SEGURIDAD EN TRANSACCIONES CON TARJETAS EMV

Galeano, Johnny.
johnnygaleano@gmail.com
Universidad Piloto de Colombia

Resumen—EMV es un nuevo estándar de medios de pagos, que afecta a los dos elementos que intervienen en una transacción con tarjeta; El plástico que presenta un nuevo chip, y el terminal en el que se realiza la transacción, el cual deberá interactuar fuertemente con ese chip.
Este estándar está suponiendo una revolución dentro del mundo de las tarjetas financieras, y como tal revolución, también está causando un gran impacto en las aplicaciones informáticas de las entidades y otros sectores que de acuerdo a regulaciones nacionales e internacionales se deben acoger para estar en cumplimiento.
El presente artículo tiene como objetivo central hacer el análisis e identificación del tipo de seguridad que ofrece el uso del estándar EMV en transacciones con tarjetas, para la disminución de fraudes y riesgos actuales.
Se establecieron las diferencias más importantes entre la seguridad de una tarjeta de crédito con tecnología de banda y una con tecnología de chip. Se identificaron las normas que rigen el uso de tarjetas inteligentes y los distintos mecanismos de seguridad utilizados en este estándar.
Por último, se aportan unas conclusiones sobre cómo ha funcionado hasta ahora el estándar y cuál podría ser el futuro del mismo de ahora en adelante.

Índice de Términos—Banda Magnetica, Chip, Cifrado, EMV, PIN, Tarjetas.

I. INTRODUCCIÓN

EMV es un estándar de medios de pago definido por los sistemas internacionales VISA y MasterCard, y adoptado por la Unión Europea en sus normativas SEPA.
Antes de profundizar en las características de este estándar, se repasará brevemente la historia de las tarjetas bancarias o de pago, desde sus comienzos hasta la aparición de EMV. Este estándar nos ofrece entre sus principales objetivos:

- Aumento de la seguridad y reducción del fraude, respecto al incurrido con las tarjetas de banda magnética, apoyándose en el uso del chip y en algoritmos de cifrado más complejos y avanzados que los usados anteriormente.

- Posibilidad de controlar de forma más minuciosa el uso de la tarjeta sin conexión, en entornos “Off Line”, consiguiéndose una mayor rapidez y flexibilidad a la hora de tomar decisiones sobre el riesgo de la tarjeta conforme a la situación y operatividad del titular.

- Obtención de otros beneficios adicionales, gracias a las posibilidades que permite el chip incorporado: por ejemplo, se pueden añadir en el mismo chip otras aplicaciones, como productos de prepago, aplicaciones de fidelización, control de acceso, firma digital, entre otros.

II. ANALISIS

A. Problemática

En la actualidad, existen dos tipos de tarjetas, las que usan banda magnética y las que usan chip (para estas últimas deben existir terminales de lectura con ambas tecnologías) las dos brindan diferentes tipos de seguridad. Cada una cuenta con niveles de seguridad estandarizados y probados, pero ¿Es suficiente esto?, los bancos entregan y enseñan procedimientos para mejorar esta seguridad dentro y fuera de él, ¿será que alguien más nos está observando?, la publicidad no se cansa de promover campañas para que se bajen los indicen de fraudes y robos electrónicos, ¿estaremos preparados para este tipo de educación?, En referencia a lo anterior se ve

la necesidad de hacer el siguiente cuestionamiento: ¿la seguridad que brinda el estándar EMV es suficiente para disminuir fraudes y minimizar los riesgos que se presentan en la actualidad?.

B. Funcionamiento

La tarjeta de crédito es un instrumento material de identificación del usuario, que puede ser una tarjeta plástica con una banda magnética, un microchip y un número en relieve. Es emitida por un banco o entidad financiera que autoriza a la persona a cuyo favor es emitida, utilizarla como medio de pago en los negocios adheridos al sistema, mediante su firma y la exhibición de la tarjeta[1]. Una banda magnética es toda aquella banda oscura presente en tarjetas de crédito, que está compuesta por partículas ferromagnéticas incrustadas en una matriz de resina y que almacenan cierta cantidad de información mediante una codificación determinada que polariza dichas partículas. La banda magnética es grabada o leída mediante contacto físico pasándola a través de una cabeza lectora/escritora gracias al fenómeno de la inducción magnética. Fue inventada por IBM en 1960 [2].

Una tarjeta inteligente (smart card), o tarjeta con circuito integrado (TCI), es cualquier tarjeta del tamaño de un bolsillo con circuitos integrados que permiten la ejecución de cierta lógica programada. Aunque existe un diverso rango de aplicaciones, hay dos categorías principales de TCI. Las Tarjetas de memoria contienen sólo componentes de memoria no volátil y posiblemente alguna lógica de seguridad. Las tarjetas micro procesadoras contienen memoria y microprocesadores[3]. Hasta el punto mencionado la tecnología chip aporta prácticamente lo mismo que la banda magnética.

Sin embargo hay al menos tres campos en los que la potencialidad implícita en el chip da a esta última tecnología una clara ventaja de cara al futuro.

- ✓ Seguridad
- ✓ El contenido de la banda magnética, por la tecnología que implica, puede ser leído y, aunque no es sencillo, puede ser manipulado por personas con conocimiento y medios adecuados. El chip, sin embargo, contiene una tecnología interna mucho más sofisticada que hace que las posibilidades de manipulación física se reduzcan de forma muy sensible. Además, por su capacidad interna, es capaz de soportar procesos criptográficos muy complejos (DES simple, triple DES, RSA...). Más adelante en este documento se hablara más sobre la seguridad en las tarjetas inteligentes.
- ✓ La cantidad de información incorporable a una banda magnética es pequeña y, parcialmente modificable, por lo que la relación entre el usuario de la tarjeta y el emisor es unidimensional: únicamente se actualiza cuando sé interactúa a través de hardware sofisticado (ATMs). El chip, sin embargo, une a su mayor capacidad de recogida de información, la virtualidad de poder gestionar dicha información, con lo que se abren nuevas posibilidades para la relación usuario-emisor. Estas características diferenciales motivan que la difusión de la tecnología chip aplicada en tarjetas de plástico sea altamente deseable.
- ✓ Capacidad de almacenamiento de información
- ✓ Flexibilidad

El propósito del estándar EMV es permitir una interoperabilidad segura, a nivel mundial, entre tarjetas IC y terminales de pago de tarjetas de crédito que cumplan el mismo. Existen dos ventajas principales fruto del hecho de cambiar a tarjetas de crédito y sistemas de pago basados en EMV. Por un lado, destaca la mayor seguridad, lo que implica una reducción del fraude, así como la posibilidad de controlar de forma detallada la aprobación de transacciones off-lineen cada uno de sus usos. Las transacciones financieras mediante EMV ofrecen una mayor protección contra el fraude que los pagos tradicionales mediante tarjeta de crédito con banda magnética. Esto se debe al uso de

[1] Tarjeta de Crédito, http://es.wikipedia.org/wiki/Tarjeta_de_cr%C3%A9dito.
[2] Banda Magnética, http://es.wikipedia.org/wiki/Banda_magn%C3%A9tica.
[3] Tarjeta Inteligente, http://es.wikipedia.org/wiki/Tarjeta_inteligente.

algoritmos de cifrado como DES, Triple-DES, RSA y SHA para la provisión de autentificación por parte de la tarjeta al terminal que lo procesa, y al centro que se encarga de la transacción. Sin embargo, el procesamiento es generalmente más lento que utilizando tarjetas de banda magnética, debido a los cálculos criptográficos necesarios en el intercambio de mensajes entre tarjeta y terminal.

C. Estandar EMV y Funcionalidad

EMV es un estándar de interoperabilidad de tarjetas con Chip y TPV con este soporte de Chip, para la autentificación de pagos mediante tarjetas de crédito y débito. EMV es acrónimo de "Europay Mastercard Visa", las tres compañías que inicialmente colaboraron en el desarrollo del estándar de este sistema operativo.
Los sistemas de tarjeta con Chip basados en EMV están introduciéndose de forma escalonada en todo el mundo. Esta tecnología supone para su tarjeta:

- Un mayor nivel de seguridad ya que implica una reducción del fraude.
- Una protección extra en el uso de su tarjeta.
- La posibilidad de controlar de forma más detallada la aprobación de transacciones con su tarjeta sin conexión ("offline").

La inversión de responsabilidades en su uso en comercios, ya que los comerciantes son responsables de todo fraude resultante de una transacción realizada sin EMV en sus sistemas.

Funcionamiento en comercios y cajeros

Cuando se ha realizado una compra en un comercio, pueden ocurrir dos cosas:

Que el comercio disponga de un terminal apto para tarjetas con Chip

Que el comercio disponga de un terminal que solo lea tarjetas con banda magnética

Si el comercio dispone de un terminal apto para tarjetas con Chip, una vez introducida la tarjeta le solicitarán que teclee su número PIN (cuide siempre que nadie lo observe ni pueda copiar su número) y a continuación finalizará la operación y se emitirá recibo de compra que no es necesario firmar. En caso de que por cualquier circunstancia no funcionase correctamente el terminal, su tarjeta también puede funcionar con el sistema de banda magnética en cuyo caso sí será necesario firmar el comprobante de la operación.

En caso de que el PIN tecleado sea incorrecto, el terminal lo solicitará de nuevo hasta 3 veces y si no se introduce el correcto no se autorizará la operación y se desactivará automáticamente la tarjeta. Durante todo el tiempo que dure la operación de pago la tarjeta permanecerá insertada en el terminal TPV. Si el comercio no dispone de un terminal apto para tarjetas con Chip, su tarjeta se encuentra igualmente preparada para funcionar con el sistema de banda magnética. En este caso se le solicitará la firma en el comprobante de la operación.

Cuando se realiza cualquier consulta o extracción de efectivo en un cajero automático, el funcionamiento es similar tanto si la tarjeta funciona con el sistema de Chip como con banda magnética, ya que siempre será solicitado teclear el número PIN para validar la operación. Estas tarjetas presentan bastantes ventajas en comparación con las de bandas magnéticas: Son capaces de almacenar más información.

Pueden proteger la información que almacenan en sus memorias de posibles accesos no autorizados.

Poseen una mayor resistencia al deterioro de la información almacenada.

Dado que el acceso a la información se realiza a través de un puerto serie y supervisado por el propio sistema operativo de la tarjeta, es posible escribir datos confidenciales que no puedan ser leídos por personas no autorizadas. En principio, las funciones de escritura, lectura y borrado de la memoria pueden ser controladas tanto por el hardware como por el software, o por ambos a la vez. Esto permite una gran variedad de mecanismos de seguridad. Siendo el chip integrado el componente más importante, las tarjetas están clasificadas según el tipo de circuito.

III. RECOMENDACIONES

Cada uno de los actores involucrados en este proceso de seguridad con manejo de tarjetas como lo son productores, emisores y usuarios deben saber e implementar cuales son los controles mínimos exigidos por la industria para poder garantizar que no se presenten fraudes ni desfalcos en las instituciones financieras ni en los clientes.

IV. CONCLUSIONES

La conciencia de seguridad debe existir en todos los sectores.

Las instituciones deben garantizar que las medidas implementadas se cumplan.

La conciencia de seguridad debe ser conocida y propagada por todos los medios.

La seguridad es responsabilidad de todos.

REFERENCIAS

[1] Tarjeta de Crédito, http://es.wikipedia.org/wiki/Tarjeta_de_cr%C3%A9dito.
[2] Banda Magnética, http://es.wikipedia.org/wiki/Banda_magn%C3%A9tica.
[3] 1 Tarjeta Inteligente, http://es.wikipedia.org/wiki/Tarjeta_inteligente.
[4] Guía de Seguridad EMV. Criptografía Simétrica en Transacciones EMV. Versión 2.01, Septiembre de 2.007 Documentación EURO6000-CEC
[5] Guía de Seguridad EMV. Servicios de Certificación EMV. Versión 2.00, Septiembre de 2.007 Documentación EURO6000-CECA
[6] EMVCo http://www.emvco.com/