Seguridad en ARAMCEL: Arquitectura basada en agentes móviles para Comercio Electrónico.

Sergio F. Castillo C.
Universidad Industrial de Santander, Escuela de Ingeniería de Sistemas,
Bucaramanga, Colombia,
scastill@uis.edu.co

Luis Antonio León Chacón
Universidad del Valle, Escuela de Ingeniería de Sistemas,
Tuluá, Colombia,
luisleonc@univalle.edu.co

Janeth Gissella Gómez Gualdrón
Universidad Industrial de Santander, Escuela de Ingeniería de Sistemas,
Bucaramanga, Colombia,
nanigiss@yahoo.fr

Abstract

Mobile agents are software entities that they can transport their program code and data from one computer to another through Internet. There are several security risks because as much the mobile agents as the servers with which interact are vulnerable to attacks and breaches of security. In this paper, three problems of security are focused: Authentication, Authorization and No Repudiation. In the context of the Architecture based on Mobile Agents for Electronic Commerce "ARAMCEL" a mechanism of security is presented which proposes a solution to those problems. The security model depends on a central server, reliable servers and the Infrastructure of public key (PKI). ARAMCEL's validation was carried out by means of the prototype ADAM: Application of the mobile agents to the e-commerce.

Keywords: Security, Electronic Commerce, Mobile Agent, Malicious Agent, Malicious Server.

Resumen

Los agentes móviles son entidades software que pueden transportar su código y datos desde un computador a otro a través de Internet. Hay varios problemas de seguridad porque tanto los agentes móviles como los servidores con que interactúan son vulnerables a ataques y brechas de seguridad. En este documento, se enfocan tres problemas de seguridad: Autenticación, Autorización y No Repudio. En el contexto de la Arquitectura basada en Agentes Móviles para Comercio Electrónico "ARAMCEL" se presenta un mecanismo de seguridad que propone una solución a esos problemas. El modelo de seguridad depende de un Servidor Central, servidores confiables y la Infraestructura de llave pública (PKI). La validación de ARAMCEL se realizó por medio del prototipo ADAM: Aplicación de los agentes móviles al comercio electrónico.

Palabras claves: Seguridad, Comercio Electrónico, Agente Móvil, Agente Hostil, Servidor Hostil.

1. Introducción

La aparición y crecimiento de Internet ha variado la forma de vivir y pensar de las personas en la sociedad; de igual forma este cambio ha afectado a las empresas, las cuales han modificado su concepción acerca de la manera de negociar e intercambiar información, bienes y servicios y han ingresado a la economía electrónica. Todo eso ha originado una nueva forma de negocios a través de Internet, llamada Comercio Electrónico (CE) [13].

Actualmente existen en el mercado algunos sistemas para CE, la mayor parte de ellos basados en el modelo Cliente / Servidor (C/S). Bajo este enfoque, cuando un cliente desea obtener un producto ó servicio debe interactuar con el sitio del proveedor, enviando peticiones y recibiendo respuestas, tantas veces como sea necesario para cumplir su tarea, esto incrementa el tráfico en la red, el tiempo invertido para realizar la actividad y los costos de conexión (Figura 1).

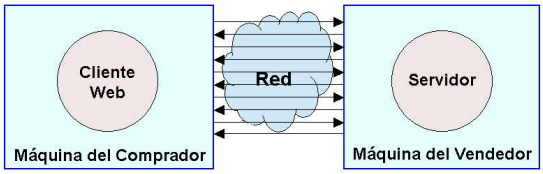

Figura 1. Interacción basada en el modelo C/S.

Buscando la forma de disminuir estos inconvenientes, se ha propuesto el modelo de Agentes Móviles (AM) [7], el cual por sus características disminuye el tráfico en la red, supera los inconvenientes de una conexión intermitente y ofrece soluciones para la poca disponibilidad de tiempo en los usuarios. En la Figura 2 se presenta el tráfico generado en la red por la interacción necesaria para realizar tareas que utilizan recursos que se encuentran ubicados en un equipo remoto, utilizando el modelo de AM.

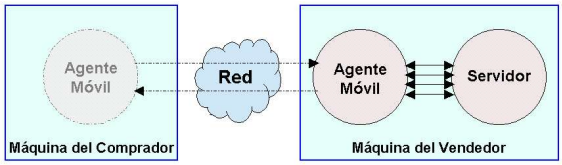

Figura 2. Interacción basada en el modelo de AM.

Para realizar esas tareas un agente móvil cuenta con características que lo hacen autónomo, reactivo y proactivo [2]; además el agente puede representar un usuario dentro de una transacción comercial, puesto que en ellas se requiere la intervención de entidades que negocien o actúen con base en exigencias, necesidades, intenciones, gustos, etc.; en algunos casos la realización de transacciones requiere de acceso en tiempo real a recursos que se hallan distribuidos en la red, es de esta forma que la movilidad de los agentes es una ventaja para realizar aportes en este entorno.

Pero el modelo de agentes móviles también tiene desventajas y se deben a la seguridad [5]. Los agentes móviles se ejecutan en servidores remotos y allí interactúan con otros agentes en la red, por tanto es inevitable que tanto los agentes como los servidores estén sujetos a ataques de entidades hostiles. Estas entidades incluyen agentes hostiles, servidores hostiles e intrusos intentando atacar agentes móviles o servidores, por esa razón el componente de seguridad de ARAMCEL es un aspecto crucial a tener en cuenta durante el desarrollo de sistemas basados en agentes móviles.

Por las razones mencionadas anteriormente surge la arquitectura ARAMCEL, que pretende apoyarse en el modelo de agentes móviles para dar una solución a esas necesidades. ARAMCEL ha sido propuesta como Tesis de Maestría en Informática en la Universidad Industrial de Santander y su objetivo general es considerar los principales problemas relacionados con la seguridad requerida en un contexto de Comercio Electrónico y así permitir el desarrollo de aplicaciones en ese campo. Para comprender ARAMCEL, en las siguientes secciones se hace una descripción de los componentes, funcionamiento, amenazas de seguridad, así como el modelo de seguridad y la solución propuesta a las amenazas mencionadas.

1. ARAMCEL: Arquitectura basada en el modelo de Agentes Móviles para Comercio Electrónico.

ARAMCEL (Figura 3) es una arquitectura que permite realizar transacciones de Comercio Electrónico utilizando el modelo de Agentes Móviles. La especificación de ARAMCEL está basada en el lenguaje de programación JAVA, en los conceptos del modelo de AM y en las necesidades presentes en un entorno de Comercio Electrónico.

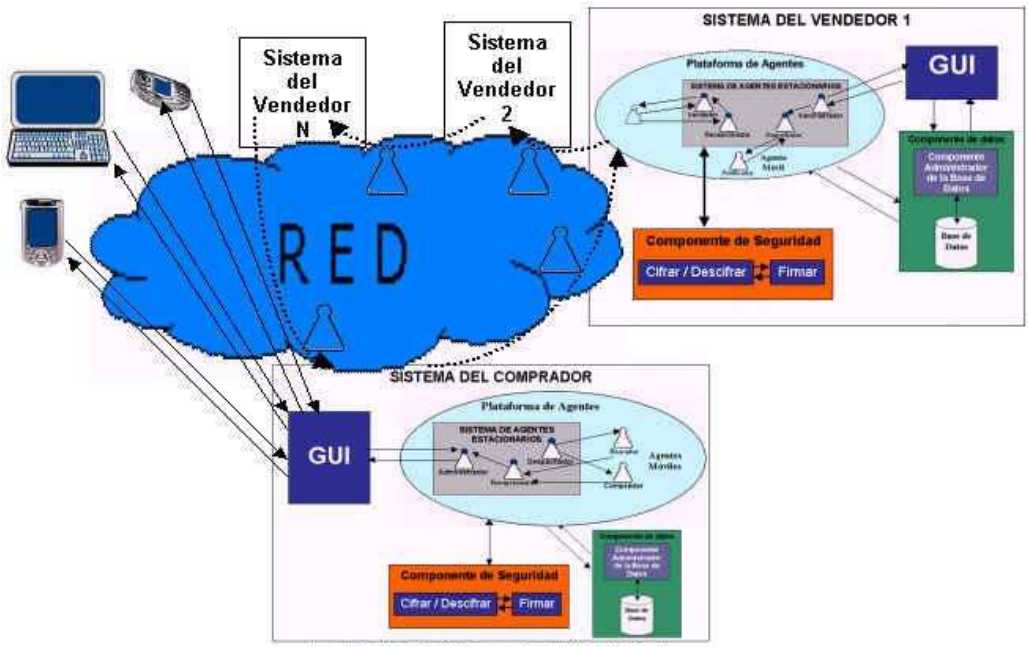

Figura 3. Arquitectura ARAMCEL.

1.1. Descripción de ARAMCEL.

En la Arquitectura ARAMCEL se utiliza el modelo de negocios en el cual el Comprador, con base en sus requerimientos, envía agentes móviles que acceden a los productos ofrecidos por el Vendedor. ARAMCEL está distribuida en dos sistemas definidos, el Sistema del Comprador y el del Vendedor.

1.1.1. Sistema del Comprador

El sistema del Comprador está conformado por la interfaz gráfica de usuario, la plataforma de agentes, el componente de seguridad y el componente de datos (Figura 4).

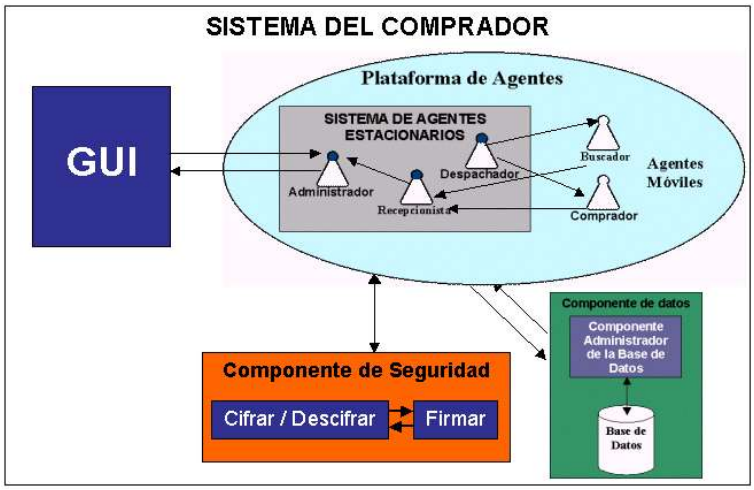

Figura 4. ARAMCEL - Sistema del Comprador.

El sistema del Comprador se encuentra instalado en un equipo denominado Servidor de Compradores (SC), al cual acceden los usuarios Compradores por medio de la interfaz de usuario. Un Comprador puede acceder al sistema desde cualquier dispositivo que posea conexión a la red (computador, asistente digital personal, celular, computador portátil, etc.). Los usuarios previamente registrados, sólo necesitan un navegador para Internet, mediante el cual se conectan al SC y pueden usar el sistema.

A continuación se hace una descripción de cada uno de ellos.

- *Interfaz Gráfica de Usuario (GUI):* Permite que el usuario ingrese información al sistema; esta información corresponde a requerimientos, preferencias sobre artículos y demás datos que sean necesarios. Además se utiliza como medio para mostrar al usuario la información que los agentes han encontrado.

- *Plataforma de Agentes*: En ella se encuentra el Sistema de Agentes Estacionarios y los agentes móviles. Los agentes estacionarios son aquellos que permanecen en la máquina del Comprador y cumplen funciones como el despacho de agentes a los sitios de los Vendedores y la recepción de los agentes móviles cuando retornan con la información que han recolectado. Los Agentes Móviles son agentes creados para la búsqueda y compra de artículos, llevan la información de las preferencias del usuario sobre los artículos que desea y el itinerario con los sitios a visitar.

- Componente de Seguridad: Este componente está subdividido en dos módulos, el primero se encarga del cifrado y descifrado de los datos y el segundo de los procesos de firmado y verificación de firmas. Este componente es utilizado por el Agente Despachador para solicitar el cifrado y firmado de la información que va a transportar el agente móvil. También es usado por el Agente Estacionario Recepcionista del Comprador para verificar la firma del Vendedor y descifrar la información que se recibe del agente móvil.

- *Componente de Datos:* Este componente está conformado por la Base de Datos y el Componente Administrador de la Base de Datos. La primera contiene la información relacionada con las solicitudes del Comprador y el resultado de los procesos realizados por el Agente Móvil; también se almacena una lista con las direcciones de los sitios de los Vendedores y el tipo de artículos que ofrecen, ese listado es usado para la generación del itinerario del agente móvil. El Componente Administrador de la Base de Datos es el encargado de realizar las consultas y modificaciones a la información almacenada en ella.

1.1.2. Sistema del Vendedor

El sistema del Vendedor contiene la interfaz gráfica de usuario, la plataforma de agentes, el componente de seguridad y el componente de datos (Figura 5). El nombre de los componentes es el mismo que en el sistema del Comprador, pero cambia la funcionalidad en algunos de ellos como se describe a continuación.

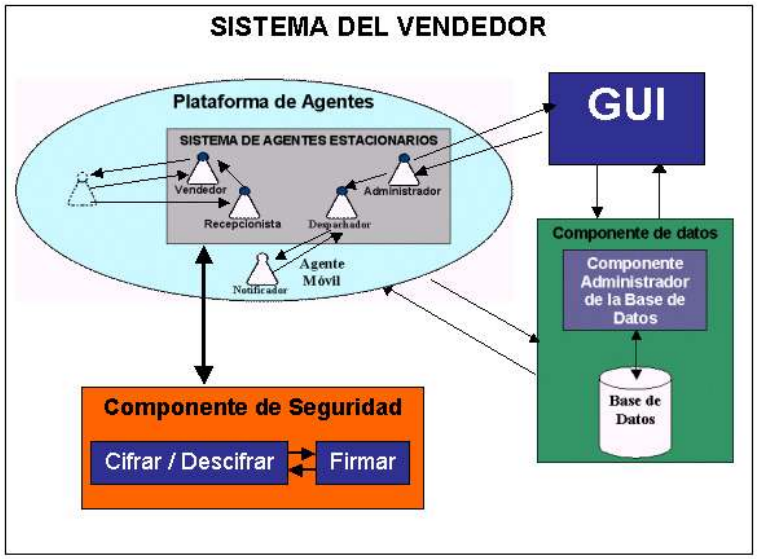

Figura 5. ARAMCEL - Sistema del Vendedor

- *Interfaz Gráfica de Usuario (GUI):* Permite al usuario (dueño o administrador del sitio del Vendedor) realizar modificaciones en los datos existente en ese sitio y obtener la información de las transacciones comerciales realizadas.

- *Plataforma de Agentes:* Entre los agentes estacionarios de esta plataforma, se encuentra el agente Recepcionista, encargado de asignar un agente Vendedor que interactúe con el agente móvil que hace una consulta o solicita una compra. El agente Despachador es el que crea y envía al Agente Notificador, éste es un agente móvil del Vendedor que se encarga de informar a los Compradores sobre las ofertas vigentes en el sitio, nuevas adquisiciones y demás mensajes que desee enviar el Administrador de la tienda.

- *Componente de Seguridad:* Al igual que en el sistema del Comprador, está subdividido en dos módulos, el primero se encarga del cifrado y descifrado de los datos y el segundo de los procesos de firmado y verificación de firmas. Este componente es utilizado por el Agente Vendedor para el procesamiento de la información recibida del agente móvil del Comprador y la que a su vez va a ser entregada dentro del proceso de venta; además tiene la función de revisar la integridad de los agentes.

- *Componente de Datos:* Esta conformado por la base de datos que contiene la información referente a los artículos que ofrecen en ese sitio, ventas realizadas y ofertas; y por el Administrador de la base de datos que permite realizar consultas y modificaciones a la información almacenada en ella.

1.2. Funcionamiento de ARAMCEL

Para realizar las transacciones de Comercio Electrónico, ARAMCEL representa los componentes y la interacción entre ellos, donde un Usuario Comprador puede enviar un agente para que lo represente e interactué con otros agentes en sitios remotos de la red y así obtener el artículo que busca. Los siguientes numerales dan una breve descripción del funcionamiento de ARAMCEL.

Sistema del Comprador.

Para ingresar al Sistema del Comprador, el usuario se conecta a la GUI utilizando un protocolo de comunicación segura y solicita el inicio de sesión; para esto debe ingresar su nombre de usuario "*login*" y la clave de acceso "*password*".

Una vez que sea válida la entrada, el Usuario puede hacer búsquedas en la red de los artículos que quiere. El sistema mediante sus agentes móviles toma la información de los artículos y las preferencias del Usuario, como puede ser el tiempo de entrega del artículo, costo, cantidades de unidades, etc.; cuando se tienen todos los datos, los agentes se desplazan a través de la red a cumplir con la búsqueda de información y cuando la recolectan, regresan a su sitio de origen a reportar los resultados obtenidos.

El Usuario Comprador puede finalizar su sesión en el sistema y después reconectarse, para revisar el listado que contiene los resultados que trajeron los agentes; con base en esa información, puede dar la orden de crear un agente móvil Comprador que viaje al sitio elegido y procese la orden de compra.

Sistema del Vendedor.

En el caso de los sitios correspondientes a cada Vendedor, los agentes estacionarios son los encargados de interactuar con los agentes móviles buscadores de información y con aquellos que llegan a realizar procesos de compra.

La GUI de este sitio permite al propietario o administrador verificar los artículos existentes, obtener información de ventas realizadas, crear ofertas, actualizar precios, modificar la cantidad de artículos cuando llega nuevo inventario y realizar promociones.

1.3. Transacciones básicas en ARAMCEL

Las transacciones corresponden a los procesos de Comercio Electrónico que se realizan en ARAMCEL, como son la búsqueda y compra de artículos. A continuación se describen de manera general los pasos presentes en cada una de ellas.

Búsqueda de información.

- El Usuario Comprador (UC) hace una solicitud de artículos a través de la Interfaz Gráfica de Usuario (GUI).
- El Agente Estacionario Administrador del Comprador (AEAC) procesa la petición y le entrega los datos de los artículos y las preferencias suministradas por los usuarios al Agente Estacionario Despachador del Comprador (AEDC).
- El AEDC con esos datos crea un Agente Móvil Buscador (AMB) por cada artículo de la lista, con las respectivas preferencias.
- El AMB solicita al AEDC información de sitios de Vendedores que ofrezcan el tipo de artículo que necesita. Esos sitios son evaluados por medio de un puntaje que los clasifica con base en la calidad del servicio prestado.
- El AMB viaja siguiendo un itinerario que ha formado con base en los sitios recibidos.
- Al llegar al sitio del Vendedor el AMB establece comunicación con el Agente Estacionario Recepcionista del Vendedor (AERV).
- El AERV le asigna un Agente Estacionario Vendedor (AEV) para que interactúe con el AMB.
- El AMB solicita el artículo al AEV y espera la cotización que incluye precio, cantidad y tiempo de entrega del artículo.
- El AMB almacena la oferta recibida, si cumple con las preferencias del UC, y continua su recorrido.
- Una vez que haya finalizado el itinerario, el AMB retorna a su sitio de origen y reporta al AERC los resultados obtenidos en su viaje.

Compra de Artículos

- El UC a través de la GUI revisa los resultados de las búsquedas de artículos y decide cuales comprar.
- El AEAC toma la información de los artículos que desea comprar el UC y la envía al AEDC.

- El AEDC crea un Agente Móvil Comprador (AMC) por cada artículo.
- Cada AMC viaja al sitio donde se encuentra el artículo seleccionado por el UC.
- El AMC llega y el AERV le asigna un AEV que recibe la solicitud del artículo y entrega los resultados.
- El AMC envía el código de pago y solicita el código de aceptación al AEV.
- El AEV entrega el código de aceptación al AMC, quien regresa al origen a entregar los resultados al AERC.

Estas transacciones corresponden a un escenario sin inconvenientes de seguridad. En la siguiente sección se presentan las amenazas de seguridad que se pueden manifestar al realizar una transacción de búsqueda o una compra en sitios remotos.

2. Amenazas de seguridad en ARAMCEL

La movilidad de agentes y la interacción con otras entidades en la red, hace surgir unos requerimientos de seguridad en ARAMCEL que pueden ser clasificados en dos categorías. La primera de ellas se refiere a los problemas de seguridad que se presentan en el modelo de los Agentes Móviles y la segunda los aspectos que se requieren para garantizar la seguridad en un entorno de Comercio Electrónico. Los siguientes numerales detallan cada una de las categorías mencionadas.

2.1. Amenazas de Seguridad Inherentes al Modelo de Agentes Móviles.

La seguridad ha sido tradicionalmente un inconveniente en los sistemas informáticos, pero el modelo de agentes móviles por sus características presenta un nuevo tipo de inconvenientes de seguridad. Los dos problemas principales son [8, 12, 13]:

El Problema del Agente hostil.

Cuando los agentes móviles de ARAMCEL llegan a cada sitio de su itinerario, necesitan algunos permisos de usuario para poder ejecutar su código. Tradicionalmente el control de acceso a los equipos de una red se hace por medio de contraseñas, en donde cada usuario se autentica al inicio con su *login* y su *password*; pero este esquema funciona para sistemas estáticos y no para agentes móviles, puesto que el agente debe llevar una contraseña para cada sitio de su itinerario, lo que aumenta su tamaño y así mismo incrementa los requerimientos de seguridad para poder proteger esas contraseñas.

Entre los agentes puede existir agentes hostiles que realizan acciones perjudiciales, como el acceso no autorizado, alteración de los recursos locales (datos y llamadas al sistema), sobrecarga de esos recursos o incluso daños a la integridad del servidor. En la figura 6 se presenta un agente hostil que llega a un sitio y ha sido diseñado para realizar labores que atentan contra la integridad del servidor, como es la utilización no autorizada de los recursos para obtener información privada.

Figura 6. Agente Hostil.

El problema del agente hostil ha generado tres tipos de amenazas a los servidores, las cuales se detallan a continuación:

- *El acceso no autorizado a los recursos.* Cuando un agente móvil llega a cada sitio de su itinerario, ejecuta su código usando los recursos del computador del Vendedor. Por esta razón, los recursos de la máquina receptora están expuestos al ataque de un agente hostil, puesto que si no existen los mecanismos de control apropiados, ese agente podría acceder a información privada del sistema. En el caso del Comercio Electrónico, la información que almacenan los Vendedores está relacionada con sus datos comerciales, de esa forma, si un agente accede a ella puede alterarla y tomar ventaja de su contenido para fines ilegales.

- *Sobrecarga de los recursos del servidor.* Es necesario proveer medidas de seguridad adecuadas para prevenir el consumo excesivo de recursos por parte de agentes hostiles, puesto que al sobrecargar el servidor hace que el tiempo de respuesta se incremente o que no haya respuesta a los agentes de los demás Compradores que buscan acceder a la información. En el caso particular de ARAMCEL los sitios de los vendedores son clasificadas con

base en su servicio mediante un puntaje, por lo tanto el problema mencionado podría ocasionar la reducción de esa valoración.

- *Creación de agentes residentes en el sitio del Vendedor.* Otro de los ataques de los cuales puede ser víctima un servidor por parte de un agente hostil, es la creación de otros agentes que residan en el servidor. Con esos nuevos agentes puede suceder cualquiera de los dos ataques anteriormente mencionados, ó que se creen tantos agentes que también sobrecarguen los recursos. En la mayor parte de los sistemas de Comercio Electrónico actuales se utiliza un agente "esclavo", creado por el agente móvil, para que resida en el sitio del Vendedor y asegure la reserva de un producto; este proceso no se realiza de la misma forma en ARAMCEL, en secciones siguientes se explicará el proceso utilizado.

La solución tradicional al problema del agente hostil se realiza por medio de restricción de privilegios a los agentes, pero eso puede ocasionar que los agentes sean incapaces de lograr sus metas, por lo tanto es necesario buscar mecanismos alternos que provean seguridad y permitan la realización de las transacciones.

El problema del servidor hostil

Un servidor hostil es una máquina que intenta espiar ó manipular el código, los datos o el control de flujo del agente, proporciona llamadas falsas al sistema, ejecuta código del agente incorrectamente, invierte la ingeniería y manipula su código ó los secretos comerciales; puede hacerlo mediante la clonación del agente, proporcionando información errónea ó interceptando el agente. Un ejemplo del ataque de un servidor hostil a un agente móvil puede observarse en la figura 7.

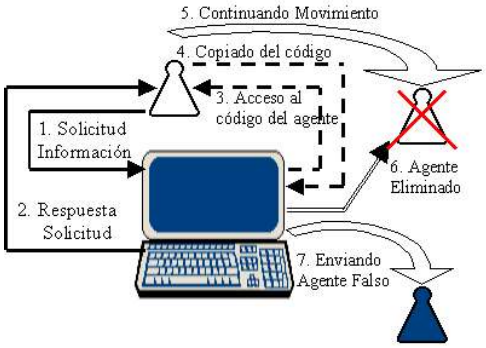

Figura 7. Servidor Hostil.

Cuando un agente móvil llega a un determinado sitio, ya no depende de su máquina de origen, por el contrario, la máquina receptora debe instanciar la clase que dio origen al agente, leer el estado de datos que se encuentra serializado y ejecutarlo dentro de ella, por lo cual el código y datos del agente móvil quedan totalmente expuestos. Los ataques de Servidores contra agentes son de diversos tipos y pueden resumirse como sigue:

- *Clonación del Agente*. Uno de los ataques al agente móvil consiste en que un servidor captura y construye una réplica de él, de esa manera, se hace pasar por el agente original pero para los propósitos que ese servidor programa. En el caso del Comercio Electrónico un Vendedor puede clonar un agente para enviarlo a buscar información privada y de esa forma acceder a los secretos comerciales de sus competidores.

- *Negación de servicio.* Los ataques de negación del servicio pueden ser de dos tipos, el primero ocurre cuando el servidor impide que el agente continúe su itinerario, el segundo consiste en permitir al agente continuar, pero no al sitio que tiene determinado en el itinerario, sino a aquel que el servidor elige. Este segundo tipo de ataque es frecuente en los sistemas de Comercio Electrónico, puesto que evita que el agente vaya al sitio del competidor y puede enviarlo al de un socio ó a otra sucursal del mismo Vendedor.

- *El ataque del hombre en el medio*. Un agente móvil puede ser interceptado y modificado mientras se desplaza de un servidor a otro. La forma de realizarlo es utilizando un programa denominado "monitor de comunicación" que se encarga de observar los mensajes intercambiados por los sistemas de agentes para extraer o modificar la información o el código de los agentes. Con este tipo de ataque un Vendedor hostil puede espiar o alterar los datos que los demás Vendedores han entregado al agente.

- *Modificación de los datos que lleva el agente*. Cuando un servidor ejecuta un agente móvil puede observar su contenido, por esta razón, si no se establecen los mecanismos de seguridad necesarios, un Vendedor hostil puede modificar los datos que le han sido entregados por otros Vendedores al agente y de esa forma competir deslealmente.

2.2. Principales problemas del Comercio Electrónico

Con el auge de Internet y las comunicaciones aparecen avances en el desarrollo tecnológico que buscan aumentar la competitividad empresarial; en el caso del Comercio Electrónico, el modelo de agentes móviles ofrece grandes oportunidades para realizar transacciones. Así mismo se encuentran en el mercado sistemas basados en agentes móviles, se cuenta con estándares, plataformas y productos que facilitan su desarrollo, pero aún el Comercio Electrónico no ha llegado al auge esperado; una de las razones para que esto suceda son los problemas de seguridad existentes [1]. Por eso se hace necesario buscar soluciones para minimizar el riesgo al realizar transacciones de Comercio Electrónico y la manera de lograrlo es implementar los siguientes aspectos de seguridad [4]:

Autenticación.
Asegura que el escritor de un documento o el remitente de un mensaje es quién dice ser. Para lograr esta autenticación están surgiendo métodos de gran importancia que conducen a un manejo efectivo de la seguridad y la confidencialidad. Algunos de los métodos utilizados son: la Identificación Biométrica, los Documentos de Identificación y la Información Confidencial.

En la autenticación mediante información confidencial se utiliza una combinación de caracteres como contraseña, donde sólo el usuario y el proveedor de ella pueden conocerla o se utiliza una firma digital. Una firma digital es una identificación electrónica, creada por medio de un computador para representar a la persona o entidad, con el mismo efecto legal que tendría una firma hecha a mano.

Autorización.
Asegura que el usuario que va acceder a la información posee los permisos de seguridad necesarios, por tanto la información en la red permanece privada. Se puede cumplir usando métodos matemáticos complejos para realizar procesos como el de cifrado y descifrado.

No-repudio.
Asegura que ninguno de los implicados en la transacción puede negar su participación en ella, así mismo, los participantes no podrán rechazar las obligaciones contractuales adquiridas en el negocio; el creador del mensaje no puede negar que lo envió, y el receptor del mensaje no puede negar que lo recibió. Este aspecto es útil principalmente por razones comerciales y legales. Hay dos clases de No-Repudio:

- *De origen*: Provee al receptor del mensaje con la prueba de su origen, la cual podrá emplearse para defenderse de la negación del emisor sobre el envío del mensaje. Actualmente se está empleando la firma digital para evitar el no-repudio del emisor, la firma es anexada al mensaje enviado.

- *De recepción*: Provee al emisor del mensaje con la prueba de su entrega, la cual podrá ser empleada para defenderse de la negación del receptor. Para evitar el no-repudio del receptor actualmente se está optando por incluir una entidad, es decir, una tercera parte confiable, que en la mayoría de los casos es una autoridad de certificación, que actúa como "notario" dentro de la transacción y verifica la recepción del mensaje.

Confidencialidad.
Asegura que ninguna entidad ajena a la transacción pueda acceder a los datos que utilizan, de la misma manera los actores (personas, programas, procesos, etc.) de esa transacción tan sólo conocerán aquella información necesaria para su realización.

Integridad.
Asegura que un mensaje no ha sido modificado mientras es transportado. En Comercio Electrónico, el contenido de una transacción no debe ser alterado por alguna de las partes implicadas en ella, ni por una tercera parte no involucrada inicialmente; así mismo, la transacción debe poder ser perfectamente reconstruible frente a terceros en caso de disputas legales. Una forma para lograrlo es mediante el uso de firmas digitales con criptografía de llave pública, en las cuales es necesario registrar la llave pública antes de la transacción.

3. El Modelo de Seguridad en ARAMCEL

Dada la amplitud del problema de seguridad, en ARAMCEL se seleccionaron los aspectos de seguridad autenticación, autorización y no-repudio como los más relevantes en esta investigación. Esos problemas de seguridad se pueden resolver con la ayuda de técnicas para el cifrado de información. Hay dos esquemas para realizar ese cifrado:

- *Esquema común*: En este esquema la misma llave es guardada secretamente, se usa para el cifrado y descifrado de la información, se le llama cifrado simétrico. En este caso el autor del mensaje debe utilizar la clave para cifrarlo y el destinatario debe poseer esa misma clave para poder descifrarlo.

- *Esquema de llave pública*: En este esquema se usan llaves diferentes para el cifrado y descifrado, se denomina cifrado asimétrico, una llave se guarda confidencialmente y la otra es pública. El término utilizado para referirse a la infraestructura de seguridad creada con base en criptografía de clave o llave pública es PKI (Public Key Infrastructure) [6, 11]. PKI también permite la gestión de certificados digitales, donde un certificado es un documento firmado digitalmente por una persona o entidad confiable denominada Autoridad de Certificación (CA), que enlaza cierta información perteneciente a un sujeto con su llave pública para poder asegurar que la entidad con que se está tratando es quién dice ser.

En ARAMCEL, para encontrar una solución se utiliza la infraestructura de llave pública (PKI); PKI tiene la ventaja de no tener que compartir información confidencial entre las entidades involucradas en el intercambio de información, además permite realizar la autenticación de mensajes puesto que si una llave se utiliza para cifrar un mensaje sólo se puede descifrar con la otra.

Es importante aclarar que dentro de las políticas de ARAMCEL se tiene que los Vendedores y Compradores deben estar registrados para poder acceder al sistema, de esta forma un componente Administrador dentro del Servidor Central actúa como entidad de certificación expidiendo las llaves correspondientes y entregando la información que tanto Vendedores como Compradores deben tener. Cada sitio en ARAMCEL posee una llave privada y una llave pública, así mismo tiene acceso a las llaves públicas de los demás sitios, de esa manera los datos de respaldo generados durante la transacción son cifrados y firmados por el emisor.

Por ejemplo, el Comprador A posee una llave pública CP y una llave privada CR, el sitio del Vendedor N posee una llave pública VP y una llave privada VR. De esta forma, si un agente es enviado a realizar una transacción llevará cifrada la información que debe entregar al Vendedor, con la llave pública del Vendedor, por lo tanto, únicamente la llave privada correspondiente puede ser usada para leer la información cifrada por esa llave pública, como se muestra en la figura 8. La utilización de estas llaves ayudan a autenticar al creador de un mensaje.

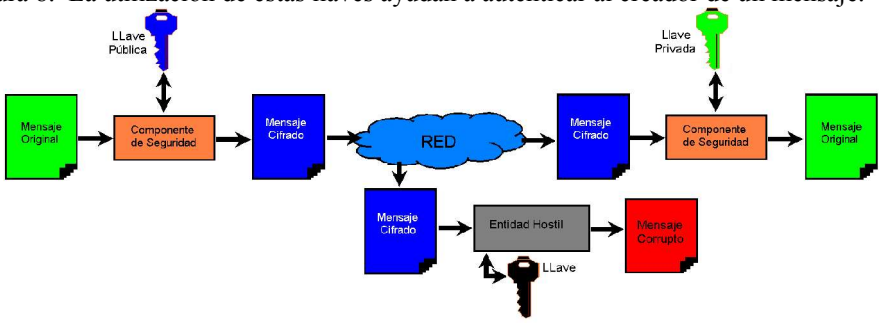

Figura 8: Esquema de Cifrado / Descifrado.

3.1. Autenticación

El esquema de autenticación de ARAMCEL se basa fundamentalmente en la firma digital. Cuando un Comprador envía un agente a realizar un proceso de búsqueda, este lleva consigo el identificador del usuario, cifrado con la llave privada del Comprador. Este esquema proporciona gran versatilidad y resuelve el problema de autenticación, además presenta una gran ventaja al utilizarlo para autentificar los agentes móviles, ya que cuenta con la certeza que la información no ha sido alterada y se sabe con seguridad quién los envía. Para realizar la autenticación, los agentes móviles de ARAMCEL han sido divididos en cuatro partes como se muestra en la Figura 9, donde cada una de ellas está diseñada para apoyar el protocolo de seguridad. A continuación se presenta su descripción:

- La identidad del sitio del comprador (C_Id) que lo creó.
- Una cabecera que contiene el identificador del agente (A_Id) y el resultado de una función HASH [9, 10] aplicada al código. Esos valores están cifrados con la llave privada del Comprador, de tal manera que sólo utilizando la llave pública de ese Comprador pueden ser descifrados.
- El código del agente puede verificarse mediante una función HASH, el resultado de ella se compara con la que lleva cifrada en la cabecera para indicar que ese agente proviene de un sitio confiable y no ha sido modificado.
- Los datos cifrados que el agente recoge de los diferentes Vendedores a lo largo de su itinerario.

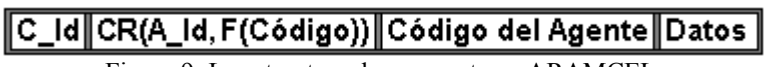

Figura 9: La estructura de un agente en ARAMCEL.

El uso de llaves y certificados es crucial para la autenticación, por ello ARAMCEL fortalece la seguridad con base en los conceptos de la clase de Java llamada *Keystore* [10] que representa una colección en memoria de llaves y certificados. Esa clase maneja dos tipos de entradas:

- *Llave:* este tipo de entrada del keystore maneja una llave confidencial de cifrado, la cual es almacenada en un formato protegido mediante una contraseña para evitar el acceso no autorizado. Generalmente, una llave almacenada en este tipo de entrada es una llave secreta o una llave privada acompañada por un certificado que corresponde a la llave pública. Las llaves privadas y los certificados son usados para que una entidad se auto autentique.

- *Certificado confiable:* este tipo de entrada contiene un certificado con una llave pública perteneciente a otra entidad. Es llamado un certificado confiable porque el propietario del keystore asegura que la llave pública dentro de ese certificado realmente pertenece a la entidad identificada en el certificado como el propietario de la llave.

Por seguridad se tiene una contraseña para todo el contenido y además cada entrada en el keystore se protege por una contraseña diferente.

3.2. Autorización

Los Agentes Móviles que llegan a cada sitio se consideran no confiables y dentro del archivo de políticas de seguridad se establece que los agentes sólo tienen acceso al envío de mensajes; de esa forma se asignan permisos que restringen a los agentes evitando acciones hostiles pero con la capacidad suficiente para interactuar con el sistema. Es necesario ser un usuario Comprador o Vendedor autorizado por el sistema con sus respectivas llaves públicas y privadas para cifrar o descifrar información; sólo quién esté autorizado, puede realizar el proceso de descifrado de la cabecera del agente y reconocer si ese agente pertenece a un usuario. Una vez el agente ha sido autenticado, se le autoriza para que use los recursos establecidos para él, con base en las políticas de seguridad del sistema.

Para el proceso de compra se requiere la previa autenticación tanto del agente Vendedor como del agente Comprador; el código de pago que lleva el agente Comprador va cifrado con la llave pública del Vendedor, para que sólo el Vendedor autorizado pueda usarlo; el código de aceptación de la transacción, va cifrado con la llave pública del Comprador para evitar que usuarios compradores no autorizados usen el código.

3.3. No-Repudio

En ARAMCEL, se utilizan las firmas digitales para evitar el repudio de origen y recepción. Cuando el agente móvil entrega el identificador de su usuario y el código de pago cifrado y firmado, está entregando la prueba que acredita que el Comprador envió el agente y ordenó la compra, de esa forma se evita el repudio de origen. Por su parte, cuando el Agente Vendedor, entrega el código de aceptación de la transacción, cifrado y firmado, se puede verificar que el Vendedor aceptó la transacción y por tanto se evita el repudio de recepción.

3.4. Solución al problema del Agente hostil

El lenguaje de programación Java [10] provee funcionalidades que permiten implementar políticas de seguridad basadas en un mecanismo de autenticación y autorización; en ARAMCEL, los permisos de archivos restringen al agente el uso de recursos en el computador del Vendedor, al igual que las operaciones que esos agentes pueden realizar. Además en ARAMCEL el sistema del Comprador que crea el agente, le añade una cabecera que contiene el identificador del propietario y cifrados con la llave privada del Comprador, el identificador del agente y el resultado de una función aplicada al código. Cuando un agente llega al sitio del Vendedor, la identidad del Comprador se verifica al aplicarle la llave pública del Comprador. El descifrado autentica al Comprador y revela la identidad del agente; en caso de no realizarse el descifrado de la cabecera del agente Comprador o si el agente intenta exceder su límite de permisos mientras se ejecuta, el Vendedor aborta la ejecución del agente y reporta al Servidor Central el ataque.

El Servidor usa las características de seguridad para definir los privilegios apropiados y restringir el acceso del agente a los recursos del sistema. Además ARAMCEL no permite la creación de agentes residentes, puesto que para reservar un artículo es suficiente con la cotización entregada y cifrada con la llave privada del Vendedor y nuevamente cifrada con la llave pública del Comprador. Los Servidores son protegidos de los agentes hostiles, pero los agentes aún están expuestos a ataques; utilizando las opciones de seguridad, un agente solicita cierto nivel de protección, pero esa solicitud depende del servidor en el cual está ejecutándose. Por tanto, no es posible para los agentes, protegerse de servidores hostiles que ignoran los parámetros de protección pedidos por ellos; se requieren técnicas adicionales para proteger a los agentes de esos servidores hostiles.

3.5. Solución al problema del Servidor hostil

Los agentes Compradores que llegan al sitio de un Vendedor ejecutan su código dentro de esa máquina, exponiéndose al problema del servidor hostil. En ARAMCEL, cada sitio de un Vendedor se encuentra en una lista de servidores confiables que están dentro del SC y han sido previamente acreditados por el sistema. Además, con la ayuda de PKI las entidades certificadas por el Servidor Central tendrán el par de claves necesarias para el cifrado y descifrado de mensajes y datos con los agentes. En caso que un servidor trate de modificar los datos o el código del

agente, se verifica por medio de la información contenida en la cabecera del agente; en ese caso el agente es tratado como hostil y eliminado por el sistema donde se encuentre. Si un agente desaparece cuando recorre el itinerario, ARAMCEL permite el envío de un agente móvil Fiscalizador que sigue el mismo recorrido y envía mensajes cuando llega y sale de cada servidor, para informar al sistema el sitio donde ocurrió el ataque.

Al encontrar un sitio hostil inmediatamente el Servidor Central lo marcará como No Confiable y será eliminado de la lista de sitios posibles para viajar, en caso de no encontrarlo los agentes móviles que tengan que pasar por esos sitios serán acompañados por agentes fiscales, durante la cantidad de viajes que el Administrador del Servidor Central con base en su autonomía considere necesario.

3.6. Protocolo de Seguridad

Los aspectos más relevantes del protocolo se presentan en la figura 10 y su proceso, en forma general, se describe a continuación.

Cuando el Agente Móvil del Comprador (AMC) llega al dominio del Vendedor solicita la asignación de un agente vendedor y recursos en el servidor. Antes de cumplir con la solicitud, el Agente Estacionario Recepcionista del vendedor (AERV) lee los datos del agente y se los envía al Componente de Seguridad, para que realice la autenticación del agente y del Usuario Comprador. El Componente de Seguridad busca el certificado digital del comprador y extrae la Clave Pública, confirma la existencia del usuario y revisa la integridad del código del agente; descifra el A_Id y la F(código), aplica la función Hash al código del agente y compara la función obtenida con la descifrada. Cuando el AMC es autenticado, se le asignan recursos y un Agente Estacionario Vendedor (AEV); con este último, el AMC realiza la interacción del proceso de Compra / Venta.

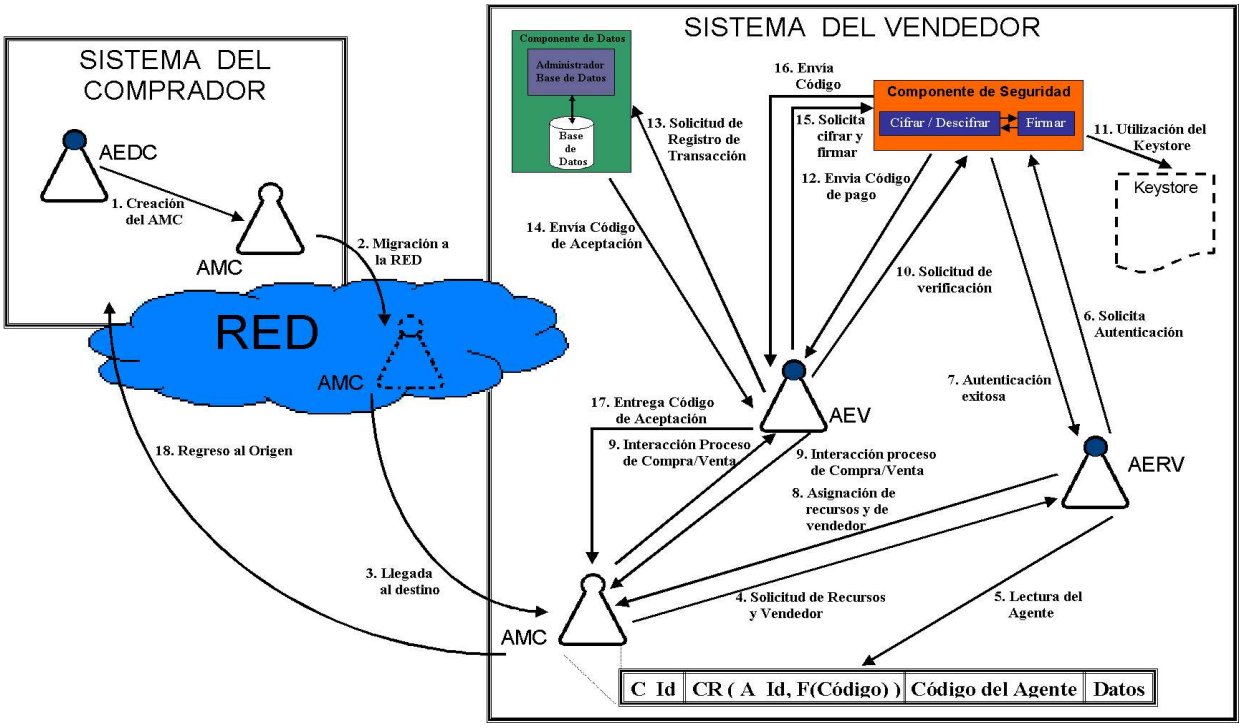

Figura 10. Protocolo de seguridad en ARAMCEL.

El AMC entrega el código de pago, cifrado y firmado al Agente Estacionario Vendedor (AEV). El AEV envía el código de pago al Componente de Seguridad y le solicita la verificación de la firma. Ese componente utiliza la información almacenada en el Keystore para descifrar el código de pago y verificar la firma; después de esto, devuelve el código de pago descifrado al AEV. Este último hace la solicitud de registro de la transacción al Componente de Datos, el cual genera y almacena el código de aceptación y envía al AEV. A su vez el AEV solicita al Componente de Seguridad el cifrado y firmado del código, cuando esto se ha llevado a cabo, el código es entregado al AMC, quién regresa a su origen.

La validación de este trabajo de investigación se realizó por medio del prototipo ADAM: Aplicación de los agentes móviles al comercio electrónico [3], al cual se le hicieron pruebas de verificación, validación y rendimiento.

Conclusiones

Los agentes móviles debido a las ventajas que poseen presentan fortalezas para trabajar de manera eficiente en sistemas distribuidos, pero también tienen inconvenientes de seguridad; los cuales son una oportunidad al generar un campo de acción en investigación para generar soluciones.

Con ARAMCEL se presenta una propuesta para crear aplicaciones que con base en las especificaciones dadas, aprovechen las ventajas de los agentes en el Comercio Electrónico; así mismo, ARAMCEL pretende dar un aporte a las necesidades de un mundo en proceso de globalización y que a su vez provea un entorno seguro de ejecución para ese tipo de sistemas.

A lo largo de este artículo, se han discutido las amenazas de seguridad existentes en un sistema para Comercio Electrónico basado en agentes móviles, los problemas del agente hostil y servidor hostil. Con base en esos ataques, en los aspectos de seguridad autenticación, autorización y no-repudio y en PKI se presentó el modelo de seguridad de ARAMCEL que ofrece una solución a esos problemas.

Aunque se ha ofrecido una solución a algunos de los problemas de seguridad, existen otros que son objeto de investigación en el mundo, además de aquellos que se presenten a medida que los sistemas basados en agentes móviles para Comercio Electrónico se hagan más frecuentes. Sin embargo, considerando las características del modelo de seguridad presentado es posible extenderlo y enriquecerlo para contrarrestar nuevos tipos de ataques que surjan en el entorno.

Agradecimientos

El segundo autor desea expresar su agradecimiento por la colaboración y apoyo recibido de la Universidad del Valle - Sede Tuluá.

Referencias

[1] Dávila, J. El Comercio Electrónico todavía está por llegar. Asociación Española de Criptología y Seguridad de la Información. España. 2000.

[2] Desouza, K. Intelligent Agents for Competitive Intelligence: Survey of Applications. University of Illinois at Chicago. US. 2001

[3] Gómez, J.; Castillo, S. (Director) y León, L. (Codirector). ADAM: Aplicación de los Agentes Móviles al Comercio Electrónico. Tesis de Pregrado (Ingeniería de Sistemas). Universidad Industrial de Santander. Colombia. 2004.

[4] Hidekazu, T. Security Technology for Electronic Commerce. Electronic Commerce Promotion Council. Japan. 2000.

[5] Jansen, W. and Karygiannis, T. Mobile Agent Security. National Institute of Standards and Technology. Computer Security Division. US. 1999.

[6] Kabay, M. A Primer on Public Key Infrastructures. Program Master of Science in Information Assurance. Division of Business & Management. Norwich University. US. 2004

[7] Lange, D. and Oshima, M. Programming and Deploying Java Mobile Agents with Aglets. Addison Wesley. US. 1998.

[8] Man M.C. and Wei V.K. A Taxonomy for Attacks on Mobile Agent. IEEE EUROCON'2001 Trends in Communications, International Conference. 2001.

[9] Mascagni, M. Complexity and Analysis of Data Structures and Algorithms. Department of Computer Science. Florida State University. US. 2004.

[10] Oaks, S. Java Security, Second Edition. O'reilly & Associates, Inc. US. 2001.

[11] Smart, N. Public Key Infrastructure. Department of Computer Science. University of Bristol, UK. 2004

[12] Vigna G. Mobile Agents and Security, Lecture notes in Computer Science. Springer-Verlag, 1998.

[13] Zhao, J. and Blum, T. Next-Generation E-Commerce: XML + Mobile Agent + Trust. Fraunhofer CRCG, Providence, Rhode Island, USA. 2000.