16h	EM Microelectronic-Marin SA

Datos usuario

page	Byte			
	0	1	2	3
Administrative block				
00h	User data block			
...	...			
3fh	User data block			

El EPC

- Etiquetas cuentan con un numero de serie y una EEPROM que puede almacenar información como el EPC
  - Electronic Product Code
- EPC
  - código internacional único del fabricante

EPC Type 1			
01	0000A66	00016F	000169DCD
Header	EPC Manager	Object Class	Serial Number
8 Bit	24 Bit	24 Bit	36 Bit

Cookies

- Tal y como en las páginas web es posible instalar una cookie en alguien que porte ropa con etiquetas inteligentes
  - cada vez que pase a través de una puerta o campo RFID, p.. en frente de la ventana de la tienda se incrementa en uno
  - la próxima vez que se cuente con un número de tarjeta de crédito, puede escribir la etiqueta de esta con un id en claro, posible saber quien estaba viendo la ventana de la tienda
  - posible verificar si un cliente toma un producto del estante y lo regresa, si el cliente no es confiable, se le puede hacer un descuento solo para el en 10 segs

RF-DUMP

- Herramienta para leer y escribir etiquetas ISO
  - escrita por Boris Wolf y Lukas Grunwald
- Detecta y opera sobre casi todas las etiquetas inteligentes
- Requiere un lector RFID ACG Compact-Flash
- Corre sobre un PDA o una notebook
- Software libre, GPL

Atacando Etiquetas Inteligentes

- La mayor parte no protegidas contra lectura
- UID y bloque administrativo no pueden almacenar el EPC
- EPC almacenado en el área del usuraio
- Meta datos como “best-before” también son almacenados en el área del usuario
- Solo es cuestión de tiempo que todo mundo utilice al menos una etiqueta RFID

Problemas de privacidad

- Lectores se pueden instalar en cualquier lugar
- Competidores pueden leer que tipo de vestimenta usa y que se tiene en la bolsa de comprars.
- Big Brother puede conocer que tipo de libros estamos leyendo
- Se le puede dar seguimiento al cliente por todos lados.

Futuros ataques

- La mayor parte del software es diseñado sin tomar en cuenta la seguridad
- Algunos registros llevan a cabo un reboot instantáneo después de leer una etiqueta con un campo manipulado.
- Si se envuelve la etiqueta , ningún sistema puede leer las etiquetas.

La tienda del futuro

Probando la tienda

Atacando la tienda

- Posible cambiar los precios de los artículos por otros más bajos.
- Cambiar contenido que describe el producto
- Divirtiendose con los EAS
  - La puerta de supervisión electrónica (EAS), verifica si alguien saca un DVD que no se pago
  - Para desactivar el sistema, tomar una etiqueta barata por 50 centavos, tomar la EPC de un DVD en el estante, transferirla el EPC del DVD a la etiqueta
  - Pegar la etiqueta bajo la puerta
  - La puerta activa una alamarma
  - Encarga atenderá alarma, después de 5 minutos desactivará la puerta.

Posibles soluciones

- Congreso “RFID Privacy Workshop” se propusieron varias soluciones
- Emitir números de identificación falsos a lectores no-autorizados
- Desarrollo de dispositivos de bajo costo para detectar y desactivar etiquetas RFID.
- Poder señales disminuyen conforme las etiquetas se alejan del lector
  - configurar etiquetas para ignorar peticiones abajo de un mínimo de potencia

Solución no tecnológica

- Problema criptologia en etiquetas
  - muy caro
- La mayor parte concuerda en que la solución, con respecto al problema de privacidad,
  - solución no esta del lado tecnológico;
  - definir una política que defina el tipo de información que puede contener una etiqueta y alertar al consumidor

RSA y RFID

- RSA desarrolla un dispositivo RSA Blocker Tag, dirigido a combatir los posibles efectos lesivos sobre la privacidad de consumidores y usuarios
- Se trata de una etiqueta RFID la cual previene que los lectores lean y den seguimiento a la gente o bienes, después de que fueron comprados – sin afectar el funcionamiento normal del RFID
- Solo teoría
  - prueba en productos farmacéuticos no fue un completo éxito

Algunas ligas interesantes

- http://www.stop-rd.org
- http://www.boycottgillette.com
- http://www.boycottbenetton.org
- http://www.spychips.com
- http://www.rfid-handbook.com

Conclusiones

- Toda nueva tecnología trae riesgos
- Los clientes pueden cambiar el EPC y nadie lo detectaría a la hora del pago
- Ataques pueden ser usados en drogas y material restringido a ciertas edades.
- Los atacantes solo necesita un dispositivo de lectura/escritura de RFID
  - software disponible públicamente
- Importante saber que estamos adquiriendo

Seguridad en Sistemas RFID

Roberto Gómez Cárdenas
ITESM-CEM
rogomez@itesm.mx
http://webdia.cem.itesm.mx/ac/rogomez