J. Areitio, J. Lopez, and J. M. Troya, "Horizontes y Tendencias de Seguridad en Internet", *Novática*, vol. 145, pp. 65-71, 2000.
NICS Lab. Publications: https://www.nics.uma.es/publications

NUEVAS TENDECIAS DE SEGURIDAD EN INTERNET

Javier Areitio[*], Javier López[**] y José M. Troya[**]
[*]Facultad de Ingeniería – ESIDE – Universidad de Deusto
jareitio@orion.deusto.es
[**]E.T.S. de Ingeniería Informática – Universidad de Málaga
{jlm, troya}@lcc.uma.es

Resumen

El comercio electrónico está llamado a ser el fenómeno de mayor importancia en el futuro de Internet. Entre sus aplicaciones se encuentran las compras en línea, la banca electrónica, la tele-educación, los casinos virtuales, los servicios de pago por visión y vídeo bajo demanda, etc. Desde el punto de vista de la Seguridad, estas aplicaciones presentan una serie de nuevos requisitos que van a imponer un gran esfuerzo investigador a corto y medio plazo. En este artículo se presentan algunos de los más importantes, como la administración de la confianza, la utilización de pagos electrónicos, la necesidad de la protección de la propiedad intelectual, los servicios de protección de privacidad y anonimato, y la autonomía de código y la detección de fraudes, identificándose las áreas de investigación relacionadas.

1. INTRODUCCIÓN

Bien es sabido que la orientación inicial en el diseño de Internet fue la investigación. Como red abierta, fue creada para un entorno mucho más benigno del que ahora existe pues sus intereses se centraban en un intercambio libre de información. No obstante, tan pronto como Internet ha dejado de ser una red experimental para convertirse en un entorno extremadamente útil, otras personas con diferentes intereses éticos y diversos comportamientos se han incorporado a la misma.

Es evidente que actualmente el entorno de Internet es poco confiable pues se pueden encontrar muchos estados de riesgo. La desconfianza está presente en la mayoría de las ocasiones, y de esta forma es difícil que la Red pueda conseguir el nivel de penetración que está llamada a tener dentro de las estructuras organizativas de la sociedad.

Esta situación ha derivado en que la Seguridad sea, en la actualidad, un tema a debate. Más aún si tenemos en cuenta que el mayor campo de aplicación de Internet parece estar reservado al comercio electrónico, donde los aspectos de seguridad son esenciales para su desarrollo [1]. Por lo tanto, la cantidad de investigación va en aumento, así como el desarrollo y distribución de muchos productos de seguridad. Además, las actividades de varios organismos internacionales, como la OCDE [2] y la Comisión Europea [3], muestran claramente que la Seguridad ha de ser un pilar básico en cualquier iniciativa tendente a solucionar el problema del desarrollo de las infraestructuras de información. Es evidente que los procedimientos y aplicaciones criptográficas son las herramientas fundamentales para tal fin pues permiten, entre otras,

la transmisión confidencial, la salvaguarda de la integridad de los datos, y la autenticación de usuarios de una red abierta, como es el caso de Internet.

Cuando se hace referencia a la Seguridad en Internet siempre vienen a la mente los aspectos más típicos de la misma, como son la seguridad en el sistema Cliente, en el sistema Servidor, y en la propia transmisión. Se conoce que donde más esfuerzo investigador se ha realizado recientemente es, precisamente, en todos aquellos aspectos de seguridad relacionados con la última de esas opciones, la de la comunicación, aunque es evidente que existen en ella puntos indisociables respecto a las otras dos.

Por ello, en el apartado 2 de este trabajo nos detenemos a examinar cuál es la situación respecto a las soluciones existentes para dotar de seguridad a la comunicación en sí; esto es, estudiamos la situación actual de lo que se ha dado en denominar *Seguridad en Red*, y revisamos los problemas que quedan por solucionar aún. Por otro lado, en el apartado 3, y bajo la premisa de que el comercio electrónico se vislumbra como el campo de aplicación por excelencia para Internet, se analizan los nuevos requisitos de estas aplicaciones, que van más allá de los tradicionales de la Seguridad en Red. Al mismo tiempo se indica cómo esos nuevos requisitos están originando o pueden dar lugar a nuevas líneas de investigación. Finalmente, en el apartado 4, se presentan las conclusiones.

2. SEGURIDAD EN RED: OPCIONES

Los protocolos criptográficos desarrollados para proporcionar servicios de comunicación segura en Internet son similares si atendemos tanto a los servicios de seguridad que proporcionan como a las técnicas y a los algoritmos criptográficos que emplean [4]. Su diferencia fundamental estriba en la forma de proporcionar esa seguridad y en su localización dentro de la pila de protocolos de TCP/IP.

En particular, hay soluciones para cada una de las capas o niveles. Por ejemplo, en el *nivel de acceso a red* encontramos los protocolos *PPTP (Point-to-Point Tunneling Protocol)* [5] y *L2TP (Layer 2 Tunneling Protocol)* [6]; en el *nivel de red* destaca, por encima de los demás, el protocolo *IPSEC* [7]; en el *nivel de transporte* sobresalen los protocolos *SSL (Secure Socket Layer)* [8] y *TLS (Transport Layer Security)* [9]; y por último, en el *nivel de aplicación* encontramos casi tantas soluciones como tipos de aplicaciones específicas de los usuarios [10,11,12]. En cualquiera de los casos ninguna está exenta de inconvenientes.

Ahora bien, la cuestión relativa a cuál es el mejor nivel para proporcionar los servicios de seguridad no ha sido estudiada todavía en profundidad, por lo que aún es bastante difícil de contestar. En nuestra opinión existen razones, en general, para proporcionar servicios tanto en las capas bajas como en las altas.

Por un lado, la seguridad en las capas bajas se puede implementar de forma transparente a los usuarios y a las aplicaciones, pero estas soluciones intentan hacer demasiadas cosas de forma simultánea. Además, la protección es aplicada de forma automática, por lo que los usuarios no pueden decidir cuándo usar los mecanismos de seguridad, resultando ineficiente en muchos casos.

Por otro lado, las soluciones ubicadas en las capas altas pueden cumplir mejor con los requisitos de seguridad específicos de la aplicación correspondiente. Pero, en ocasiones, es absolutamente necesario que los usuarios no puedan saltarse individualmente una política de seguridad general y obligatoria, como la de la Intranet de una empresa. A veces también es conveniente que la arquitectura de red bloquee las comunicaciones con máquinas y subredes que no son de confianza. Las soluciones de las capas altas no son apropiadas en ambos casos.

En realidad, la capa a elegir debe depender de los servicios de seguridad requeridos y del entorno de aplicación en los que éstos se deben proporcionar. Por ejemplo, la transformación criptográfica y masiva de datos ha de realizarse en la capa de red, que está normalmente ligada con el núcleo del sistema operativo y que permite tanto una implementación como una planificación eficiente del hardware disponible. Por el contrario, es recomendable que todas las operaciones asociadas con firmas digitales sean realizadas en la capa de aplicación, ya que el uso de esas claves debe originar una responsabilidad asociada directamente al usuario.

Este último caso origina un nuevo e interesante problema a resolver. Actualmente cada aplicación mantiene sus claves criptográficas de forma individual, pero ésta no será la forma apropiada de hacerlo en futuras aplicaciones pues el usuario deberá disponer de algún tipo de *Agente de Claves* que almacene de forma segura sus claves criptográficas, proporcionando a cada aplicación las claves requeridas.

2.1 Un caso de estudio: los protocolos SSL y TLS

La comunidad de usuarios del protocolo SSL está creciendo muy rápidamente, apareciendo éste en lo alto de la lista de protocolos más utilizados. El hecho de que Netscape desarrollara SSL para integrarlo en sus navegadores lo ha catapultado hasta límites insospechados. Tanto es así que, para muchos usuarios, hablar de SSL, o de su sucesor, el protocolo TLS, es sinónimo de "seguridad absoluta para Internet", aunque esto dista mucho de ser cierto. Dada su popularidad y gran implantación dedicamos este subapartado a tales protocolos.

Ambos protocolos presentan los mismos inconvenientes. En primer lugar, tanto uno como otro proporcionan servicios de seguridad para las aplicaciones basadas en TCP; es decir, requieren de una conexión TCP previa. Esto ocasiona problemas porque cada vez existe un mayor número de aplicaciones que hacen uso del protocolo UDP, como las comunicaciones en tiempo real y las aplicaciones multicast. Ninguno de los dos proporciona una solución viable para los problemas de seguridad de aplicaciones que, como éstas, se basan en el uso del protocolo UDP en el nivel de transporte.

En segundo lugar, existe una dificultad práctica en hacer un encapsulamiento del tráfico de datos de SSL y TLS a través de un cortafuego. Esta dificultad se debe al hecho de que ambos protocolos son punto a punto.

Un tercer problema es que el desarrollo de soluciones basadas en SSL y TLS están limitadas seriamente por el control de las exportaciones de USA. Estas restricciones de exportación hacen que las versiones internacionales de los productos (navegadores y servidores) basados en estos protocolos incorporen criptografía débil.

La mayoría de las aplicaciones internacionales utilizan el cifrado RC4 con una longitud efectiva de clave de 40 bits. Sólo se cifran 40 bits de los 128 que posee la clave de sesión del RC4, mientras que los restantes 88 se envían en claro. Igualmente, las cadenas de certificados contienen claves o firmas RSA de 512 bits, las cuales pueden no ser apropiadas en muchos entornos por su escasa longitud.

Una posible solución a este problema puede consistir en utilizar herramientas que mejoren los navegadores mediante la utilización de criptografía fuerte. Otra solución puede consistir en emplear una versión internacional aunque añadiendo un *servidor proxy* personal que proporcione al SSL las características de cifrado fuerte [13]. En realidad ese servidor actúa como un amplificador de cifrado.

Recientemente, Microsoft ha propuesto la solución *SCG (Server Gated Cryptography)*, la cual define un mecanismo de negociación de criptografía fuerte para sesiones basadas en SSL ó TLS con la presencia de un servidor especial de certificados. Este servidor sólo emite certificados a instituciones que se consideran confiables y que cooperan con entidades nacionales autorizadas (por ejemplo, bancos y otras instituciones financieras). La distribución de los certificados SGC es controlada de acuerdo con la licencia de exportación del Departamento de Comercio de USA, siendo Verisign la única compañía autorizada, por el momento, para emitir tales certificados. En definitiva, con esta solución el avance es nulo.

3. NUEVOS REQUISITOS DE SEGURIDAD

Normalmente, en las aplicaciones de comercio electrónico existen diversas entidades y protocolos involucrados. Estos deben ser eficientes, escalables y seguros para todas las partes intervinientes. Más aún, muchas de tales aplicaciones requieren la disponibilidad permanente de algunas de las partes, como, por ejemplo, los *Centros de Distribución de Claves*, o los componentes de revocación de certificados de las *Infraestructuras de Clave Pública*.

Todas estas características, que complican de forma considerable el diseño, la implementación y la verificación de las aplicaciones, originan que los requisitos de seguridad del comercio electrónico vayan más allá de los tradicionales requisitos de la Seguridad en Red. En esta sección se analizan los nuevos requisitos de las aplicaciones de comercio electrónico, tales como la administración de la confianza, la utilización de pagos electrónicos, la necesidad de la protección de la propiedad intelectual, los servicios de protección de privacidad y anonimato, la autonomía de código y la detección de fraudes. Consideramos que todos ellos son componentes fundamentales para el completo desarrollo del comercio electrónico en Internet. Aún así, en todos los casos, las líneas de investigación abiertas están sólo en su fase inicial.

3.1 Administración de Confianza

Una *Infraestructura de Clave Pública* (*PKI*) es el marco subyacente que permite que la tecnología de clave pública se pueda implantar de un modo extenso, proporcionando la base confiable necesaria para la correspondencia electrónica entre

aquellos usuarios que no pueden intercambiar manualmente sus claves. Por lo tanto, mediante la administración de los certificados de claves públicas de una PKI, se puede establecer y mantener un entorno de red seguro, posibilitando el uso de servicios de cifrado y, especialmente, de firma digital en una amplia gama de aplicaciones.

En entornos reales, especialmente en aquellos que involucran a una gran diversidad de empresas y comunidades de usuarios que trabajan de forma conjunta, encontramos el problema de cómo estructurar las relaciones entre las entidades de los diversos dominios involucrados. Esas estructuras dan lugar a los denominados *modelos de confianza*. Por consiguiente, el establecimiento de las PKIs es sólo un bloque de construcción adicional dentro de otro problema, más general, que es esencial en el éxito del comercio electrónico, la *administración de confianza* a través de la Red.

Sin embargo, es complicado encontrar soluciones a la administración de confianza cuando los bloques de construcción, en este caso el de las PKIs, no tienen una base definitivamente clara. Aunque se ha desarrollado una gran cantidad de trabajo sobre el establecimiento de PKIs, existen dos filosofías, totalmente contrapuestas, en competencia. Por un lado, la recomendación X.509 de la ITU-T y la infraestructura X.509 del grupo de trabajo PKIX del IETF [14]. Estas propuestas asumen la existencia de un espacio global de nombres y, por lo tanto, la configuración de una jerarquía de Autoridades de Certificación. Por otro lado, las propuestas de la iniciativa SDSI y del grupo de trabajo SPKI del IETF no asumen la existencia de un espacio global de nombres, sino de una multitud de espacios locales enlazados, donde el concepto de jerarquía desaparece por completo [15].

Otra cuestión ligada a la administración de confianza, que está por solucionar, es el problema de la autorización para las aplicaciones de comercio electrónico, pues no está claro, por el momento, cuál es la mejor solución. Además, la administración de la confianza también dependerá de la existencia de interfaces de usuarios apropiados, que actualmente brillan por su ausencia.

A estos interrogantes hay que unir otro, de mayor calado y trascendencia, relativo a si, en realidad, la criptografía de clave pública es la herramienta adecuada para solucionar los problemas de la administración de confianza. El objetivo original de la criptografía de clave pública era minimizar los costes para la iniciación de un camino de comunicación segura entre entidades que no tenían una relación previa. Se asumía que ésta era la razón principal por la que este tipo de criptografía dominaría las aplicaciones de comercio electrónico. Sin embargo, ha ido apareciendo la necesidad de idear otros conceptos, como, por ejemplo, el encadenamiento de certificados, la revocación de los mismos o los servicios de directorio que, a la postre, han llevado a un incremento de la sobrecarga administrativa, que era lo que originalmente se intentaba evitar.

No queda totalmente claro que los costes de la criptografía de clave pública sean mucho más bajos que los de la tradicional criptografía simétrica, habida cuenta de la dificultad que entraña establecer una PKI completamente operativa. De cualquier forma, no cabe duda de que, por el momento, no existe ningún método mejor para la utilización de esquemas de firma digital, y éstos son realmente esenciales para el comercio electrónico.

3.2 Utilización de Pagos Electrónicos

La creciente importancia del comercio electrónico y de sus aplicaciones ha dado lugar a la creación de una diversidad de sistemas electrónicos de pago que han resultado ser incompatibles [16]. Para los desarrolladores de aplicaciones esta variedad ha implicado la necesidad de entender los detalles de sistemas de pago diferentes así como la de adaptar el código de sus aplicaciones tan pronto como aparecía uno nuevo.

Parece que en el futuro habremos de utilizar, dependiendo de las aplicaciones, unos sistemas de pago u otros. En tal caso será necesaria la utilización de una *capa de negociación* por encima del correspondiente sistema de pago. Esta idea no es nueva pues hace unos años el *World Wide Web Consortium* (W3C) y el consorcio *Commercenet* iniciaron el *Proyecto JEPI* (Joint Electronic Payment Initiative), aglutinando a las industrias del sector para asegurar que los múltiples esquemas de pago, protocolos y mecanismos de transporte trabajaran juntos para interoperar en Internet. El objetivo de JEPI ha sido permitir la negociación automática de pagos, de tal forma que, tras una negociación entre los ordenadores, sean los propios usuarios los que tomen la decisión final. Actualmente, JEPI ha frenado su labor, habiendo retomado el trabajo el recientemente formado *Grupo de Interés de Comercio Electrónico* del W3C.

Sin embargo, cabe la posibilidad de que se produzca un grado de convergencia en la industria. Dentro del Proyecto Europeo SEMPER, un grupo de investigadores liderados por IBM está tratando de unificar los diferentes mecanismos de pago en un marco común [17]. Esto podrá permitir que los programas se desarrollen con independencia del sistema de pago específico, y con el beneficio adicional de proporcionar un punto de control centralizado para la información y políticas de pago.

Además de esta disyuntiva, existen otros interrogantes sobre la regulación de los pagos electrónicos para los que no se ha encontrado solución. Por ejemplo, ¿quién va a estar autorizado para emitir dinero electrónico?, ¿podrá cualquier banco emitir su propio dinero y monedas digitales?. De ser así, ¿cómo habrá de prevenirse el fraude?, y ¿quién se encargará de controlar las operaciones de los bancos para proteger a los consumidores?. Hay que hacer notar que los instrumentos de pago convencionales son operados por los bancos, estando sujetos a una regulación por parte de los bancos centrales nacionales. ¿Ocurrirá algo similar para los pagos electrónicos? Estas cuestiones y algunas otras están aún por resolver, y cuando tengan respuesta desde el punto de vista administrativo/legal, entonces habrá que crear los protocolos que resuelvan el problema desde el punto de vista técnico.

3.3 Protección de Propiedad Intelectual

Como es sabido, un documento multimedia está compuesto de datos digitales que pueden contener texto, gráfico, imágenes, audio o video. Debido a la proliferación de la WWW, gran cantidad de documentos multimedia están actualmente a disposición de millones de usuarios en Internet. La representación digital y la distribución de tales documentos ha incrementado su mal uso y ha intensificado significativamente los problemas asociados con la protección del copyright.

Los problemas nacen con las características intrínsecas de los datos digitales: hacer y distribuir una copia es fácil, barato y rápido, y, además, cada copia es idéntica a la original. Por lo tanto, la protección de la propiedad intelectual es un requisito para la implantación con éxito de las aplicaciones de comercio electrónico que buscan la distribución de mercancías inmateriales.

Una de las soluciones para resolver este problema es la aplicación del denominado *control de uso*. De acuerdo con esta solución, cada uso del material protegido, como ver, ejecutar o imprimir, es controlado por algún hardware o software autorizado [18]. Pero existen problemas prácticos relacionados con la naturaleza restrictiva del control de uso, y esos problemas serán prohibitivos para la implantación a gran escala de esta tecnología.

Otra solución es permitir copias y usos ilimitados que proporcionen pruebas para el caso de comportamientos ilícitos. Esta solución se basa en la utilización de técnicas de *etiquetado de copyright digital* que insertan marcas digitales en el material a proteger con información sobre origen, dueño, receptor, etc. Por lo tanto, las etiquetas de copyright digital pueden proporcionar pruebas a posteriori de los actos ilegales. El uso de técnicas de etiquetado no es contrario al de la técnica de control de uso, sino más bien complementario, ya que proporciona otra defensa ante comportamientos ilícitos sobre el material protegido.

Hay dos tipos de etiquetas para identificar y proteger los copyrights de documentos multimedia. En el primero, un documento se puede marcar con una etiqueta que identifique unívocamente al autor; es el denominado *etiquetado de propiedad*. En el segundo, un documento se puede marcar de forma que permita que su distribución sea rastreada; es el denominado *etiquetado de receptor*. Estos etiquetados se conocen normalmente como *marcas de agua* y *huellas digitales*, respectivamente [19].

En este campo existen varios problemas a resolver. Primero, es necesario encontrar una solución a cómo combinar las tecnologías de protección de datos, protección de copyright, cifrado y autenticación de datos de una forma efectiva y eficiente.

Un segundo problema es el desarrollo de un sistema de protección que mantenga las etiquetas ocultas, ya que los sistemas existentes en la actualidad no aseguran que una etiqueta pueda sobrevivir a todas las transformaciones y operaciones de procesamiento de señal que se pueden aplicar. Además, esta tecnología será útil mientras la inserción y la extracción de etiquetas sea una tarea costosa para aquellos que quieran actuar de forma deshonesta.

Por último, para que las técnicas de etiquetado puedan cumplir su cometido, es necesario definir una situación dentro del sistema legal que permita a los dueños del copyright denunciar acciones ilegales. Si ha llevado más de veinte años establecer una práctica comercial común de la firma digital y una acción legislativa acorde a las necesidades, entonces puede que quede mucho camino por recorrer; o quizás no, si se aprende del camino recorrido para la firma digital.

3.4 Servicios de Protección de Privacidad y Anonimato

Aunque la navegación a través de la Web parece una actividad anónima, en realidad no lo es. Los servidores Web y los administradores de red pueden conseguir mucha información sobre los usuarios y su comportamiento de navegación. Por ejemplo, el servidor Web puede tomar nota del día y la hora de cada petición http, la dirección IP o el nombre del sistema del cliente, la URL del recurso requerido por el cliente y alguna otra información.

Sin embargo, en muchas ocasiones, y especialmente en las aplicaciones de comercio electrónico, alguna de las partes puede desear permanecer anónima durante una transacción específica. Por ello, los servicios de protección de privacidad y de anonimato en el WWW se están convirtiendo en un campo importante de investigación.

Es importante hacer notar que el anonimato no es lo mismo que la confidencialidad ya que ésta intenta proteger la privacidad de los datos que se transmiten, mientras que la primera intenta proteger las identidades de las partes comunicantes o la relación entre ellos. Los servicios de anonimato tratan de proteger contra formas específicas de análisis de tráfico, pues éste se está convirtiendo en una amenaza significativa para la privacidad de los usuarios y de sus conductas de navegación, que cada vez más son objeto de observación. A medida que el comercio electrónico basado en Web se hace más importante, esas conductas empiezan a incluir los patrones de hábitos de compra, de dinero gastado, y de otros datos personales, que son considerados privados, y, por lo tanto, "golosos" para muchas compañías.

Hay tres tipos de propiedades de comunicación anónima que han de ser proporcionadas bien individualmente o bien combinadas: *anonimato del emisor* (por ejemplo, publicación anónima en la Web); *anonimato del receptor* (por ejemplo, navegación anónima en la Web); y *desvinculación entre emisor y receptor* (por ejemplo, operaciones de bolsa) [20].

En la actualidad existen varias técnicas bajo investigación que se pueden utilizar para proporcionar los servicios de anonimato mencionados. Pero estas técnicas se deben refinar más y, sobre todo, deben ser probadas en aplicaciones del mundo real. También será importante estudiar la relación entre éstos y otros servicios de seguridad pues los requisitos de anonimato están, normalmente, en contradicción con otros requisitos de seguridad, como el control de acceso, la autenticación y el no-repudio. Así pues, los conflictos resultantes deben ser solucionados.

3.5 Autonomía de Código

El *código móvil* y los *sistemas basados en agentes* se perfilan como uno de los más importantes paradigmas de computación en el futuro (tras el paradigma cliente/servidor). Así, se argumenta que las aplicaciones de comercio electrónico requerirán de código móvil que recorran de forma autónoma la red en representación del usuario. Es evidente que existen varios aspectos de seguridad relacionados con este asunto [21].

La mayoría de los investigadores se han concentrado en el planteamiento de un primer problema, la protección del servidor ante potenciales agentes hostiles. Este es, sin duda, y de forma lógica, el primer problema que viene a la mente cuando pensamos en los problemas de seguridad relativos a este asunto. Es decir, la primera reacción es proteger nuestros sistemas ante esos códigos que se desplazan de un sitio a otro de la red.

Sin embargo, el caso contrario, cómo proteger el código móvil, es un segundo problema que, aunque se ha planteado, no se ha estudiado con detenimiento. El hecho de que un entorno de ejecución pueda atacar a un programa no juega un papel destacado en la seguridad clásica. Esto es porque la parte que mantiene el entorno de ejecución también, generalmente, utiliza el programa. Pero esta situación es totalmente opuesta al caso del código móvil y los sistemas basados en agentes. En este caso, el dueño del código móvil y el operador del entorno de ejecución son diferentes en la mayoría de los casos.

Esto conduce automáticamente al problema de cómo proteger el código móvil ante los entornos de ejecución hostiles. Un *entorno de ejecución hostil* se puede definir, en general, como una parte capaz de ejecutar un agente que no le pertenece, con ánimo de atacarlo de alguna forma. Por ejemplo, podría tratar de manipular código, datos, o control de flujo, impersonando a otros sistemas o entornos de ejecución para, con posterioridad, dejar que el código modificado siguiera su recorrido a través de entornos autorizados. Esa modificación podría perseguir resultados tales como espiar sistemas remotos, provocar que éstos produzcan resultados erróneos en las llamadas del sistema emitidas por el agente, etc.

Como ya se ha comentado, ha sido escasa la investigación llevada a cabo relacionada con la protección del código móvil ante sistemas y entornos de ejecución hostiles. Las soluciones propuestas parecen ser insuficientes porque son demasiado restrictivas. De entre ellas, las que se pueden tildar de más útiles son las *cajas negras limitadas en tiempo* o la *computación con funciones cifradas*. Ambas pueden proteger el código móvil en el entorno de ejecución, pero entonces nos encontramos con el primer problema, esto es, se pierde la posibilidad de decidir si un segmento específico de código móvil es hostil o no. En este caso, resultará difícil, sino imposible hacer decisiones inteligentes respecto a la protección del entorno de ejecución. Por lo tanto, estas soluciones al segundo de los problemas planteados son contradictorias con la posibilidad de encontrar soluciones apropiadas para el primer problema.

En general, la seguridad del código móvil es, ante todo, un problema de los lenguajes de programación, pues estos deberían estar diseñados alrededor de ciertas propiedades de seguridad [22]. Pero la realidad es diferente, ya que en los lenguajes de programación utilizados para el código móvil y los sistemas basados en agente, los modelos y las arquitecturas de seguridad se han desarrollado con posterioridad.

En definitiva, todavía quedan muchos temas por resolver de forma apropiada antes de que los agentes móviles puedan llegar a ser el instrumento de aplicaciones a gran escala. Hemos comentado que, desafortunadamente, los dos problemas planteados no son independientes, y que las soluciones para uno de ellos pueden limitar en gran medida las soluciones para el otro. Consecuentemente, la interdependencia de los dos

problemas y sus soluciones es un importante campo de estudio para la mayor implantación del código móvil y los sistemas basados en agentes.

3.6 Detección de Fraudes

Sin duda alguna un área de elevado crecimiento para el Comercio Eléctrónico es la convergencia de las comunicaciones móviles e Internet. Pero esta simbiosis entraña un colectivo creciente de nuevos problemas para la seguridad. Se estima que la industria de las comunicaciones móviles pierde al año varios millones de ECUs debido al fraude. Por tanto la detección y prevención de toda actividad fraudulenta es clave tanto para los usuarios como prestatarios (proveedores/operadores de red).

Es evidente que queda mucho que hacer en cuanto a medidas de seguridad en la implantación de las tecnologías de comunicaciones celulares GSM/GPRS/UMTS. La utilización conjunta de técnicas modernas de inteligencia artificial (como sistemas expertos adaptativos basados en reglas) y sofisticadas redes neuronales puede ser una alternativa a tener en cuenta en los próximos años.

Existen diferentes tipos de comunicaciones en la actual infraestructura de Telecomunicaciones: (a) TCP/IP. (b) Comunicaciones telefónicas conmutador a conmutador (p.e conmutadores celulares y telefónicos). (c) Comunicaciones satélite a/desde tierra. Las intrusiones a las comunicaciones del tipo (a) son las más conocidas, respecto a las otras comunicaciones su problemática ha sido menos estudiadas [23]. En esta área los futuros sistemas de detección basados en verificación de integridad, en reglas y visualización de datos parecen ser prometedores.

El paradigma de seguridad clásico de protección, detección y reacción que se ha aplicado tradicionalmente al campo de la seguridad de la información con cortafuegos asumiendo la función de protección mientras la detección era gestionada por los sistemas de detección de intrusiones parece cambiar. Actualmente los sistemas de detección/actuación frente a intrusiones/fraudes operan en línea y pueden programarse reactiva ó proactivamente. Se pueden plantear respecto al comportamiento potencial de la defensa activa de los sistemas de detección/respuesta a intrusiones tres tipos de consideraciones: (1) Cuestiones técnicas (qué comportamiento es posible en la práctica). (2) Cuestiones legales (qué comportamiento esta dentro del marco legal adecuado). (3) Cuestiones éticas (qué comportamiento es aceptable en un contexto social, de negocios ó militar concreto).

4. CONCLUSIONES

Muchas organizaciones están aprovechando las oportunidades ofrecidas por el comercio electrónico basado en Internet, y se espera que muchas más lo hagan en poco tiempo. Entre estas aplicaciones se encuentran las compras en línea, la banca electrónica, la teleeducación, los casinos virtuales, los servicios de pago por visión y vídeo bajo demanda, etc. Pero aún queda una gran cantidad de empresas, y sobre todo un enorme número de potenciales clientes, que recelan de tomar parte en el comercio electrónico, alegando una inadecuación de los servicios de seguridad.

Es indudable que no les falta razón, pues las aplicaciones de comercio electrónico presentan una serie de nuevos requisitos que van más allá de los

tradicionales requisitos de la Seguridad en Red, el área donde más investigación se ha desarrollado recientemente. En este artículo se ha proporcionado un compendio de esos nuevos requisitos: la administración de la confianza, la utilización de pagos electrónicos, la necesidad de la protección de la propiedad intelectual, los servicios de protección de privacidad y anonimato, la autonomía de código y la detección de fraudes.

A nuestro juicio, se hace imprescindible un mayor grado de investigación en estas áreas para poder realizar una implantación a gran escala de las aplicaciones de comercio electrónico. También se hace necesaria una mayor investigación en otras áreas relacionadas, como, por ejemplo, la de las tarjetas inteligentes, ya que éstas serán el soporte básico en la utilización de la mayoría de las aplicaciones. Asimismo, será de vital importancia el desarrollo de nuevas técnicas de análisis de protocolos de seguridad, debido a que los protocolos orientados al comercio electrónico presentan características de eficiencia y escalabilidad diametralmente opuestas a las de los tradicionales protocolos de seguridad, como los de intercambio de claves o los de autenticación de usuarios.

En definitiva, queda aún mucho trabajo por desarrollar y bastantes áreas que requieren un mayor grado de estudio antes de que el comercio electrónico pueda llegar a tener el nivel de implantación que se vislumbra, pero no cabe duda de que el camino recorrido hasta momento es significativo y que la dirección parece ser la correcta.

Referencias

[1] British Department of Trade and Industry, *Building Confidence in Electronic Commerce*, 1999.

[2] OCDE, *Recommendation of the Council Concerning Guidelines for Security Policy*, 1997.

[3] European Commission, *Ensuring Security and Trust in Electronic Communication. Towards a European Framework for Digital Signatures and Encryption*, COM(97) 503, 1997.

[4] R. Oppliger, *Internet and Intranet Security*, Artech House, 1998.

[5] Microsoft Corporation, *Understanding Point-to-Point Tunneling Protocol (PPTP)*, White Paper, 1997.

[6] P. Srisuresh, *Secure Remote Access with L2TP*, PPPEXT Working Group Internet Draft, September 1999.

[7] S. Kent, R. Atkinson, *Security Architecture for the Internet Protocol*, RFC 2041, November 1998.

[8] Netscape Communications. *SSL 3.0 Specification*. *http://www.netscape.com/libr/ssl3/index.html*

[9] T. Dierks, C. Allen. *The TLS Protocol Version 1.0*, RFC 2246, January 1999.

[10] M. Horowitz, S. Lunt, *FTP Security Extensions*, RFC 2228, October 1997.

[11] A. Schiffman, E. Rescorla, *The Secure Hypertext Transfer Protocol*, Internet Draft, June 1998.

[12] B. Ramsdell, *S/MIME Version 3 Message Specification*, Internet Draft, August 1998.

[13] M. Abadi, A. Birrel, R. Stata, E. Wobber, *Secure Web Tunneling*, Proceedings of the 7th International World Wide Web Conference, 1998, pp. 531 – 539.

[14] R. Housley, W. Ford, W.Polk, D. Solo, *Internet X.509 Certificate Management Protocols*, RFC 2510, March 1999.

[15] SPKI Working Group Internet Draft, *Simple Public Key Certificate*, 1998.

[16] D. O´Mahony, M. Pierce, H. Tewari, *Electronic Payment Systems*, Artech House, 1997.

[17] J. Abad Peiro, N. Asokan, M. Steiner, M. Waidner, *Designing a Generic Payment Service*, IBM Systems Journal, Vol.37, No.1, 1998, pp. 72-88.

[18] B. Lehman, R. Brown, *Intellectual Property and the National Information Infrastructure*, Report of the Working Group on Intellectual Property Rights , 1995.

[19] F. Petitcolas, S. Katzenbeisser, *Steganography and Watermarking*, Artech House, 2000.

[20] A. Pfitzmann, M. Waidner, *Networks without User Observability*, Computers & Security, Vol. 2, No.6, pp. 158 – 166.

[21] D. Chess, *Security Issues in Mobile Code*, Mobile Agents and Security, LNCS 1419, 1998, pp. 1-14.

[22] D. Volpano, G. Smith, *Language Issues in Mobile Program Security*, Mobile Agents and Security, LNCS 1419, 1998, pp. 25-43.
[23] J. Areitio. *Tecnología de Sistemas de Detección y Respuesta a Intrusiones y Vulnerabilidades para Entornos de Red: Identificación, Clasificación y Análisis*, Securmática'99. Abril 1999.