SEGURIDAD EN LAS TRANSICIONES CON TARJETAS DE CRÉDITO

Por Adrian Tendero Lara

Contenido

Introducción a las Tarjetas de Crédito

Las tarjetas de crédito fueron inventadas en 1914 por la empresa Wester Union que permitía a sus clientes, realmente selectos, acceder a una línea de crédito dentro del banco aunque dicha tarjeta de crédito no permitía ninguna de las funciones actuales como pagar en cualquier tienda y que el banco te avale sino que solo era valido para las propios establecimientos de las empresas, Dicha idea la fueron implementando otras empresas como “General Petroleum Corporation en 1924 para comprar gasolina o “American Telephone & Telegraph” en 1929, este modelo económico de tarjetas de crédito fue utilizado durante mas de 30 años.

Entonces en 1949 cuando Frank X. McNamara creo la tarjeta de “Diner’s Club” con la idea de poder pagar en distintos restaurantes con una sola tarjeta cuya idea principal es que los establecimientos paguen una comisión por cada operación con dicha tarjeta y cobrarle al comprador (Usuario de la tarjeta) una cuota por mantenimiento. Ante el éxito de dicha tarjeta a finales de 1951 las entidades financieras empezaron ha subirse al carro y emitiendo sus propias tarjetas de Crédito.

Como se puede suponer, al principio dichas tarjetas de crédito eran de papel o cartón donde la única medida de seguridad era un numero de cuenta valido, el nombre y dirección del propietario de la tarjeta, la firma de dicho usuario, muchas veces escritas ha mano por el propio banquero, y así como la plantilla de la propia tarjeta, es decir no muy segura.

Los picaros y estafadores de la época se encontraron campando a sus anchas timando a las tiendas ya que cualquiera que consiguiera imitar la plantilla de una tarjeta de crédito podía poner rellenar el mismo ha mano o ha maquina el resto de datos y presentarla ante un establecimiento que acepten dicha tarjeta y “pagar” con ella sus servicios que en muchos casos no se detectaban dicha irregularidad hasta que el establecimiento intentara cobrar del banco dicha cuenta y se comprobaran que los datos de dicha tarjeta eran falsos, ya demasiado tarde para evitar el daño.

Ha finales de la década de los sesenta el uso de tarjetas de crédito se estaba masificando y ante la necesidad de una mayor seguridad IBM invento en 1962 las tarjetas de crédito con banda magnética, donde se grababan datos sensibles y de autentificación, añadiendo una capa mas de seguridad y dificultad que los falsificadores tendrían que superar y fueron el formato mas utilización por las tarjetas de crédito hasta prácticamente el nuevo siglo.

Las tarjetas Inteligentes o con Microchip se patentaron en los años 70 no fue hasta la década de los 90 que se empezó ha utilizar en la banca y en el año 1996 se creo el primer estándar para dichas tarjetas de crédito, el “EMV”, que procede

de los nombres de las tres grandes empresas que lo fomentaron (Europay, MasterCard y Visa) y revisado dicho estándar en 2000.

Actualmente el estándar EMV es tan costoso de implementar y cuyo único beneficio es impedir la estafa y robo de datos que los expertos debaten si el coste de implementarlo se compensa con los beneficios que se obtienen o si por el contrario merece la pena esperar y no implementar dichas implementaciones y comenzar ha implementar la nueva tecnología Contactless (Sin contacto) que se esta poniendo de moda estos últimos años.

Durante 2017 y 2018 se esta dando un auge en las tarjetas de crédito Contactless que utilizan la tecnología NFC o (near Field Communication) que se está implantando en la actualidad.

Tecnología de Tarjetas con bandas Magnéticas

LA tecnología de Bandas Magnéticas se basa en la codificación de diferentes datos en bandas magnéticas y generalmente siguen y cumplen con las Estandarizaciones de ISO7810,7811,7813 y el ISO 4909 que define las especificaciones estándar de las tarjetas de crédito.

Por estándar las tarjetas de crédito tienen 3 bandas magnéticas consecutivas

El estándar ISO7810 describe las características físicas de la tarjeta, formato, datos que debe mostrar donde tiene que estar, que no tiene que estar, esas cosas, cosas que para este trabajo no nos interesan demasiado, en cambio los ISO7811 se centran en como codificar la información en las diferentes bandas magnéticas.

La primera pista de la banda magnética es la única que tiene incorporada en su codificación caracteres Alpha-numéricos por eso mismo cada carácter esta codificado en 7 bits siendo el ultimo bit un bit de paridad mientras que la segunda y tercera pista solo contienen datos numéricos y en consecuencia solo utilizan 5 bits para la codificación siendo el ultimo también para bit de paridad.

Como primera medida de seguridad contra los impostores que intentaran utilizar una tarjeta robada o clonada se implemento el PIN de la tarjeta de crédito que seria enviado a la entidad financiera para que comprobara si el pin introducción coincidía con el suministrado por el usuario a la hora de expedir la tarjeta de crédito.

El problema con esta solución es que al principio los datos se mandaban sin ninguna protección y si el canal de comunicación se encuentra comprometido se puede obtener el código PIN sin ninguna dificultad ya que se trasmitida como texto plano.

Por tanto para evitar esto se procedió ha encriptar el pin utilizando el algoritmo DES y una clave común ha ambos lados de la comunicación.

Es decir se estaba implementando una seguridad criptográfica de forma simétrica donde la clave para descifrar es la misma que se utiliza para cifrar es decir el código PIN y el numero Aleatorio por tanto este proceso no se podía realizar de forma Offline, tenia que haber una comunicación entre la Autoridad financiara y el comercio.

Teniendo en cuenta que los terminales de los comercios tenían que tener capacidad para cifrar y descifrar el DES se innovo procediendo ha validar la tarjeta de crédito desde el propio terminal del establecimiento gracias al uso de un Numero Aleatorio generado en la entidad financiera a la hora de crear la tarjeta y grabada en las bandas magnéticas se concatena junto al código PIN introducido y aplicando el algoritmo DES o Triple-DES en las ultimas generaciones de tarjetas magnéticas, asimismo no se llego ha aplicar de manera generalizada el algoritmos AES mas reciente y seguro en tarjetas de crédito con bandas magnéticas, tras realizar aplicar el algoritmo el resultado se compararía con el Parámetro de Autentificación, que también se graba en las bandas magnéticas y si coincide el Parámetro de autentificación con el resultado de aplicar DES al Numero Aleatorio concatenado con el PIN se autoriza la operación ya que el pin introducido es valido.

Esto aumenta la seguridad de las tarjetas con bandas magnéticas pero siguen siendo muy vulnerables ya que si alguien clona la tarjeta de crédito obtendría tanto el Numero aleatorio y el Parámetro de Autentificación ya que están grabadas en la banda magnética y con ataques de fuerza bruta se podría obtener el código PIN, que es la base de toda la seguridad de esta generación de tarjetas y por tanto un desastre en potencia.

Por este motivo se crearon una nueva generación de tarjetas de crédito las denominadas tarjetas inteligentes o con microchips.

Tecnología de Tarjetas Inteligentes

Las tarjetas inteligentes o con microchips suponen una innovación al mundo de las transiciones bancarias ya que permiten un aumento muy significativo de la seguridad gracias a que ahora parte de la información más sensible se esta introduciendo en el chip en vez de estar en la banda magnética así mismo el chip no solo es un elemento de almacenamiento de datos como las bandas magnéticas sino que tienen más capacidades como la de generar un código de

identificación de operación única para cada compra, facilitando la detección de operaciones ilícitas.

Las tarjetas con microchips siguen el estándar EMV este presenta innovaciones como la seguridad Offline gracias al uso de la Criptografía Asimétrica en concreto al algoritmo RSA.

Este proceso se basa en un trípode por un lado se encuentran las autoridades de certificación (VISA, MasterCard) que actúan de intermediario y certificando que las claves publicas tanto del establecimiento como del banco que emite las tarjetas tengan un certificado que contiene la clave publica de la autoridad de certificación.

Con esto se permite que el establecimiento como la tarjeta de crédito que ambos tienen la clave publica de la autoridad de certificación se legitimen mutuamente como actores validos en la transición y no sean duplicados o falsificaciones.

Para validar las operaciones es necesario que el banco o entidad financiera que abala la tarjeta de crédito genere un par de claves RSA (publica y privada) y cuya parte publica sea certificada por la autoridad de certificación correspondiente y que esta le mande su clave publica para que sea incorporada a la tarjeta de crédito.

Hay tres formas de autentificación offline, SDA (Static Data Authentification), DDA (Dinamic Data Authentification) y CDA (Combined Data Authentification).

El funcionamiento del SDA es el siguiente, el terminal del comercio tiene que obtener la clave pública de la Autoridad de certificación de la tarjeta y comprobar que coincida con la que tiene almacenada el, después procederá a obtener la clave publica del emisor de la tarjeta y después proceder a verificar la firma sobre los datos de la terminal que son estáticos.

El método DDA busca garantizar que los datos contenidos o generados por la propia tarjeta de crédito sean veraces y evitar la falsificación de la tarjeta de crédito y comprobar también que la terminal del comercio sea legitima para ello se procede ha firmar los datos dinámicos de la tarjeta (ICC Dynamic Data) y la lista de datos que son recibidos por el terminal DDOL (Dynamic Data authentification Object List).

Y el CDA es una combinación mixta del SDA y DDA donde se realizar las comprobaciones del SDA y se proceden a firmar los datos relevantes de la tarjeta de crédito asi como los recibidos por la terminal del comercio, mezclando ambos métodos.

Después el Estándar EMV también contempla la autentificación online para compras por internet, por ejemplo. Para ello se utiliza un método de autentificación de la tarjeta en la cual la tarjeta tendrá que enviar un ARQC (Authorization Request Cryptogram).

Cuando el terminal de la tienda recibe el ARQC de la tarjeta de crédito este genera un ARPC (Authorization Response Cryptogram) con sus datos y procede a

enviarlos a la tarjeta de crédito como parte del mensaje de los datos de autentificación del emisor, gracias al cual la tarjeta puede autentificar al terminal de la tienda.

Para general el ARQC que se realiza en la propia tarjeta el algoritmo toma como entradas los datos seleccionados y la clave maestra especifica de la tarjeta que se encuentra en la propia tarjeta y computa un criptograma de 8 bytes en los cuales se tiene en cuenta la clave de la sesión actual que se obtiene a partir de la clave maestra y el contador de transacciones de la tarjeta.

Esto se aplica a una función MAC (Message Authentication Codes) cifrando con Triple DES en el Modo CBC con la clave de sesión a los datos Seleccionados de tal forma que se genera el ARQC.

ARQC: = MAC: = MAC (Clave de Sesión) [Z]

En Cambio, el ARPC de un tamaño de 4 o 8 bytes son generados por la terminal de la tienda como respuesta al ARQC enviado previamente por la tarjeta con microchip y que al enviárselo al terminal servirá para acreditar al terminal como legitimo frente al microchip de la tarjeta.

Este ARPC se puede generar de dos maneras según el estándar EMV:

La primera opción necesitamos el código ARQC enviado por la tarjeta y un código de respuesta de autorización (ARC) de un tamaño de 2 bits.

El algoritmo es, primero rellenar el ARC con 6 bits a 0 para que el resultado X sea de 8 bytes, segundo Hacemos la operación XOR entre el ARQC y la X anterior para darnos Y tercero obtenemos el ARPC aplicando triple-DES usando la clave de Sesión y la Y para generar el ARPC de 8 bytes.

La segunda opción necesita el uso del ARQC de 8 bits enviado por la tarjeta así como el CSU (Card Status Update) de 4 bytes y los datos de autentificación de los propietarios (DAP) de 0 a 8 bytes.

el algoritmo consiste en concatenar el ARQC con el CSU y los DAP en ‘Y’, y después utilizar esta ‘Y’ en la generación del ARPC de tal forma que se aplique el MAC (tipo 3) con s=4 de tal forma que quedaría así.

ARPC: = MAC: = MAC (SKAC)[Y]

Pero en este caso el ARPC no es la respuesta que enviamos a la tarjeta sino que realizamos una operación más y generamos el llamado IAD (Issuer Authentification Data) que es simplemente la concatenación del ARPC generado, el CSU y la DAP.

Con esto conseguimos la verificación y autentificación de las tarjetas de crédito de modo online con un nivel de seguridad bastante más destacable que las medidas que incluían la generación anterior de tarjetas con banda magnética.

Conclusiones

Yo con todo lo dicho anteriormente me quedo convencido que la seguridad de las antiguas TBM (tarjetas con bandas magnéticas) son prácticamente irrisorias en el principio y aunque se mejoro notablemente durante su ciclo de vida, las TCM (Tarjetas con microchips) son claramente superiores a las TBM puesto que incorporan bastantes mas medidas de seguridad.

También me habría gustado de poner información mas concreta sobre la tecnología que se esta empezando ha usar actualmente que es la tecnología contactless o sin contacto que emplea los protocolos de NFC pero es bastante difícil de localizar y sintetizar la información.

Me ha sido bastante difícil encontrar información sobre este tema la mayoría de las páginas que he visitado la única información que aportaban era por que esto es mas seguro que lo otro y poco mas que publicidad para la siguiente generación de tarjetas, es decir mucha información sobre por que las TCM (Tarjetas con microchips) son mejores que las TBM pero no profundizan nada en los procesos.

Bibliografía

TFC de Santiago Garran Martin (INFO sobre TBM y TCM)

Información General Sobre TCM

TD de Joaquin Torres Marquez (Info sobre TCM)

WIKI TBM

WIKI General Tarjetas de Crédito

Wiki TCM o TI

WIKI info Estandard EVM

Info sobre la evolucion de las Tarjetas de Crédito

Mas info sobre la Evolucion de las TC

Autentificacion Online de TCM

Wiki Algoritmos MAC

Nota : en caso de que el TFC de Santiago Garran o el TD de Joaquín Torres no estén disponibles en los enlaces tengo yo los PDF descargados, en caso de necesitarlos pídamelos y se lo facilitare.