RFID – Otro round entre la funcionalidad y la seguridad

Por **Ezequiel Martin Sallis**
Senior Security Consultant
CISSP Certified

Introducción:

En la lucha eterna del equilibrio entre la seguridad y la funcionalidad, ya hemos visto pasar a varias tecnologías, solo por mencionar algunas 802.11, Bluetooth entre otras, pero como no podía ser de otra manera le llego el turno a RFID (Radio Frequency Identificación).

RFID, es una tecnología de identificación por radiofrecuencias, que permite el reconocimiento automático a distancia, basado en uno de sus principales componentes los TAGS (Etiquetas) de RFID, permitiendo esto un beneficio muy importante en lo que refiere a la logística, la distribución y la cadena de abastecimiento, pero como veremos mas adelante la aplicación de esta tecnología, también esta siendo adoptada en muchos otros aspectos y procesos, como el control de accesos y el pago electrónico y la identificación de documentación personal.
Un Sistema de RFID suele basarse en varios componentes: Tags, Tag Readers, Front-Ends, Middleware, Back-Ends.

RFID – La tecnología y sus componentes

Esta tecnologia permite la transmisión de información a distancia gracias a la etiqueta RFID (TAG), la cual, al ser leída por el Lector de RFID transmite la información contenida en ella a la aplicación intermedia (Middleware) la cual, se encargara de procesarla, para finalmente tomar o depositar la información, en una base de datos, típicamente ubicada en el back-end **(Ver Figura 1)**.
Esa información transmitida por el Tag puede proveer información relacionada con la identificación del producto, la ubicación de la mismo, o bien otros datos específicos que puede contener el Tag, tales como color, precio, datos de compra, datos de vencimientos entre otros.

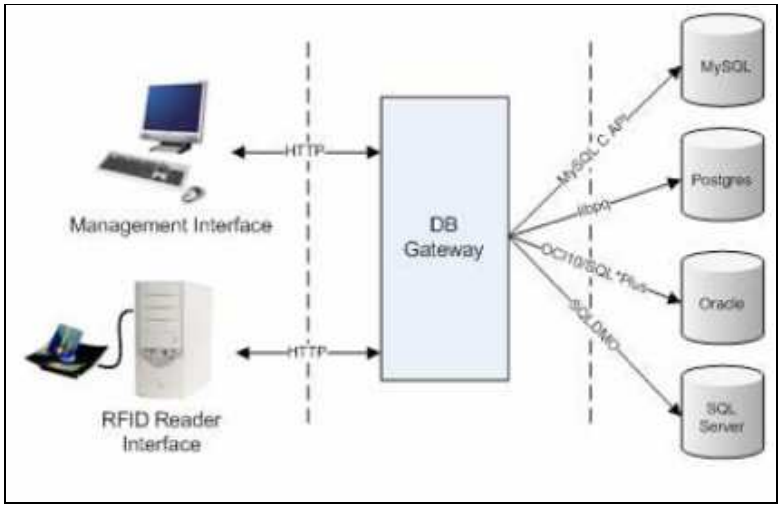

Figura 1

RFID – Tipos de Etiquetas

Existen distintos tipos de etiquetas (**Ver figura 2),** estas se diferencian entre si, por la frecuencia en la que operan, la cantidad de información que pueden contener, el tipo de funcionamiento y su durabilidad.

Figura 2

Existen tres tipos de etiquetas

Etiquetas Pasivas:

Estas operan en la Frecuencia de los 13,56 MHZ y no tienen fuente de energía interna, sino que la pequeña corriente inducida en la antena, brindada por la señal entrante de la frecuencia radial, produce la energía suficiente para que el circuito integrado, pueda encenderse y comenzar a transmitir (Backscatter).
Estas etiquetas son las de menos tamaño, por ende las más livianas y con una vida útil que puede ir hasta los 99 años.

Etiquetas Semipasivas:

Son muy similares a las etiquetas Pasivas, salvo por el agregado de una pequeña batería, esta batería mantiene una corriente continua en la memoria no volátil del circuito integrado, por lo cual la antena no debe preocuparse por recolectar la dicha corriente. La antena esta más optimizada a su función de transmisión de radio frecuencia lo cual hace que sea más rápida y robusta que los Tags Pasivos.

Etiquetas Activas:

Las etiquetas activas poseen su propia fuente de energía y son capaces de alcanzar mayores distancias (10 metros aproximadamente), a poseer una batería su vida útil de es de hasta 10 años, estos economizan el consumo de energía, trabajando en intervalos definidos de operación.

RFID – Tipos de Frecuencias

Existen distintas frecuencias en las que los sistemas de RFID, pueden operar, cada una de ellas representa distintos pro y contras en base a su aplicación.

Low Frequency (125 a 134.2 kHz y de 140 a 148.5 kHz)

Las etiquetas y lectores de baja frecuencia, se encuentran típicamente en tarjetas utilizadas para el control de acceso (Contact less Smartcards). La distancia en este caso es muy acotada y esta limitada a centímetros.

High Frequency (13.56 MHz)

Esta frecuencia opera en distancias de hasta un metro y se utiliza típicamente en la Identificacion de productos o personas (Pacientes, Convictos y otros)

Ultra-High Frequency (915 MHz, 433.92 MHz. o 315 MHz)

Dependiendo la tecnología pueden llegar a operar en una distancia de hasta 10 Metros o mas, típicamente esta tecnología es la que se utiliza para las cadenas de distribución y abastecimiento

Microwaves

Utilizadas para grandes distancias y mayor velocidad, operan en el rango que va de los **30 metros a los 100 metros**, un lugar donde se la utiliza suele ser por ejemplo los sistemas de pase automático de las autopistas.

Aplicaciones de RFID:

Hoy en día, existen numerosas aplicaciones para estas tecnologias **(Ver figura 3),** pero la mas creciente, es el que esta bajo el estándar EPC (Electronic Product Code), utilizada en la identificación de productos, la cual brinda una clave única para un producto o ballet, que permite detallar información sobre el mismo, en cualquier momento de la cadena de abastecimiento.

Figura 3

Adicionalmente, entre otras aplicaciones podemos mencionar las siguientes:

- Implementaciones ganaderas, para la identificación de ganado, su historial, sus progenitores, sus descendientes y su producción.

- Identificación en medicamentos de la fecha de vencimiento o bien la información sobre los efectos secundarios del mismo.
- Medios de pago electrónico (Mastercard Paypass)
- Identificación de pacientes
- Identificación de convictos
- Identificación de billetes de alta denominación
- Identificación de pasaportes
- Identificación de registros de conducir
- Identificación de entradas a eventos deportivos y espectáculos (Mundial Alemania 2006)
- Sistemas de Control de acceso
- Otras, muchas otras aplicaciones…

Podemos agregar a esto, que ya existen implementaciones de RFID mandatorias, por ejemplo entre algunas de las empresas y organizaciones que han emitido su mandato de implementación podemos mencionar al DOD (Departamento de Defensa de los Estados Unidos) y a Wal-Mart, este ultimo, obliga a todos sus Proveedores a colocar los Tags de RFID en todos los productos que tengan como destino final la góndola de Wal-Mart, impactando de esta manera en miles de compañías alrededor de todo el mundo. La fecha límite fue postergada en varias ocasiones, debido a que muchos vendedores tuvieron dificultades al implementar los sistemas de RFID.

RFID – Riesgos – Desde la invasión a la privacidad hasta SQL Injection

Tal como mencionamos, en nuestra introducción, nos encontramos nuevamente en la dificultad de buscar el equilibrio entre la funcionalidad de esta tecnología y los riesgos que esta puede introducir desde la óptica de la seguridad de la información. Es por esto que a continuación, haremos un breve análisis de los riesgos, desde dos ópticas bien diferenciadas, por un lado, el tema de la privacidad vs RFID y por otro, desde un punto de vista bien técnico algunas de las técnicas de ataques ya presentes contra algunas implementaciones de esta tecnología.

RFID - Privacidad

Los especialistas piensan en como transformar esta tecnología en la herramienta para poder establecer y entender el perfil del consumidor tan buscado y trataran de personalizar sus productos, sus mensajes y sus descuentos para acrecentar sus ventas, es por esto que ya, tanto en Estados Unidos, como así también en algunos lugares de Europa, se han levantado movimientos en contra de esta tecnologia, argumentando que la misma invade la privacidad de los cuidadanos, a decir verdad, esta tipo de cosas nos llevarían a preguntarnos por ejemplo:

- Y si comprase medicamentos RFID-tagged, como por ejemplo anti-depresivos, ¿quisiera que alguien que pase caminando a mi lado (o no tan a mi lado) lo sepa?
- Y si estoy en mi casa, y alguien pasa con su auto y un lector de RFID, ¿puede determinar todo lo que he comprado hasta el momento y establecer mis características de consumidor?

- Y con esta tecnología en mi ropa, ¿alguien puede determinar con precisión donde encontrarme?

Igualmente, y con sinceridad, si nosotros continuamente compramos con tarjetas de créditos, utilizamos tarjetas shopping para los descuentos, damos nuestros datos a cambio de una remera de Merchandising de una compañía, permitimos a las páginas Web, setear cookies en nuestras PCs… y siendo que todo esto permite potencialmente realizar un seguimiento sobre nosotros, hacer un estudio de nuestros consumos, poder ubicarnos en un determinado momento… ¿De que nos preocupamos entonces con el RFID?, en fin si bien, quizás este conflicto se demore un tiempo en llegar por estos lados, en el país del norte ya existe gran cantidad de legislación encargada de proteger la privacidad de los consumidores y otros aspectos relacionados con la utilización de la tecnologia RFID.
Entre algunas de las leyes existentes podemos mencionar las siguientes, a modo de ilustrar un poco mas la relevancia que se le da a esta problemática:

California - SB1834

Restringe la manera en que los comercios de California utilizan los Tags de RFID, en pos de que los tags de sus productos no sean utilizados para la identificación de un individuo.Junio 25, 2005.

Massachussets – HB 1447, SB 181

Requiere de la advertencia al usuario sobre la existencia de Etiquetas de RFID en los productos que adquiere, como así también, indicar el procedimiento para realizar la remoción del mismo, por otro lado limita la información de la etiqueta a aspectos de inventario solamente.

New Hampshire – HB 203

Requiere la comunicación escrita o verbal, por parte del comercio de que el producto que vende contiene una etiqueta.

Rhode Island – HB 5929

Prohíbe la utilización de RFID, para la identificación y el seguimiento de Estudiantes, empleados y clientes con fines que beneficien al negocio.

Utah – HB 185

Enmienda la ley de delitos informáticos para la inclusión de la tecnología RFID.

RFID - Riesgos Técnicos

Los sistemas RFID, se relacionan con varios procesos críticos, como el control de acceso físico, el seguimiento de productos, los sistemas de pago y otros más.
Si bien, como vimos, los riesgos mas publicitados de esta tecnología se relacionan con la privacidad, a continuación veremos algunos otros, que también deberían ser considerados.

- **Relay Attacks en tarjetas de proximidad**
- **Destruccion del TAG y Prevencion de Lectura**
- **RFID - SQL Injection**
- **RFID - Virus**
- **Algoritmos de Encripcion debiles**
- **Sniffing**
- **Spoofing**

RFID – Relay Attacks en Tarjetas de Proximidad

Un Sistema de Smartcard sin contacto (ISO 14443A), se comunica con otros dispositivos sin la necesidad de contacto físico, y lo hace a través de RFID, la tarjeta es pasiva y es activada por el lector, para realizar la transferencia de datos.
Las implementaciones de estos sistemas en Pasaportes, medios de pago electrónico y tarjetas de acceso (típicamente físico), esta incrementándose día a día y uno de los puntos mas importantes, en relaciona a esta tecnología y a la seguridad es por un lado su corto rango de operación (10 centímetros aproximadamente) y por otro, el hecho de que la comunicación entre un extremo y el otro va cifrada (**Ver Figura 4).**

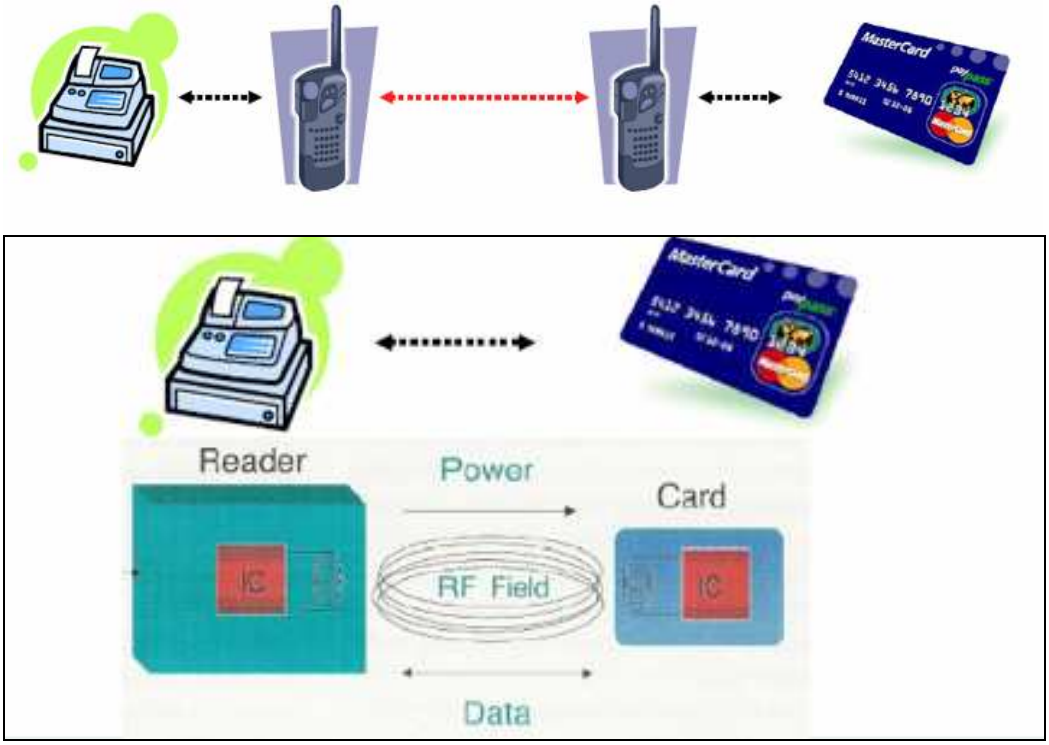

Figura 4

Lo que se ha logrado en un estudio llevado a la cabo por la Universidad de Tel Aviv (Israel), es que creando un lector falso (Leech) y una tarjeta falsa (Ghost), uno podría impersonar un usuario o una transacción, prácticamente sin limites de distancia.
El concepto de esta ataque nace en base a un ataque basado en memory cards, las cuales no tienen la capacidad de procesar la información y almacenan la misma en una banda magnética, que es leída y procesada por el lector, mediante un **POST Interceptor** y gracias a la utilización de algoritmos de encripción débiles **"Static**

Data Authentication" (SDA), la información de la tarjeta y el pin era almacenado en el POST Interceptor para una posterior utilización fraudulenta.
Es en base a lo anterior, a la creciente implementación de smart cards, y a sus variados usos es que los atacantes optan por el **Ataque de Relay** y utilizan la información en **Real Time.**

Pongamos un ejemplo, un usuario de una organización, que cuente con una smartcard contactless, para el acceso físico a un area restringida, típicamente podría llevar su tarjeta colgando en la cintura como habitualmente se hace, este podría ser sorprendido por un potencial atacante, en un recinto donde exista poco espacio y gran cantidad de gente (Ascensor, Subterraneo), alli el potencial atacante podría acercarse lo suficiente, como para lograr activar el smartcard del usuario, mediante un Smartphone. Modificado para actuar y emular a un lector (Leech), una vez logrado esto, el atacante transmitiría en tiempo real via GRPS, los datos a otros dispositivo similar, en este caso, la tarjeta falsa (Ghost), la cual por ultimo y estando cerca del lector orginal, transmitirá los datos recibidos y brindara acceso al intruso al área restringida 9Ver Figura 5). Es importante destacar, que en la mayoria de este tipo de ataques, la distancia no importa, como asi tampoco el cifrada de datos, ya que en la mayoría de los casos este no detecta el MITM (Man in The Middle).

RFID – Destruccion del TAG

Este tipo de ataque, requiere poco conocimiento técnico para ser realizado, la idea del mismo es destruir el tag pasivo colocado en un producto, de manera que este no pueda ser identificado, ni tampoco se permita realizar su seguimiento, típicamente este tipo de acciones esta motivada en defensa de la privacidad de los consumidores. Técnicamente, esto podría llevarse adelante cortando la antena o bien friendo el tag en un microondas, pero de seguro que el producto también resultaría destruido, es por eso que se creo el **“RFID-Zapper” (Figura 5),** el cual utiliza el método del microondas, pero en una dosis menor, evitando así la destrucción del producto, mediante la generación de un campo electromagnético fuerte, que desactivara el chip para siempre.

Figura 5

RFID – Prevención de Lectura

La idea de esto, no es desactivar el tag pasivo, sino la de prevenir su lectura, el fin de esta practica es la protección de la privacidad, o bien, como hemos visto anteriormente también podrían prevenir ataques de Relay contra las tarjetas de proximidad (imagínense cuan cerca podría estar alguien de su tarjeta en un ascensor) Existen dos materiales que impiden la lectura de RFID el metal y el agua, pero mucho mas cómodo es darle un nuevo uso al famoso **SILVER TAPE (Figura 6)**

Figura 6

RFID – Spoofing

Un atacante podría escribir, en un TAG en blanco, datos validos que impersonen a un producto, de hecho, ya se realizaron dos ataques (en ambiente controlado) uno se baso en sniffear, descifrar y spoofear un dispositivo RFID utilizado para cargar gasolina y el otro, se utilizo para desactivar un sistema de alarmas para automóviles basado en la inmovilización del mismo.

RFID – SQL Injection

Si bien se trata de un ataque ya conocido y muy utilizado hoy en dia, esta nueva tecnología no queda fuera del alcance del mismo, este ataque se basa en la inyección a la base de datos (Back-End) de sentencias SQL especialmente creadas, que podrían permitir acceder a información no autorizada, realizar modificaciones o borrar una tabla, entre otras cosas.
En base a la estructura de una implementación RFID **(Figura 1),** esto es posible por falta de controles de seguridad adecuados en el middleware y en la base de datos, en este tipo de ataques, el potencial intruso debería grabar, previamente, en un tag en blanco, del tipo activo, una sentencia de SQL previamente armada, con el fin de que cuando este TAG sea leído por el lector, este pase los datos al middleware y posteriormente esta sentencia se ejecute en la base de datos.
Otro aspecto a tener en cuenta es la cantidad de datos que pueden entrar en un tag, esto no es un limitante ya que con pocas cantidades de información se puede causar un gran impacto.
De la misma manera que se inyecta esta sentencia, se han realizado en ambiente de laboratorios, pruebas en las cuales se logro con éxito crear y replicar el primer worm que utiliza la tecnología RFID.
Por ultimo cabe aclarar que este tipo de ataques, no tiene relación directa con la tecnología RFID en si misma, sino que al igual que en las aplicaciones Web y similares, la falta de validación de entrada de datos y la falta de metodologías seguras de programación hacen que esto sea posible.

Conclusión:

Como hemos podido leer, a lo largo de este articulo, la incorporación de nuevas tecnologías, en lo procesos del negocio, no solo debe contra con una análisis funcional y económico, sino también que la seguridad debe ser uno de los puntos a tener muy en cuenta.

La creatividad, que tienen este tipo de ataques hacen que los controles de seguridad existentes puedan no tener sentido, es por eso que como profesionales de seguridad tenemos que desarrollar también el sentido de la percepción y la creatividad.

Referencias y Lecturas Complementarias

- Fundamentals and Applications in Contactless Smartcards & Identification
  Klaus Finkenzeller
- Python library for exploring RFID devices
  http://rfidiot.org
- Practical Relay Attacks Against ISO 14443 Proximity Cards
  Gerhard Hancke & Dr Markus Kuhn
- Low Cost Attacks on Tamper Resistant Devices
  Ross Anderson & Markus Kuhn
- A New Approach to Hardware Security Analysis
  in Semiconductors
  Sergi Skorobogatov
- RFID Essentials
  O'Reilly
- Texas Instruments DST attack
  http://www.jhu.edu/news_info/news/home05/jan05/rfid.html
- RFID relay attacks
  http://www.cl.cam.ac.uk/~gh275/relay.pdf
- RFID virus
  http://www.rfidvirus.org/papers/percom.06.pdf
- Smartdust
  http://en.wikipedia.org/wiki/smartdust