Clasificación de las amenazas a la seguridad en sistemas RFID - EPC Gen2

Joan Melià-Seguí*, Joaquin Garcia-Alfaro*†, Jordi Herrera-Joancomartí‡

* Universitat Oberta de Catalunya, Rambla de Poblenou 156, 08018, Barcelona
† Institut Telecom, Telecom Bretagne, 35576, Cesson-Sevigne, France
‡ Universitat Autònoma de Barcelona, Edifici Q, 08193, Bellaterra

***Abstract*—La tecnología EPC (Electronic Product Code) está basada en la utilización de radio-etiquetas de bajo coste. El uso de estas radio-etiquetas proporciona una gran flexibilidad para la identificación de objetos en movimiento en cadenas de suministro y de producción industrial. Sin embargo, la carencia de mecanismos específicos de seguridad que garanticen propiedades tan indispensables como autenticación o confidencialidad no se recogen actualmente en las especificaciones del estándar EPC. Por ello, es difícil hoy en día hablar del uso de esta tecnología sin que nos venga a la mente problemas de seguridad y de posibles violaciones a la privacidad de sus usuarios. Presentamos en este artículo una vista rápida a la familia de amenazas a las que se enfrenta la tecnología EPC.**

***Index Terms*—RFID, EPC Gen2, modelo de adversario, seguridad, privacidad.**

I. Introducción

La tecnología EPC (del inglés, *Electronic Product Code*), se basa en la utilización de dispositivos RFID (*Radio Frequency IDentification*) [1]. Esta tecnología está destinada a ser la sucesora de los hoy omnipresentes códigos de barras. Diseñada en los laboratorios Auto-ID del MIT (*Massachusetts Institute of Technology*) y más adelante desarrollada por el consorcio EPCglobal Inc., la tecnología EPC representa el elemento clave de una arquitectura distribuida conocida como EPCglobal Network. Los elementos principales de un sistema RFID son las etiquetas electrónicas, los lectores y los sistemas de información (servidores y bases de datos). El objetivo de esta arquitectura es la identificación automática de objetos en movimiento en cadenas de suministro y de producción industrial.

Las etiquetas electrónicas del sistema EPC, cuyas características principales se detallan en la Tabla I, son pasivas (se alimentan del campo eléctrico generado por el lector, debido a la ausencia de batería en la etiqueta). Funcionan en la banda *Ultra High Frequency* (UHF), siendo en Europa entre los 865 y 868 MHz. El rango de lectura entre lector y etiqueta se sitúa alrededor de los 5 metros. Su funcionamiento responde al modelo de una máquina de estados. En un sistema RFID de bajo coste como el EPC Gen2 las etiquetas electrónicas tienen una capacidad muy limitada, permitiendo reducir su coste por debajo de los 10 céntimos [3], pero a su vez, con severas limitaciones para gestionar las amenazas de seguridad.

Como sucede en otras tecnologías emergentes, la falta de seguridad y las amenazas contra los componentes de la arquitectura pueden comportar múltiples inconvenientes a sus usuarios (por ejemplo, difusión de datos privados y pérdida de intimidad). El presente artículo se centra en las amenazas a la integridad de las comunicaciones entre los lectores y las etiquetas electrónicas, debido a la limitación de las etiquetas en el sistema EPC Gen2, y al uso de un canal inalámbrico inseguro que no garantiza la autenticidad de las entidades participantes en el sistema [4].

TABLE I
Principales características de la tecnología EPC Gen2

Identificador	96 bits
Rango de lectura	$\sim$ 5 m
Consumo etiquetas	$\sim$ 10 μW
Frecuencia	865-868 MHz (UHF)
Ratio Tx etiquetas	40 - 640 kbps
Ratio Rx etiquetas	26.7 - 128 kbps
Identificaciones por segundo	$\sim$ 200

El análisis de las vulnerabilidades relativas a la comunicación entre el lector y el sistema de información no se considera en este artículo, puesto que estos equipos tienen la potencia suficiente para ejecutar los mecanismos de cifrado necesarios, además de utilizar canales de comunicación más seguros como interfaces cableadas de red local.

De este modo para el resto del artículo nos referimos a la comunicación entre etiquetas y lectores EPC por el canal de radiofrecuencia como sistema EPC Gen2 , en donde se encuentran la mayoría de las vulnerabilidades de seguridad.

El modelo de comunicación en el sistema EPC Gen2 es común al del resto de sistemas RFID de bajo coste, en donde el lector inicia la comunicación (ITF *interrogator talks first*, del inglés) ya que la etiqueta es pasiva y necesita de la energía del lector para responder. Concretamente existen tres etapas en la comunicación entre un lector y etiqueta EPC Gen2. En las etapas de *selección* e *inventariado*, el lector inicia la comunicación lanzando una petición de identificación (*request*). Las etiquetas presentes en el rango de lectura responden (*response*) con un identificador provisional. En el momento en que el lector responde al identificador provisional (*acknowledge*), las etiquetas devuelven el identificador completo de 96 bits [1]. En este punto si el lector quiere acceder a contenidos de la memoria

reservada, o modificar partes de la memoria de la etiqueta, se entra en la etapa de *acceso*. La Sección II profundiza en esta etapa, en que la comunicación lector-etiqueta se cifra para no revelar datos sensibles del sistema, mientras que el canal etiqueta-lector se transmite sin cifrar.

Como se ha comentado previamente, la característica principal del sistema EPC Gen2 es la simplicidad y bajo coste de las etiquetas electrónicas. Este punto es determinante para la inclusión de posibles mejoras de seguridad que den respuesta a las amenazas que se detallarán en la Sección III, debido a las vulnerabilidades relacionadas con la restricción de la capacidad de computación, memoria y energía, presentes en el sistema EPC Gen2 [5].

En este artículo, presentamos una visión general sobre la familia de amenazas contra la tecnología EPC. Describimos el modelo de adversario del sistema EPC Gen2, las principales vulnerabilidades existentes en la tecnología y los puntos que podrían ser explotados por un atacante para hacer efectivas las amenazas. El resto del artículo se organiza de la siguiente manera. La sección II presenta el modelo de adversario que supondremos durante la presentación de las vulnerabilidades, y las peculiaridades de la tecnología EPC que hacen posible suponer dicho modelo. La sección III describe una presentación general sobre el conjunto de amenazas seleccionado para nuestro estudio. La sección IV cierra el artículo con un conjunto de conclusiones.

II. Mecanismos de seguridad en EPC Gen2

Todo sistema de comunicaciones padece amenazas relacionadas con la seguridad de la información gestionada por el sistema. Por este motivo es importante determinar la naturaleza de dichas amenazas e identificar los posibles adversarios, para poder analizar las medidas de seguridad a adoptar y en qué circunstancias deben ser implementadas.

Las amenazas relativas a la seguridad y privacidad de los datos transmitidos en un sistema EPC Gen2, vienen dadas por el valor intrínseco del objeto etiquetado, o del valor derivado de correlacionar la información de la etiqueta con la identidad del individuo que está identificando [6].

A. Modelo de adversario: definiciones

Para evaluar los principales problemas de seguridad que pueden afectar un sistema EPC Gen2, se debe definir un modelo simple contemplando las características de comunicación del sistema EPC Gen2 de RFID de bajo coste, y los posibles adversarios, así como las capacidades y objetivos de ambos. En primer lugar se listan las principales entidades del sistema EPC Gen2 participantes en el modelo, así como una descripción de sus características. Para un análisis más amplio de modelos de adversario para RFID de bajo coste puede consultarse [7].

- *Lector autorizado*: El que estando registrado en el sistema dispone de los mecanismos necesarios para acceder a los contenidos restringidos de la memoria. Por tanto el lector autorizado puede leer y escribir en las etiquetas electrónicas.
- *Etiqueta legítima*: Una etiqueta electrónica presente en la base de datos del sistema, y que ha sido previamente identificada por un lector autorizado.
- *Lector no autorizado*: El que no está registrado en el sistema, pero tiene acceso al rango de lectura del sistema EPC Gen2.
- *Etiqueta ilegítima*: Etiqueta fraudulenta que accede al rango de lectura de un sistema EPC. Cuando la identificación de una etiqueta fraudulenta ha sido copiada de una etiqueta legítima, se conoce como etiqueta clonada.

A continuación, se definen las características del canal de comunicaciones.

- *Canal lector-etiqueta*: Trasmisión de lector a etiqueta. El lector transmite a una potencia muy superior a la de la etiqueta, ya que esa energía debe ser suficiente para alimentar la respuesta de la etiqueta. Por este motivo, el canal lector-etiqueta puede ser capturado a centenares de metros del punto de transmisión [2].
- *Canal etiqueta-lector*: Transmisión de etiqueta a lector. Como se ha citado en la Introducción, las etiquetas electrónicas del sistema EPC Gen2 son pasivas, por lo que no disponen de una fuente de energía en la propia etiqueta. La transmisión se realiza mediante la señal proveniente del lector reflejado por la antena de la etiqueta, por lo que su alcance se limita a unos 5 metros.

Finalmente, se definen los dos modos de interacción básicos entre lector y etiqueta, la *identificación* y el *acceso*.

- *Identificación*: La etiqueta electrónica legitima o ilegítima transmite (en claro) los 96 bits de su código EPC de identificación tras completar los estados de selección e inventariado.
- *Acceso*: Una vez completada la identificación de la etiqueta electrónica, un lector (autorizado o no autorizado) se dispone a activar los mecanismos de seguridad para poder acceder a todo el contenido de la memoria de la etiqueta para leer o escribir en ella (la Tabla II detalla la esctructura lógica de la memoria). Los peticiones de *acceso* a la memoria de una etiqueta EPC Gen2 pueden ser *read*, *write*, *kill*, *lock*, *access*, *blockwrite*, *blockerase* y *block permalock* [1].

Una vez definidas las características básicas del sistema EPC Gen2, pasamos a describir los posibles tipos de adversarios del sistema. Para el modelo de adversario del sistema EPC Gen2 se supone que las etiquetas y los lectores no autorizados se encuentran, salvo que se indique lo contrario, a una distancia superior a la del rango de lectura del canal *etiqueta-lector*. El motivo por el que este modelo prioriza las amenazas sobre el canal *lector-etiqueta*, es debido a la sencillez de capturar la información de este canal mediante cualquier lector compatible EPC Gen2 a distancias de centenares de metros. El canal *etiqueta-lector*, en cambio, necesita de equipos especiales con antenas muy directivas, o bien situarse dentro del rango de lectura del canal (alrededor de 5 metros).

TABLE II
MAPA LÓGICO DE LA MEMORIA DE LAS ETIQUETAS EPC GEN2

User:	Opcional
TID:	TID [15:0]
	TID [31:16]
EPC:	XPC_W1 [15:0]
	EPC [15:0]
	⋮
	EPC [95:79]
	PC [15:0]
	CRC [15:0]
Reserved:	Access Password [15:0]
	Access Password [31:16]
	Kill Password [15:0]
	Kill Password [31:16]

- *Vulnerabilidad*: Es la propiedad del sistema que un adversario trata de atacar para conseguir el objetivo de la amenaza.
- *Amenaza*: Es el objetivo del adversario para violar una vulnerabilidad relativa a la seguridad del sistema.
- *Adversario pasivo*: Es la entidad que trata de explotar una vulnerabilidad en el sistema para ejecutar la amenaza [8]. Se limita a capturar información en el rango de lectura, sin dar evidencias de su presencia en el sistema.
- *Adversario activo*: Igual que el adversario pasivo, pero puede transmitir y recibir información en el rango de lectura. En caso de poder situarse en el rango del canal *etiqueta-lector*, también podría afectar el contenido de la memoria de las etiquetas.

B. Seguridad del sistema EPC Gen2

El protocolo de comunicación del sistema EPC Gen2 se basa en un sistema de petición-respuesta (*request-response*) entre lector y etiquetas electrónicas en tres etapas diferentes (selección, inventariado y acceso), en el que la etiqueta pasa por diferentes estados. La integridad de los mensajes se comprueba mediante un código de redundancia cíclica (CRC) de 16 bits. La *identificación* de una etiqueta se realiza de manera automática por cualquier lector compatible EPC Gen2, sin ningún tipo de autenticación segura por ambas partes. Es decir, cualquier lector puede identificar etiquetas en el rango del canal *etiqueta-lector*.

Por contra, el protocolo de comunicación para EPC Gen2 sí incluye mecanismos básicos de seguridad para la etapa de *acceso* a las etiquetas electrónicas. El estándar EPC Gen2 incluye en sus especificaciones una contraseña de 32 bits para el acceso a la memoria de la etiqueta electrónica. Además el estándar incluye una contraseña de 32 bits para la opción *kill*, que en caso de ser activada permite desactivar el funcionamiento de la etiqueta de forma permanente, o bien desbloquear determinadas partes de la memoria de la etiqueta electrónica previamente bloqueadas, en función de la codificación del comando como *kill* o como *recommission* [1].

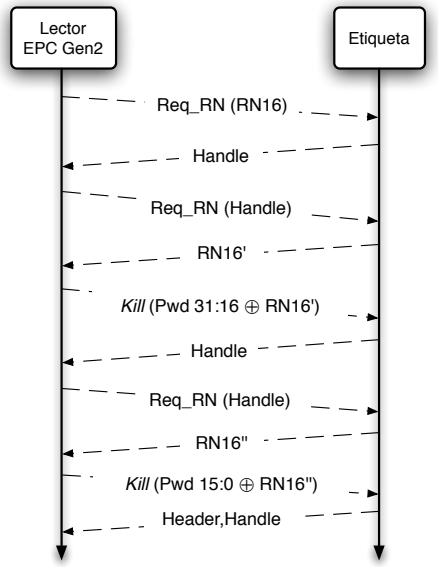

Fig. 1. Protocolo para ejecutar la opción *kill* en EPC Gen2.

Las contraseñas de acceso y *kill* se almacenan en la memoria reservada de la etiqueta electrónica (la Tabla II contiene las diferentes áreas de memoria de una etiqueta EPC Gen2).

Adicionalmente, para evitar revelar información sensible en el canal *lector-etiqueta* (por ejemplo contraseñas o nuevos identificadores) que pudiera ser capturada por un lector no autorizado, las etiquetas electrónicas EPC Gen2 incluyen un generador de números pseudo-aleatorios (PRNG) para cifrar la información transmitida en ese canal. De este modo, cuando el lector requiere el *acceso* a la etiqueta, ésta transmite en plano claves de 16 bits al lector para cifrar el contenido a transmitir mediante una operación de OR-exclusiva a nivel de bit.

Por ejemplo para ejecutar la opción *kill* a una etiqueta EPC Gen2, el lector debe *identificar* previamente la etiqueta. Una vez la etiqueta ha enviado los 96 bits de su código EPC de identificación, el lector procede a la fase de *acceso* (Fig. 1). Para ello el lector solicita a la etiqueta una clave de 16 bits (RN16) como llave de la sesión de *acceso*. Cuando la etiqueta le proporciona el RN16 (representado como *Handle*), el lector solicita una nueva clave (RN16') para iniciar el cifrado de la contraseña de *kill*. Esta operación se repite para las dos partes de la contraseña de *kill* (Pwd [31:16] y Pwd [15:0]) con una nueva clave RN16". Para confirmar la finalización de la operación, la etiqueta transmite un último mensaje formado por una cabecera y el código *Handle*.

III. PRINCIPALES PROBLEMAS DE SEGURIDAD

Tras definir el modelo de adversario para los sistemas EPC Gen2, se pueden destacar las siguientes vulnerabilidades, con la correspondiente amenaza de ser explotadas por parte de un adversario [6]:

- El canal etiqueta-lector es un canal inseguro.
- Cualquier lector compatible con EPC Gen2 puede acceder a la *identificación* y *acceso* de las etiquetas en el rango del canal lector-etiqueta.
- El diseño de las etiquetas está optimizado para reducir su coste, por lo que su capacidad es muy reducida y carece de mecanismos de seguridad y autenticación fiables.

Aunque el contenido de las transmisiones entre lector y etiqueta en el modo de acceso esté cifrado, el hecho de que las claves de cifrado circulen en claro por el canal *lector-etiqueta* representa una vulnerabilidad con riesgo de ser atacada por un adversario.

Por ejemplo el uso de PRNGs con malas propiedades estadísticas, o con cierto grado de predictabilidad, puede suponer riesgos graves en la confidencialidad de las comunicaciones, como se demuestra en [9]. Un lector no autorizado puede acceder el canal *lector-etiqueta* de lectores autorizados y etiquetas legítimas. De este modo un adversario pasivo podría analizar la predictabilidad de las secuencias pseudo-aleatorias generadas en una etapa de acceso. Si el adversario puede obtener información sobre la generación de las secuencias pseudo-aleatorias, le será suficiente con realizar una operación de OR-exclusiva entre la transmisión cifrada y las secuencias predichas, para descifrar el mensaje. De este modo un lector no autorizado en el rango del canal *lector-etiqueta*, obtendría acceso a las zonas de memoria reservadas de la etiqueta tales como contraseñas de acceso y *kill*.

En los siguientes subapartados se detallan las cuatro principales amenazas a la seguridad en un sistema EPC Gen2.

A. Escuchas fraudulentas

Dado que el modelo de comunicación para un sistema RFID pasivo como EPC Gen2 contempla potencias de emisión del lector mucho mayores que la potencia de emisión de las etiquetas, las escuchas fraudulentas se definen como la presencia de lectores no autorizados con acceso a la comunicación del canal *lector-etiqueta*. Esto no excluye la presencia de lectores no autorizados en el canal *etiqueta-lector*, pero es menos probable.

El canal de comunicación entre lectores y etiquetas es fácilmente accesible dada la inseguridad del canal inalámbrico, con lo que la confidencialidad de los datos transmitidos es fácilmente vulnerable. Como se ha visto al inicio de esta Sección, un adversario puede aprovechar la vulnerabilidad de un PRNG predecible para obtener la información almacenada en la memoria reservada de la etiqueta.

Relacionados con las escuchas fraudulentas existen los ataques de *eavesdropping* o análisis, en los que un lector no autorizado podría interceptar la comunicación y analizarla para tratar de descifrar las contraseñas de *acceso* y *kill*.

Por ejemplo un adversario situado en el rango de lectura del canal *lector-etiqueta* de un centro de fabricación textil, en donde se identifica cada producto con una etiqueta EPC, podría recoger información como el número de unidades fabricadas, el modelo o el valor de la producción en cada momento. Si en cambio las etiquetas se utilizan para la identificación de personas, amenazas a la privacidad personal como seguimiento (en inglés, *tracking*) y análisis de perfiles y preferencias (en inglés, *profiling*/*clustering*) están incluidas en esta categoría [10].

B. Suplantación de identidades

Debido al bajo coste de las etiquetas electrónicas, la tecnología EPC Gen2 se utiliza para la identificación a nivel de objetos o personas [2]. Su diseño está centrado en la simplicidad de sus operaciones, lo que permite *identificar* un gran número de etiquetas de forma simultánea (Tabla I). Puesto que el sistema EPC no dispone de mecanismos de autenticación, el adversario no encontraría ninguna dificultad para conseguir la misma información que podría obtener un usuario autorizado dentro del sistema.

Un lector no autorizado podría suplantar (*spoofing*) un lector autorizado, obteniendo la identificación de etiquetas legítimas. Esta información se podría reproducir en etiquetas ilegítimas o fraudulentas por ejemplo mediante un ataque de *skimming*, lo que significaría un caso de clonación de etiquetas (*cloning*) que podría usarse para falsificación de productos (*counterfeiting*). Un lector autorizado no podría discernir entre una etiqueta legítima y una etiqueta clonada al no existir mecanismos de autenticación para la identificación de etiquetas. Del mismo modo, en un sistema de acceso personal basado en la tecnología EPC Gen2, se podría suplantar la identidad de una persona copiando la identificación de su etiqueta a una etiqueta ilegitima, obteniendo los privilegios de acceso de la persona suplantada.

En el caso que existiera la posibilidad de acceder al rango de lectura del canal *etiqueta-lector*, un lector no autorizado podría realizar ataques activos como *replay* o *scanning* para obtener información de las etiquetas directamente.

C. Divulgación de información

El riesgo derivado de la suplantación de identidad en un sistema EPC Gen2 va más allá de la posible falsificación o clonación de etiquetas electrónicas. Como se ha comentado al inicio de la Sección II, las posibles amenazas a la seguridad y privacidad de un sistema de información están directamente relacionadas con el valor económico de la información que pueda obtenerse.

Esta amenaza es especialmente relevante debido a que el código EPC puede revelar información importante como la marca, el modelo o el precio del producto, así como las estrategias de producción o distribución de la empresa en cuestión. De este modo el adversario puede obtener un beneficio económico de la venta de esta información con fines de espionaje industrial [8].

Divulgar secretos industriales es una actividad claramente ilegal, por lo que el adversario no tomará riesgos innecesarios como acceder a los recintos de producción o distribución. En cambio el adversario puede aprovechar el largo alcance del canal de comunicación *lector-etiqueta* para obtener la información deseada desde centenares de metros [4].

En el plano personal esta amenaza es también relevante, ya que supone una invasión de la privacidad de los usuarios del sistema. Podemos imaginar un escenario en el que la actividad de un grupo de usuarios sea registrada por un adversario con un lector no autorizado, para luego obtener beneficio de esa información.

D. Denegación de servicio

La denegación de servicio (*DoS*) es una amenaza que tiene por objetivo limitar o anular la funcionalidad de un sistema de información. En el caso del sistema EPC Gen2, la denegación de servicio significaría dejar inoperativo el canal de comunicación (tanto de lector a etiqueta como viceversa) haciendo inviable el intercambio de información.

Una denegación de servicio podría realizarse de diversos modos tomando como referencia el modelo especificado en la Sección II. Por ejemplo, un emisor de radio-frecuencia emitiendo señal de ruido (ataque *jamming*) entre las frecuencias 865 y 868 MHz en el rango de lectura del canal *lector-etiqueta*, ocuparía los canales de comunicación del sistema EPC Gen2, impidiendo que los lectores autorizados iniciaran la selección e identificación de las etiquetas electrónicas [1]. Sin ir más lejos, un lector no autorizado compatible EPC Gen2 en el rango de lectura del canal *lector-etiqueta* emitiendo constantemente peticiones de identificación, reduciría considerablemente la eficiencia de lectura de los lectores autorizados, retrasando los procesos de inventariado del sistema atacado.

En el caso de tener acceso al canal *etiqueta-lector*, y haciendo uso de las vulnerabilidades especificadas al inicio de la Sección III se podría realizar un ataque del tipo *tampering*. Un lector no autorizado podría hacer uso del comando *kill* eliminando toda funcionalidad de cualquier etiqueta que entrara en su campo de lectura.

IV. Conclusión

Los sistemas EPC Gen2 representan una de las tecnologías más pervasivas en el ámbito de las tecnologías de la información. La característica principal de la tecnología EPC Gen2 es el reducido precio de las etiquetas electrónicas (previsto por debajo de los 10 céntimos) lo que significa un compromiso entre coste y funcionalidad. Si a ello le añadimos que la comunicación entre etiquetas y lectores se realiza en un canal potencialmente inseguro y que cualquier lector compatible puede acceder a la comunicación de las etiquetas en su rango de lectura, la comunicación del sistema EPC Gen2 padece el riesgo de sufrir ataques a la seguridad y privacidad de sus comunicaciones.

El presente artículo plantea un modelo de adversario en función de las opciones y capacidades del adversario, y de las medidas de seguridad establecidas por el estándar EPC Gen2 (Sec. II). Se hace especial hincapié en la singularidad del modelo de comunicaciones del sistema EPC Gen2 en el que solo se establecen medidas de seguridad para los contenidos transmitidos por el canal *lector-etiqueta*. En la Sección III se hace una descripción detallada de las diferentes amenazas que puede padecer el sistema EPC Gen2, agrupadas en escuchas fraudulentas, suplantación de identidades, divulgación de información y denegación de servicio. Para un análisis más detallado sobre la evaluación de las amenazas relativas a la autenticidad, integridad y disponibilidad de la comunicación en el sistema EPC Gen2, puede consultarse [8].

Agradecimientos

Este trabajo está financiado por el Ministerio de Ciencia y Educación, a través de los proyectos TSI2007-65406-C03-03 E-AEGIS, CONSOLIDER-INGENIO CSD2007-00004 ARES, y una beca doctoral IN3-UOC.

References

[1] EPCglobal. EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860-960 MHz. Tech. report, [On-line] `http://www.epcglobalinc.org/standards/`, 2008.

[2] A. Juels. RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communication, vol. 24, no. 2, pp. 381-394*, 2006.

[3] S. Sarma. Toward the 5 cents tag. Auto-ID Lab, Withe Paper, 2001.

[4] G. Avoine and P. Oechslin. RFID traceability: A multilayer problem. In *Financial Cryptography and Data Security, vol. 3570, pp. 124-140, LNCS, Springer Ed.*, 2005.

[5] J. Sounderpandian, R. V. Boppana, S. Chalasani, and A. M. Madni. Models for cost-benefit analysis of RFID implementations in retail stores. *Systems Journal, IEEE, vol. 1, no. 2, pp. 105-114*, 2007.

[6] D. C. Ranasinghe and P. H. Cole. An Evaluation Framework. In *Networked RFID Systems and Lightweight Cryptography, Chapter 8, pp. 157-167, Springer*, 2008.

[7] G. Avoine. Adversarial model for radio frequency identification. Swiss Federal Institute of Technology (EPFL), Security and Cryptography Laboratory (LASEC, Tech. Rep., 2005.

[8] J. Garcia-Alfaro, M. Barbeau, and E. Kranakis. Handling Security Threats to the RFID System of EPC Networks. In *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET, Auerbach Publications, Taylor &Francis Group*, 2010, in Press.

[9] J. Melia-Segui, J. Garcia-Alfaro, and J. Herrera-Joancomarti. Analysis and improvement of a pseudorandom number generator for EPC Gen2 tags. In *International Workshop on Lightweight Cryptography for Resource-Constrained Devices (Co-located with Financial Cryptography and Data Security 2010 conference)*, LNCS, Springer, 2010.

[10] S. Garfinkel, A. Juels, and R. Pappu. RFID privacy: An overview of problems and proposed solutions. *IEEE Security & Privacy IEEE, vol. 3, no. 3, pp. 34-43*, 2005.