CAPÍTULO 7. PRIVACIDAD Y SEGURIDAD EN RFID

La tecnología RFID plantea riesgos que se deben considerar al diseñar sistemas en los que se utilicen etiquetas RFID, principalmente la privacidad y seguridad de esta tecnología. Se debe tener una visión de los factores de riegos para minimizarlos y establecer estándares internacionales, y poder brindar al usuario final las herramientas y seguridad para poder resguardar su privacidad y seguridad.

Existen asociaciones civiles y juristas que están en contra de esta tecnología, principalmente por la invasión de la privacidad y su afectación a los derechos humanos. A continuación se presentan algunos casos y se plantean criterios para poder evitar el mal uso de esta tecnología.[GON08]

7.1 Privacidad y seguridad

La utilización se circuitos RFID ha creado gran polémica, incluyendo el rechazo de productos por su potencial invasión de la privacidad. Existen varias razones por las que la identificación por radiofrecuencia resulta preocupante en cuanto a la privacidad:

- El producto con la etiqueta RFID logra ser leída a cierta distancia son conocimiento por parte del usuario.
- Es posible conocer la identidad del usuario del producto, cuando se crean etiquetas RFID personalizadas.
- Para el usuario final de los productos, la etiqueta puede pasar inadvertida y sería imposible removerla.
- Lectura no autorizada de la información que almacena una etiqueta con el fin de duplicarla o modificarla.

Debido a las razones anteriores, existen soluciones técnicas para controlar las utilizaciones indeseadas de los sistemas RFID, como son los procedimientos de cifrado y autenticación.

El cifrado se utiliza para asegurar que la información solo pueda ser entendida por los usuarios de la aplicación y evitar lecturas indeseadas. La autenticación se utiliza para que únicamente el personal autorizado pueda acceder a dicha información, pudiendo leer y escribir información.

En un sistema de comunicaciones existen dos tipos de ataques, los pasivos y los activos. Los ataques pasivos son cuando un intruso viola la confidencialidad de los mensajes de forma oculta, monitoreando la información que se transmite por el sistema de comunicación. Los ataques activos se realizan cuando el intruso accesa al sistema, monitorea la información, controla su flujo y es capaz de modificar la información, alterando la integridad de los mensajes.[DOM06].

Para confrontar estos ataques se ha aplicado servicios de seguridad que tienen como finalidad reconocer y autentificar a los usuarios, verificar la identidad de los usuarios, para proveer la información del sistema sin que esté presente violaciones o mal uso.[DOM06]

La privacidad es un punto muy importante en un sistema RFID, identificar exhaustivamente todo lo que nos rodea puede afectar a la privacidad del usurario de un sistema de RFID. Es por ello que se implementa un mecanismo de contraseña y con el estándar EPCGlobal, el usuario puede tener mayor privacidad, en las etiquetas pasivas

podemos tener mayor control de privacidad, ya que por su corto alcance es controlable sin filtraciones.

La EPCglobal formó una comisión encarga de buscar el equilibrio entre los aspectos de privacidad y los beneficios de la implantación de la tecnología RFID. Uno de los resultados de esta comisión fueron unas directrices para la protección de la privacidad de los consumidores. En México GS1, es la empresa responsable de brindar, los lineamientos y estándares regidos internacionalmente por EPCglobal, para ofrecer una mayor privacidad gs1 México ha creado un código seriado llamado: "Código Seriado de unidad de Embarque (SSCC), el cual es único y nos permite tener mayor privacidad, está compuesto por 18 dígitos numéricos estructurado de la siguiente forma mostrado en la figura 43.

Figura 43. Ejemplo de SSCC [URL15]

A: Identificador de aplicación

B: Digito de extensión (Libre y asignado por la empresa)

C: Código de la empresa

D: Número de serie de hasta 9 dígitos (en función del código de empresa) asignado por la empresa que codifica de una única cada producto.

E: Digito verificador.

Otra solución para salvaguardar la privacidad el usuario, es desactivando la etiqueta después de la verificación de la venta también llamado "kill tag",, con esto podemos asegurar el producto una vez que haya llegado a su destino final, puesto que se ha desactivado la etiqueta y ya no podrá ser leída, y conjuntamente es necesario colocar las etiquetas en el empaque y no en los productos. Para la privacidad individual, cabe menciona que cada etiqueta posee un bit que indica si es una etiqueta pública o privada. Se recomienda la reducción de la información contenida en las etiquetas, grabando únicamente el código de identificador de producto. El resto de la información se almacenara asociada a este código en un servidor central, minimizando así el riesgo de rescritura de las etiquetas. Y por último, una solución no técnica es colocar el producto que contiene la etiqueta un funda de metal de modo que esta se convierta en una jaula se Faraday para el aislamiento de lecturas por parte de un lector. [URL17].

De este modo, las directrices para proteger la privacidad son:

- Todo consumidor debe ser informado y advertido de la presencia de etiquetas RFID en los productos.
- Se debe informar al consumidor la utilización de RFID en un producto, y elegir si desean desactivar o eliminar las etiquetas.
- Los consumidores deben tener la posibilidad de informarse correctamente sobre el uso de las etiquetas RFID y sus aplicaciones.
- Las empresas deben almacenar registros de uso, mantenimiento y protección de la información obtenida con esta tecnología y deben mejorar la seguridad y privacidad de los datos.

7.2 Encriptación y Autentificación

Existe una alternativa altamente eficiente en cuando a la privacidad se refiere, utilizando algoritmos de autentificación de usuarios y cifrado de la información, es posible crear una capa de seguridad robusta la cual bloquee cualquier intento de intrusión en el sistema, se han creado este tipo de capas de seguridad, logrando incorporarlas a cualquier objeto con un costo de fabricación bajo, limitados a los recursos de hardware de las etiquetas. Este tipo de capas de seguridad realizan funciones de criptografía usando llaves para el proceso de cifrado de la información. [DOM06].

En cualquier sistema de comunicaciones es importante y primordial mantener la integridad, la privacidad y la confidencialidad de la información que se va a trasmitir, por lo tanto es necesario que los mecanismos de autentificación de usuarios prueben la verdadera identidad de quien aclaman ser, a fin de establecer confianza entre la comunicación y los demás elementos. En los sistemas RFID es necesario que tanto el lector como las etiquetas se identifiquen y autentifiquen, ya que un intruso puede recabar la información con un lector de etiquetas o una etiqueta intrusa puede obtener acceso a sistemas restringidos y dar una información falsa. [DOM06].

Los mecanismos de cifrado ocultan los mensajes a elementos ajenos al sistema donde se transmite la información. Por lo tanto se requiere forzosamente del cifrado de los datos para el sistema RFID, debido a que los datos se trasmiten en el aire, el cual es un método de acceso libre para cualquier dispositivo que intente leer la etiqueta de forma ilegal.[DOM06]

Algunos sistemas high-end de RFID (basados en ISO 14443) pueden encriptar y autentificar el tráfico de los datos con protocolos propietarios. Desde el intercambio de datos apartado de los identificadores no juega un papel importante en los sistemas de RFID, la mensajería segura no se mira usualmente como cuestión clave. El encriptado de los bloques de la memoria puede ser revisado en la capa de aplicación y es transparente para la etiqueta de RFID. El identificador Único es generalmente inalterable y muchos transponders de RFID permiten una escritura permanente de los bloques de la memoria. Esto puede asegurar integridad de datos pero, no la autentificación del mensaje.

Los riesgos de seguridad y privacidad inducidos por los identificadores de etiquetas RFID no protegidas dan razones para un número de contribuciones y protocolos. Así los recursos construidos con etiquetas de bajo costo tienen que ser consideradas. [WEI03]