Protocolo Seguro para un Sistema de Pago Móvil basado en el modelo céntrico del quiosco.

Jesús TÉLLEZ[1], José SIERRA[2], Antonio IZQUIERDO[3] y Mildrey CARBONELL[4]

[1] Departamento de Computación – FACYT, Universidad de Carabobo
Valencia, Estado Carabobo 2001, Venezuela.
email: jtellez@uc.edu.ve

[2,3,4] Departamento de Informática, Universidad Carlos III de Madrid
Leganés, Madrid 28911, España
email: {[1]sierra, [2]aizquier}@inf.uc3m.es, mildreycc@yahoo.es

RESUMEN

En este artículo presentamos un protocolo seguro para un sistema de Pago móvil basado en modelo céntrico del quiosco que utiliza operaciones de clave simétrica que requiere bajo poder computacional y pueden ser procesadas con mayor rapidez que las asimétricas. Nuestro protocolo protege la identidad real de los clientes que realizan la compra y se adapta a todos los sistemas de pago móvil donde el cliente no puede comunicarse con el emisor debido a la falta de acceso a Internet y a los altos costos de implementar otros mecanismos de comunicación entre estas dos entidades. Sin embargo, esta investigación muestra como un equipo portable equipado con un enlace de corto alcance (como bluetooth, infrarojo o Wi-Fi) y bajo poder computacional debería ser suficiente para interactuar con un máquina vendedora para compra mercancía de una manera segura. También, el protocolo utilizado en la propuesta de esta investigación satisface todas las propiedades de seguridad de una transacción proporcionada por otros sistemas de pago móvil que utilizan criptosistemas de clave pública.

Palabras Claves: Sistema de Pago Móvil, Protocolo Criptográfico, Protocolo de Comercio Electrónico, Seguridad.

1. INTRODUCCIÓN

La popularidad del m-comercio ha aumentado en los últimos años gracias al rápido desarrollo de las tecnologías de comunicación móviles lo que ha permitido que las personas puedan utilizar teléfonos móviles o asistentes personales digitales (PDA) para acceder a la Internet (para leer el correo electrónico, navegar en la red o para adquirir información o bienes) dondequiera y en cualquier momento.

Desde la aparición el primer dispositivo móvil en el mundo, ha habido un rápido desarrollo de nuevas funciones, mejora de los servicios y un progreso en el poder computacional de los dispositivos móviles que han hecho al m-comercio más provechoso y prometedor. Sin embargo, todavía hay un amplio escepticismo sobre comprar y pagar los productos en línea debido a los numerosos fraudes de tarjetas de crédito cometido por hackers durante la transmisión sobre los canales de comunicaciones. Por esta razón es necesario desarrollar sistemas electrónicos de pago capaces de proporcionar comunicaciones seguras y dignas de confianza entre los clientes y los proveedores de servicios móviles en línea.

Para [5], los proveedores de servicios móviles en línea deben buscar mecanismos que le permitan asegurar que no habrá ningún conflicto en cada transacción comercial y en caso de ocurrir, cómo el sistema lo resolverá sin perder la imparcialidad.

Diversos sistemas de pago electrónico (incluyendo sistemas de pago móvil) han sido propuestos en los últimos años, pero el desarrollado por Visa International se ha convertido en un estándar debido a sus bondades en cuando a seguridad y flexibilidad en los métodos de autenticación. Este protocolo, llamado 3-D Secure ([9]), permite la autenticación del cliente cuando realiza un pago en línea con su tarjeta de débito o crédito e involucra funcionalidad en 3 dominios: el dominio del emisor, el dominio del adquirente y el dominio de la interoperabilidad.

A pesar de la flexibilidad que el 3-D Secure ofrece al emisor para elegir los métodos de autenticación (contraseña, firma simétrica y asimétrica, y biometría), la relación entre el cliente y el emisor es severa (aunque requerida por el esquema 3-D Secure de Visa) y no permite el uso de esquemas en los cuales la comunicación entre estas partes no es posible debido a: 1) la imposibilidad del cliente de conectarse a Internet desde el dispositivo móvil y 2) los altos costos e inconveniencias de utilizar la infraestructura necesaria para implementar otros mecanismos de comunicación entre el cliente y el emisor.

La mayoría de los sistemas de pago móvil propuestos hasta la fecha asumen que el usuario puede conectarse a Internet desde su dispositivo móvil así que las restricciones mencionadas anteriormente no constituyen un tema de importancia. Sin embargo, es bastante común que el cliente se encuentre con situaciones en las cuales no es posible acceder a la Internet así que se hace necesario desarrollar sistema de pago móvil donde el usuario puede usar su dispositivo móvil para realizar compras incluso si tiene o no acceso a Internet.

Por otra parte, a pesar de la amplia gama de dispositivos móviles disponibles en el mercado, todo ellos tienen

limitaciones comunes: 1) capacidades de cómputo pobre, 2) espacio de almacenamiento limitado y 3) vida corta de la batería [7]. Estas limitaciones imposibilitan que estos dispositivos ejecuten, de manera eficiente, altas operaciones de cómputo como las requeridas en los esquemas tradicionales de criptografía asimétrica. Incluso, si el dispositivo móvil contara con un procesador especial, todavía tomaría un largo tiempo para procesar tales operaciones en dichos dispositivos.

La criptografía simétrica (que utiliza una clave compartida entre dos entidades) proporciona, al igual que la criptografía asimétrica, confidencialidad del mensaje, integridad del mensaje y autenticación de la entidad, y representa una alternativa en la construcción de protocolos seguros para sistemas de pago móvil debido a que las operaciones de clave simétrica se pueden procesar más rápido que las asimétricas, no requieren de un alto poder computacional ni de pasos adicionales de comunicación (como sucede es los protocolos de clave asimétrica en donde los certificados de clave pública deben ser verificados por una Autoridad Certificadora).

En este trabajo se presenta un protocolo seguro (que soporta transacciones con tarjetas de débito y crédito) para un sistema de pago basado en modelo céntrico del quiosco (propuesto por [3]) que supera las limitaciones mencionadas anteriormente. Nuestra propuesta representa una alternativa a las restricciones de todos aquellos sistemas de pago móvil (incluyendo Visa 3-D secure) en cuanto a la conexión entre el cliente y el emisor. Además, mantiene el anonimato de identidad real de los clientes que realizan la compra y utiliza operaciones de clave simétrica en todas las partes que participan en el proceso para reducir tanto los costos de montaje de la infraestructura de pago como el costo de la transacción.

Otro beneficio derivado del uso de nuestra propuesta es la reducción de las operaciones a realizar en todas las partes implicadas y de los pasos de comunicación (en comparación con los protocolos basados en infraestructura pública) que lo convierte en apropiado para dispositivos móviles con bajos poder computacional.

El resto del artículo esté organizado de la siguiente manera: en la siguiente sección se presentan los trabajos relacionados; seguidamente se detallara la propuesta para solucionar el problema planteado. Finalmente, se ofrece una perspectiva de los trabajos futuros y se muestran las conclusiones del trabajo.

2. TRABAJOS RELACIONADOS

En años recientes, diversos estudios se han realizado para mejorar la seguridad de los sistemas de pago móvil. Así mismo, los esfuerzos también han sido dedicados a unificar conceptos y escenarios en entornos de trabajo que serán de utilidad para el desarrollo de nuevos sistemas de pago electrónico. La investigación realizada por [3] es un ejemplo de un estudio que unifica diversos usos del m-comercio en un simple entorno de trabajo. Por otra parte, la misma investigación revisó el rango posible de escenarios móviles, identificando los temas de seguridad para cada escenario de conectividad. Como resultado, 5 escenarios fueron identificados y analizados: Interacción Desconectada (Disconnected Interaction), Caso Centrado en el Servidor (Server Centric Case), Caso Centrado en el Cliente (Client Centric Case), Conectividad Total (Full Connectivity) y el Caso Centrado en el Quiosco (Kiosk Centric Case). Éste último es considerado el punto de partida en el diseño de la propuesta presentado en este trabajo.

En [10], los métodos de pago son clasificados de acuerdo a varios estándares. Por otra parte, este estudio analiza y precisa las ventajas y desventajas de estos sistemas. Además, la investigación también proporciona una estructura general en capas y un proceso de pago para dispositivos móviles basado en pre-pagos y cuentas. Los requerimientos para la solución propuesta son bajos (tanto en costos como en capacidades técnicas) y también tiene altas características de escalabilidad y seguridad. Sin embargo, sus métodos y procesos no son apropiados para la propuesta de está investigación, ya que el objetivo principal es sugerir un esquema basado en post-pago[1] y criptografía asimétrica.

Un sistema de pago de un solo sentido seguro y eficiente fue propuesto por [5]. En su solución, la seguridad del sistema está basada en el control del problema discreto del logaritmo y la función hash de clave de un solo sentido. Pese a que la propuesta diseña un sistema de pago móvil con una complejidad mínima utilizando un par de claves públicas, el modelo operacional requiere que el cliente tenga comunicación con Internet lo que es opuesto a la propuesta de esta investigación.

El trabajo más cercano al nuestro es el protocolo de pago móvil propuesto por [6]. Su trabajo propuso un protocolo seguro de pago basado en cuenta, apropiado para redes inalámbricas y que utiliza operaciones de clave simétrica y requiere bajo poder computacional en todas las partes del sistema en comparación a los protocolos de pago existentes. Mientras esta propuesta satisface la mayoría de nuestros requerimientos, es necesario reformularlo para satisfacer los requerimientos del esquema que sugerimos en este trabajo, en donde el cliente nunca establece comunicación con el emisor (por ninguna vía) durante la transacción de pago y el programa de pago es enviado al cliente por el emisor a través del vendedor.

Como el software de pago (en inglés Wallet Software y se refiere a un pequeño programa utilizado para en las transacciones de compra en línea) deberá ser enviado por el emisor al cliente a través del vendedor, se hace necesario el uso de técnicas que aseguren que el programa recibido por el cliente fué creado y enviado por el emisor y no ha sido trampeado. Para lograr la protección del software en los aspectos mencionados anteriormente, dos propuestas diferentes relacionadas con las técnicas ya mencionadas serán detalladas en los próximos párrafos.

El primer trabajo (propuesto por [4]) introdujo un nuevo enfoque de marcas de agua, llamado marcas de agua basadas en caminos (en inglés, path-based watermarking) que incrusta la marca de agua, con costos relativamente bajos, en la estructura de árbol dinámica del programa (tales como código nativo IA-32 y java byte code), y muestra como las técnicas de corrección de error (error-correcting) y pruebas de trampa (tamper

[1] Pago móvil en donde el cliente recibe el bien comprado y lo consume antes de pagarlo. Las tarjetas de crédito son un ejemplo de este tipo de pago.

proofing) pueden ser utilizadas para hacer la propuesta de este trabajo resistente contra una amplia variedad de ataques.
El otro trabajo, propuesto por [8], describe 3 técnicas para ofuscar el diseño de un programa (en inglés, obfuscation of program design): 1) La ofuscación por fusión de clases reemplaza varias clases en una sola clase, 2) En la ofuscación por división de la clase, una sola clase es reemplazada por múltiples clases, cada una responsable de una parte de la funcionalidad de la clase original, y 3) La ofuscación por ocultamiento de la clase que utiliza el mecanismo de las interfaces en java para ocultar los tipos de objetos manipulados por el programa.

Los resultados experimentales (aplicando esta técnica de ofuscación a programas java de tamaño mediano) muestran que el tiempo de ejecución por encima, en el peor de los casos (ofuscación por división de la clase), es menor al 10% del tiempo total de ejecución del programa.

3. PROPUESTA

Para solucionar el problema de compra y pago de bienes en un sistema de pago móvil en donde el cliente no tiene comunicación directa con el emisor pero tiene una conexión viable con el vendedor (utilizando un enlace de corto alcance como bluetooth, infrarojo o wi-fi), es necesario construir un protocolo que permita al cliente enviar, desde su dispositivo móvil, un mensaje al emisor a través del vendedor (quien nunca podrá descifrar este mensaje). Para lograrlo, se propone un protocolo (dividido en 2 sub-protocolos) basado en operaciones de clave simétrica que permite a dos partes del sistema de pago (ejemplo, cliente – vendedor), enviar mensajes cifrados con la misma clave simétrica (no conocida por otras partes).

Entidades y Notaciones

Todas las entidades que involucradas en nuestro protocolo se comunican a través de redes inalámbricas y cableadas.

Los símbolos C, V, P, I, A son utilizados para denotar las entidades Cliente, Vendedor, Pasarela de Pago, Emisor y Adquirente respectivamente. Lo siguiente símbolos son utilizados para representar otros mensajes y protocolos:

- ID_P: la identificación de la entidad P que contiene la información de contacto de P.
- NID_C: apodo del cliente, identificación temporal.
- TID: identificación de la transacción que incluye la hora y fecha de la transacción.
- OI: Información de la Orden (OI = {TID, *h*(OI, Precio)}) donde OI y Precio se refiere a descripciones de la orden y su cantidad.
- TC: El tipo de tarjeta utilizada en durante el proceso de compra (TC = Crédito, Débito).
- Stt: Estatus de la transacción (Stt = {Aceptada, Rechazada}).
- TIDReq: La petición para TID.
- VIDReq: La petición para ID_V.
- $\{M\}_X$: el mensaje M cifrado simétricamente con la clave compartida X.
- MAC(X, K): Código de la autentificación del mensaje del mensaje X con la clave K.
- h(X): la función hash unidireccional del mensaje X.
- PSRes: Script de Respuesta del Pago (en inglés, Payment-Script Response).
- PSReq: Script de Petición del Pago (en inglés, Payment-Script Request).
- WSRes: Script de Repuesta del Reintegro (en inglés, Withdrawal-Script Response).
- DSRes: Script de Respuesta del Depósito (en inglés, Deposit-Script Response).
- WSReq: Script de Petición del Reintegro (en inglés, Withdrawal-Script Request).

Modelo Operacional

Generalmente, los modelos operacionales para el m-comercio encontrados en la literatura, involucran transacciones entre dos o más entidades. El modelo operacional utilizado en esta investigación está compuesto por cinco entidades:

- *Cliente:* un usuario que desea comprar bienes o servicios a un vendedor y tiene un dispositivo móvil con poco poder computacional (por ejemplo, un teléfono móvil, PDA, teléfono inteligente, etc.) y equipado con una pantalla integrada, un método de entrada enlace de corto alcance (como Infrarojo, Wi-Fi o Bluetooth) y capacidad para ejecutar un programa java.
- *Vendedor:* una entidad de computacional (un servidor web o una máquina de venta inteligente) que desea vender la bienes o servicios y con quien el usuario participan en una transacción.
- *Adquiriente:* la institución financiera del vendedor que verifica la validez de los instrumentos de pago depositados.
- *Emisor:* la institución financiera del cliente que le proporciona los instrumentos de pago electrónico para ser usando en un pago.
- *Pasarela de Pagos:* entidad adicional actúa como un medio entre el adquiriente/emisor (en la red privada bancaria) y entre el cliente/vendedor (del lado de Internet) para reintegrar el dinero de la cuenta del cliente y transferirlo a la cuenta del vendedor [6].

.
En la figura 1, se especifican los enlaces entre las entidades de nuestro esquema. Note que no existe conexión directa entre el cliente y el emisor. Además, la conexión entre el cliente y el vendedor (denotada con una línea segmentada) es establecida a través de un canal inalámbrico.

Por otra parte, la interacción entre el vendedor y el portal de pago (representada como una línea sólida en el esquema) debería ser confiable y segura contra ataques activos y pasivos. Por lo tanto, la conexión se supone que será establecida a través de un canal seguro no inalámbrico, utilizando un protocolo de seguridad bien conocido como SSL/TLS [5]. Note que el emisor, el adquiriente y el portal de pago operan dentro de la red bancaria privado así que esta investigación no considera los temas de seguridad de la conexión entres estas entidades.

El protocolo basado en criptografía simétrica propuesto por [6] es un punto de partida para nuestro protocolo. Nosotros reformulamos este protocolo para satisfacer los requerimientos de nuestra propuesta que pretende permitir a un cliente realizar compras desde su dispositivo móvil sin conectarse a Internet.

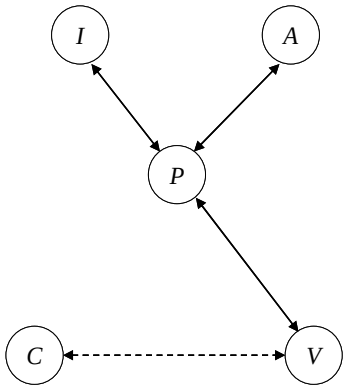

Figura 1: Modelo Operacional.

Técnica de Generación de Claves
Nuestro esquema maneja tres conjuntos diferentes de claves compartidas que son utilizados ara cifrar un mensaje simétricamente. El primer conjunto $VPSec_j$, j = 1…,n, es generado del secreto VPSec y se almacena en los terminales del vendedor y la Pasarela de Pago respectivamente. El otro conjunto $CISec_i$ (almacenado en el dispositivo del cliente y el terminal del emisor, respectivamente), i = 1…,n, se genera del secreto CISec. El último conjunto $CVSec_k$ (donde k = 1…,n) es generado del secreto CVSec y se almacena en el dispositivo del cliente y el Terminal del vendedor respectivamente.

Para generar los conjuntos de claves compartidas, aplicamos la misma técnica propuesta por [6]. Los detalles no son mostrados debido a la limitación de espacio.

Protocolos Detallados
Nuestro protocolo consiste en 4 sub-protocolos: Registro, Compra, Reintegro y Depósito. Cada sub-protocolo tiene las siguientes funciones:

Registro: Este protocolo implica al cliente, el vendedor y el emisor. El proceso comienza con la asignación de varios apodos al cliente a fin de proteger su verdadera identidad cuando se comunica con el vendedor. Estos apodos son conocidos solo por el cliente y el emisor.

Por otra parte, el cliente comparte la información de su tarjeta de crédito y/o débito (CDCI) con el emisor. CDCI contiene el secreto de largo plazo CISec (conocido solo por el cliente y el emisor) que será utilizado como método de autenticación por el cliente en futuros reintegros.

Además, el secreto SSWSec es compartido entre el cliente y el emisor y será utilizado como valor de marca de agua para el proceso de marca de agua (en inglés, watermarking process) en el lado del emisor y como entrada del programa de pago en el lado del cliente para determinar su autenticidad.

Cuando ocurre la primera compra, *V* detectará si el programa de pago está disponible en el dispositivo móvil. Si no lo está, *V* envía una petición del programa a *P*, que transmitirá la petición a *I*. El emisor protege el programa contra varios tipos de ataques en todo momento, siguiendo estos pasos: 1) selecciona uno de los métodos de ofuscación propuestos por [8] y lo aplica al código java del programa, y 2) aplica un proceso de marca de agua (propuesto por [4]) al programa (utilizando SSWSec como valor de marca de agua e incrustado en el programa).

Una vez que el programa ha sido preparado, el emisor lo transfiere a *P* para que éste lo envíe a *V* quien finalmente lo enviará a *C*. Después de que C reciba el programa, lo instala y confirma su autenticidad usando SSWSec. Si ocurre algún problema, *C* puede abortar el sub-protocolo de registro o comenzar el proceso de nuevo.

Cuando el programa ha sido instalado satisfactoriamente y está operativo, *C* genera CVSec y lo envía a *V* con NID_C y un nonce n (número aleatorio) cifrado con la clave de sesión K, generada durante la ejecución del protocolo AKE con *V*. Entonces, *V* envía *h(n,CVSec)* a *C* como confirmación del registro del cliente. Después de que el sub-procolo se ha completado, *C* y *V* pueden generar un nuevo conjunto de $CVSec_i$ utilizando la misma técnica de generación de clave. Por otra parte, el vendedor se registra en la Pasarela de Pago y comparte el secreto VPSec.

1) C → V: $\{NID_C, CVSec, n\}_k$
2) V → C: *h(n, CVSec)*

Compra: Este sub-protocolo se realiza entre *C* y *V* sobre un canal inalámbrico. El proceso comienza cuando *C* envía a *V* la información necesaria para establecer el sub-protocolo (paso 3). Después de finalizar el intercambio de información, *C* construye el PSReq con OI y TC. Luego, *C* lo cifra y envía a *V* quien lo descifra para recuperar OI.

3) C → V: NID_C, i, TIDReq, VIDReq
4) V → C: $\{TID, ID_V\}_{CVSeci}$
5) C → V: $\{OI,Precio, MAC[(Precio,TC, h(OI), ID_V), CISec_i]\}_{CVSeci}$, $MAC[(OI, Precio, NID_C, ID_I), CVSec_{i+1}]$

Observe que, aunque *V* descifra el mensaje usando $CVSec_i$, no lo puede generar puesto que no tiene el secreto $CISec_i$ necesario para construir $MAC[(Precio, TC, h(OI), ID_V), CISec_i]$. Así, cualquier entidad del sistema de pago móvil puede estar segura que el mensaje es verdaderamente enviado por *C*.

Reintegro: El sub-protocolo de reintegro ocurre entre V y P a través de un canal cableado seguro. *V* descifra el mensaje recibido de *C* (para recuperar OI), prepara el WSReq (incluyendo NID_C, ID_I y el índice *i* usado para identificar la actual clave de sesión en el conjunto de $CISec_i$) cifrado con $VPSec_j$ y luego lo envía a *P*.

Una vez que WSReq es recibido por *P*, éste lo envía *I*, agregando cierta información como su identidad (ID_P). Este nuevo WSReq será procesado por *I* para aprobar o rechazar la transacción.

Después de que el emisor ha procesado la petición y preparado el WSRes (incluyendo Stt), lo debe enviar a *P* quien lo remitirá a *V*. El sub-protocolo de depósito es activado por *P* solo cuando

el reintegro es aprobado. De lo contrario, *P* asigna el valor *Desechado* a Std.

Completados los sub-protocolo de reintegro y depósito, *P* envía el WSRes a *V* (incluyendo DSRes). Luego, *V* prepara el PSRes y lo envía a *C*.

6) V → P: $\{MAC[(Precio, TC, h(OI), ID_V), CISec_i], j, ID_V, h(OI), TID, i, Precio, NID_C, ID_I\}_{VPSecj}$, $MAC[(h(OI), i, TID, NID_C, ID_I\}VPSec_{j+1}]$

7) P → I: $MAC[(Precio, TC, h(OI), ID_V), CISec_i], i, h(OI), TID, Precio, NID_C, ID_V, h(VPSec_{j+1})$

8) I → P: $Stt, h(Stt, h(OI), h(CISec_i)), \{h(OI), Stt, h(VPSec_{j+1})\}_{CISeci}$

11) P → V: $\{Stt, \{h(OI), h(VPSec_{j+1})\}_{CISeci}, h(Stt, h(OI), h(CISec_i), \quad Std, h(Std, h(OI))\}_{VPSecj+1}$

12) V → C: $\{\{h(OI), Stt, h(VPSec_{j+1})\}_{CISeci}\}_{CVSeci+1}$

Depósito: este sub-protocolo ocurre entre la Pasarela de Pago y el Adquiriente a través de un canal cableado seguro cuando no se han encontrado problemas en el sub-protocolo de reintegro. Aquí, el DSRes es preparado por *P* quien la envía a *A* para que compruebe el Precio recibido con el negociado durante el proceso de compra. Si ambos valores coinciden, el valor *Aceptado* es asignado a Std y el monto total de OI es transferido a la cuenta del vendedor. De lo contrario, el depósito es rechazado (el valor *Desechado* es asignado a Std) y no representa una excusa para que V no entregue el bien a C porque el sub-protocolo de reintegro se ha completado con éxito. Entonces, una disputa ocurre entre *V*, *P* y *A*.

El DSRes is preparado por *A* y enviado a *P* para completar el sub-protocolo de depósito.

9) P → A: ID_P, Precio, TID, Stt, $h(OI)$, ID_V, $h(VPSec_{j+1})$

10) A→ P: ID_A, Std, $h(Std, h(OI))$

Después de que una transacción es completada, cada entidad del sistema del sistema de pago coloca en sus listas de revocaciones, los secretos $CVSec_i$ y $CISec_i$ para prevenir que sean utilizados nuevamente por el cliente y el vendedor. En las compras siguientes, el sub-protocolo de registro no se ejecutará hasta que el cliente sea notificado de actualizar el secreto CVSec. Así, cuando sea necesario renovar el secreto, el cliente ejecuta el sub-protocolo de registro para obtener un nuevo CVSec.

Mientras que el secreto no es actualizado, el cliente puede utilizar otros valores en el conjunto CVSeci para realizar transacciones. Para actualizar el secreto VPSec, la Pasasarela de Pago envía el nuevo secreto al vendedor utilizando el protocolo AKE. Finalmente, para actualizar el secreto CISec, el emisor tiene que agregar un mensaje con el nuevo secreto al WSRes que será modificado de la siguiente manera:

$$\{h(OI), Stt, h(VPSec_{j+1}), Newsecret, h(Newsecret)\}_{CISeci}$$

4. ANÁLISIS

Comparación con SAMPP

En esta sección, presentamos una comparación entre SAMPP y nuestro protocolo para establecer las diferencias entre ambos.

La principal diferencia entre ambos protocolos se refiere al ambiente operacional en el cual se utilizan. En SAMPP, el dispositivo móvil tiene acceso al Internet lo que permite al cliente comunicarse con el emisor cuando sea necesario. Nuestro protocolo se basa en la idea del cliente que no se puede conectar directamente con el emisor y en consecuencia, cualquier información o programa que el emisor desea enviar al cliente, tendrá que hacerlo a través del vendedor.

La segunda diferencia está relacionada con los métodos del pago que el cliente puede utilizar durante el proceso de la compra. En SAMPP, solamente se considera el uso de las tarjetas de crédito mientras que en el nuestros, tanto tarjetas de crédito como de débito pueden ser utilizados.

Otra diferencia digna de mencionar es el método de distribución usado para el software del pago. Mientras que en SAMPP el cliente debe descargar el software del emisor o recibirlo a través de un correo electrónico (generalmente, como adjunto al correo enviado por el emisor), en nuestra propuesta el software de pago debe ser enviado del emisor al consumidor a través del vendedor (debido a la imposibilidad del cliente para comunicarse directamente con el emisor usando su dispositivo móvil). Esto nos condujo a la inclusión de mecanismos de seguridad (tales como ofuscación y marcas de agua en el código fuente) que aseguran el programa contra varios tipos de ataques.

La cuarta diferencia se refiere a la protección de la identidad verdadera del cliente. En SAMPP, el cliente siempre utiliza su verdadera identidad durante la compra lo que impide prevenir que el vendedor conozca la identidad de sus clientes mientras que en nuestro protocolo, el cliente utiliza un apodo (solo conocido entre el cliente y el emisor) en lugar de su verdadera identidad a fin de proteger su privacidad.

La última diferencia es el intercambio del secreto compartido entre el cliente y el emisor (CISec). En el caso de SAMPP, al momento de actualizar el secreto CISec, un protocolo AKE (entre el cliente y el emisor) es utilizado mientras que en el nuestro, el nuevo secreto se debe enviar insertado en el script respuesta del reintegro (llamado Withdrawal-script Response).

Seguridad

Seguridad de la Transacción: Nuestro protocolo satisface las siguientes características de seguridad de una transacción:

- *Autenticación de la Entidad:* Que está asegurada por el cifrado simétrico por el secreto CISec (que garantiza que el mensaje es originado por el cliente).
- *Privacidad de la Transacción:* Asegurado por el cifrado Simétrico.
- *Integridad de la Transacción:* Asegurado por el MAC.

Anonimato: Para prevenir que un vendedor conozca la identidad de sus clientes, se utiliza el apodo del cliente (NID_C) en lugar de su verdadera identidad durante una comunicación entre *C* y *V*. Dado que el apodo del cliente es solo conocido por el cliente y el emisor, el vendedor no puede relacionar el apodo con la verdadera identidad del cliente. Así, la privacidad del cliente está protegida e indetectable.

Relación de Confianza: Generalmente, en una transacción, una entidad no debería confiar en otras a no ser que ellos puedan proporcionar una prueba de honradez [6]. Sin embargo, como en nuestro protocolo el emisor emite una tarjeta de débito y/o crédito al cliente y nunca revelará ninguna información relacionada con las tarjetas a otras entidades, declaramos la relación de confianza entre el cliente y el emisor.

5. CONCLUSIONES

En esta investigación se ha propuesto un protocolo seguro que utiliza técnica de criptografía simétrica. Es aplicable a sistemas de pago móvil en donde no existe comunicación directa entre el cliente y el emisor. Así, el cliente se aprovecha de la infraestructura del vendedor y del Portal de Pago para comunicarse con el emisor y comprar de manera segura desde su dispositivo móvil.

Nuestra propuesta representa una alternativa a todos los sistemas de pago móvil donde la conexión entre el cliente y el emisor es obligatoria, incluyendo el esquema Visa 3-D Secure. Además, esta propuesta ilustra como un dispositivo portable equipado con un enlace de corto alcance (como Bluetooth, Infrarojo o Wi-Fi) y poco poder computacional es suficiente para interactuar con la máquina vendedora para comprar mercancía de manera segura.

La técnica de criptografía simétrica utilizada en nuestro protocolo tiene requerimientos computacionales bajos en ambas partes (ya que ninguna operación de clave pública es requerida) y ofrece la posibilidad encargarse de fallas con el protocolo y disputas entre las partes.

Como resultado, se indica que el protocolo propuesto en esta investigación permite a los usuarios móviles tener un sistema de pago seguro y eficiente incluso si la comunicación con el emisor no es posible.

7. REFERENCIAS

[1] Al-Meaither. "Secure electronic payments for Islamic finance", PhD thesis, University of London, 2004.

[2] Bellare, M., Garay, J., Hauser, R., Herzberg, A., Krawczyk, H., Steiner, M., Tsudik, G., Herreweghen, E., and Waidner, M., "Design, implementation and deployment of the *i*KP secure electronic payment system". IEEE Journal on Selected Areas in Communications, 2000, 18(4):611-627.

[3] Chari, S., Chari, S., Kermani, P., Smith, S., and Tassiulas, L., "Security issues in m-commerce: A usage-based taxonomy", In E-Commerce Agents, 2001, pp. 264-282.

[4] Collberg, C., Carter, E., Debray, S., Huntwork, A., Kececioglu, J., Linn, C., Stepp, M., "Dynamic path-based software watermarking", In ACM SIGPLAN 2004 Conference on Programming Language Design and Implementation, 2004, pp. 107-118.

[5] Ham, W., Choi, H., Xie, Y., Lee, M., and Kim, K., "A secure one-way mobile payment system keeping low computation in mobile devices". In The 3rd International Workshop on Information Security Applications (WISA), 2002, pp. 287-301.

[6] Kungpisdan, S., "A secure account-based mobile payment system protocol", In International Conference on Information Technology: Coding and Computing (ITCC), 2004, pp. 35-39.

[7] Lei, Y., Chen, D., and Jiang, Z., "Generating digital signatures on mobile devices", In The 18th International Conference on Advanced Information Networking and Applications (AINA), 2004, pp. 532-535.

[8] Sosonkin, M., Naumovich, G., and Memon, N., "Obfuscation of design intent in object-oriented applications", In ACM workshop on Digital rights management (DRM), 2003, pp. 142-153.

[9] Visa International, "3-d secure mobile authentication scenarios version 1.0", 2002, [Online], Available: http://partnernetwork.visa.com/pf/3dsec/specifications.jsp.

[10] Zheng, X. and Chen, D., "Study of mobile payments system", In IEEE International Conference on Electronic Commerce (CEC), 2003, pp. 24-.