

Café de redacción

Existe mucha confusión en cuanto a si Internet es segura o no: virus, sistemas de autenticación, firma electrónica, certificación, medios de pago, etc. Y esta confusión está ralentizando el desarrollo del comercio electrónico entre empresas y con el cliente final

versidad y desarrollo actividades de auditoría y consultoría.

Julián Inza. He estado trabajando en FESTE, fundación dedicada a la seguridad, y también en Banesto, liderando proyectos de comercio electrónico. En la actualidad, en Mobipay estamos trabajando para que el teléfono móvil permita llevar a cabo pagos con la seguridad de una firma electrónica.

¿Cuáles son los principales problemas de vulnerabilidad en Internet?

Arturo Ribagorda. La seguridad en la red está amenazada por los virus o los "ataques" que sufren determinadas páginas, pero también por un exceso de desconfianza que se ha ido generando a partir de una serie de informaciones un tanto exageradas, y que ante el usuario crea una alarma excesiva y le impide utilizar para sus transacciones un medio muy útil.

En el caso de los virus ¿qué posibilidades hay de defenderse?

Arturo Ribagorda. El virus, en realidad, es un programa maligno. Empezaron a aparecer en los años 60. La primera tesis doctoral que hay sobre virus es de los primeros 80. Aparece el famoso virus paquistaní Brain, que se vendió como programa de software a los turistas, como una cierta venganza anti colonialista. Personalmente, durante años los creí en trance de desaparecer y obviamente me equivoqué. A comienzos de los noventa vino la explosión de Internet y los virus volvieron a reavivarse, pero antes se reproducían por medio

Red fiable para todos

Lo cierto es que el nivel de desconfianza en el consumidor no permite avanzar el comercio electrónico ni el intercambio de material sensible, a través de la red. Dado que la seguridad es un tema fácil de manipular y que el exceso de información disponible en la propia Red no ayuda precisamente, BIT ha considerado necesario reunir a tres expertos en seguridad para que nos faciliten el acercamiento al tema. Son Julián Inza, director de Sistemas de Información de Movilpago; José Antonio Mañas, catedrático de la UPM y consultor independiente; y Arturo Ribagorda, catedrático de la Universidad Carlos III.

Ante todo, vamos a contar a los lectores cuál es vuestro campo de actividad.

José Antonio Mañas. Básicamente, me muevo en lo que es la docencia, doy cursos sobre seguridad en comercio electrónico. Además, soy consultor privado en temas de integración de sistemas, seguridad de sistemas alrededor de tecnología web para proteger el negocio de las empresas.

Arturo Ribagorda. Mi dedicación principal es la docencia, que también implica dar cursos de seguridad en otros ámbitos más extensos. Además, cuento con un equipo trabajando en la uni-



De izda. a dcha.: César Rico, José Antonio Mañas, Arturo Ribagorda y Julián Inza

de disquetes y ahora a velocidad de vértigo por medio del correo electrónico. Actualmente, se multiplican y auto remiten a todo el listado de direcciones de cada ordenador al que llegan.

Los ordenadores ya no están compartimentados, no hay barreras internas en los sistemas operativos, como había en los primeros.

Es muy difícil parar el virus en el Servidor, porque tendría que analizar cada mensaje recibido. Digamos que no tienen fácil solución en el corto plazo. Y las vacunas que se crean, se hacen a partir de los virus que vas conociendo. Si puedes detectar que está entrando un fichero extraño, cuando lleva un "exe" adosado o es excesivamente grande, puedes borrarlo, pero es un control individual, del usuario

que debe estar alerta. Como ocurre con un coche, es el conductor el que se responsabiliza de gran parte de su propia seguridad. Al final, es importante el factor humano, la precaución del usuario y tener el anti virus reciente.

José Antonio Mañas. Hay además software malo y bueno, anti virus y servidores bien diseñados o no. Muchas veces, lo que se hace es vender como otro producto un programa que arregla los problemas que provocó el primero, es un negocio. Hay mecanismos de seguridad que son malos y los atacantes son superiores. Si el sistema se corrompe, el fabricante de software tiene la culpa y debería perseguirse. No veo cómo se puede asegurar la red totalmente. Hay escepticismo con los anti virus, es lógico.

¿Cómo se podría abordar entonces el problema, dónde hay que actuar dentro del proceso de recibir y abrir un correo?

Arturo Ribagorda. Creo que la responsabilidad es más del fabricante, pero tampoco toda. Quien conduce un coche a 200 por hora sabe que lo está haciendo. Es una responsabilidad compartida. Pero lo primero es subrayar que no hay que alarmarse por los virus, no hay que exagerar, el peligro se puede controlar. A los fabricantes les encarece el producto si lo proveen de un buen antivirus, somos los usuarios los que hemos de exigirlo.

José Antonio Mañas. No afectan a todo ni a todos, sino a ciertos segmentos, como los terminales de usuarios y en la infor-

mática terminal en los servidores. Cualquier comprador sabe que hay unos mínimos de calidad exigidos por Industria. En el software hay productos de gama baja, con niveles de calidad bajos.

La inquietud que produce en el sector la falta de confianza en el comercio electrónico ¿pensáis que tiene solución?

José Antonio Mañas. El comercio electrónico es el futuro, aunque se ha tratado con excesiva alegría en algunas áreas. Hay un exceso de desconfianza por parte del usuario, pero la red no es ni segura ni insegura, tiene una serie de componentes que si se utilizan mal, repercute en aspectos de seguridad como los datos personales, de pago, de garantía. Pero el riesgo en

los pagos no está del lado del consumidor, es el comerciante quien se la juega, porque el cliente puede recuperar su dinero fácilmente.

Los códigos de tarjeta bancaria pueden acabar en una base de datos ajena ¿por eso surge la duda en el consumidor?

Arturo Ribagorda. El usuario tiene miedo a que mientras sus datos viajan por la red, se los puedan captar. Pero eso no es eficaz para el delincuente, le exige mucho tiempo. El peligro no está en el viaje sino que reside en el servidor. No es una práctica frecuente que te intercepten en la red. Sin embargo, sí se capturan en los servidores mal protegidos. La gran banca funciona con la red hace tiempo y no tiene grandes problemas.

José Antonio Mañas. Para el delincuente, los medios que tiene que dedicar a entrar en un servidor y obtener una serie de datos sensibles es mucho más caro y exige más esfuerzo que robar de la manera tradicional. No les compensa.

Arturo Ribagorda. La ley te protege durante mucho tiempo, alrededor de seis meses para que reclames algún cobro dudoso. El banco es el intermediario como pagador y puedes negar una compra. Pero la tasa de fuga de información de los bancos es mínima. La tecnología avanza de forma imparable y la sociedad le sigue como puede. Lo que se hace necesario es un marchamo de calidad. El problema es que la seguridad no es demostrable, sólo se demuestra a posteriori la inseguridad. Pero que haya un cierto nivel



José Antonio Mañas:
“Actualmente el riesgo de los pagos por la Red no está del lado del consumidor sino del comerciante porque el cliente siempre puede recuperar su dinero”

de certificación dará más confianza.

Desde el punto de vista jurídico ¿hay necesidad de legislar más temas como autenticación, privacidad, comunicación entre dos interlocutores concretos?

Arturo Ribagorda. La firma electrónica cuenta ya con un Real Decreto de septiembre del 99 que se adelanta a la directiva comunitaria. Habla de la firma electrónica avanzada que equiparan a la manuscrita siempre que se cumplan dos condicio-

nes: primero, que se realice mediante dispositivo seguro. Segundo, que esté avalada por un certificado digital emitido por un proveedor de servicios de certificación acreditado. Falta ahora que determinaran qué entidades acreditarán a este proveedor y certificarán el nivel de seguridad de los dispositivos.

Julián Inza. Es curioso que la ley regule la relación entre signatario y prestador de servicios de certificación, lo que, por otro lado ya estaría cubierto por su relación contractual, y no trate los derechos y responsabilidades de terceros que confían en una firma electrónica y que no tienen una relación contractual previa. Sin embargo, no deja de tener importancia su influencia respecto a las presunciones, ya que hasta que salió la ley había que demostrar la validez de una firma electrónica y desde ahora una firma electrónica se presume válida y lo que habría que demostrar es que no lo es.

José Antonio Mañas. Lo más importante de la ley es que quede sujeto a peritaje lo que es la validación de la firma. Falta que se desarrolle como reglamento y que haya jurisprudencia al respecto. No sabemos cómo va a evolucionar.

Arturo Ribagorda. La ley es válida y es bueno que los juristas se familiaricen con éste ámbito. Falta la reglamentación, prevista en la propia ley. El problema es de tiempo. Las tecnologías nuevas se están arrojando tan rápido que no dan tiempo a prever patrones de fraude y demás.

José Antonio Mañas. Es importante empezar a andar y ver cómo evoluciona. Hay que saber cuál es la parte débil del contrato para defenderla. El volumen es pequeño en las transacciones y permite seguir la evolución. Antes de que crezca mucho, hay que ir rectificando poco a poco, como se hace con todas las leyes. Hay que valorar el proteccionismo comercial. A un país como España le conviene también utilizar las leyes como un mecanismo que le defienda de la invasión tecnológica. Hay, por tanto, que definir el comercio internacional

En cuanto a la certificación ¿cómo va su regulación?

Julián Inza. Ya tenemos el reglamento que asigna a ENAC (Entidad Nacional de Acreditación) la responsabilidad de definir las reglas de homologación de laboratorios o auditores y las que éstos utilizarían para acreditar a los prestadores de servicios de certificaciones. Pero esa normativa complementaria no se ha desarrollado mientras se observan los avances en nuestro entorno europeo. En la práctica, todavía no es posible inscribir a un PSC en el registro correspondiente conforme a la ley.

¿Qué se puede contar del PKI (Public Key Information), la "Infraestructura de Clave Pública"? ¿es una solución?

José Antonio Mañas. PKI es una tecnología potente, con futuro, que necesita vestirse de sistema para que tenga solidez. Volviendo a los problemas del comercio electrónico es que algunos creen que basta con tener tecnología para tener resueltos

los problemas de actividad comercial. Es un error, lo mismo pasa con la ley que necesita vestirse de cuerpo legal para ofrecer garantías. Pasa con todas las tecnologías, hay cierta precipitación a propósito de PKI y me daría pena que quedara desprestigiada por no cuidarse suficientemente.

Arturo Ribagorda. No lo considero una tecnología, sino un sistema más complejo, que no sólo comprende aspectos técnicos sino también procedimientos de gestión y soluciones entre usuarios y proveedores de servicios de certificación. Hay dos aspectos en PKI, uno de ellos

es de aplicación empresarial, cuando cada empresa despliega su propio PKI para autenticaciones de empleados, funciones para garantizar la integridad y el no repudio de los documentos intercambiados entre empleados. El segundo aspecto es el de los PKI para establecer soluciones de confianza entre consumidor y empresas o entre empresas entre sí.

José Antonio Mañas. La llamada firma electrónica, que es la firma digital, busca una legislación por encima de la tecnología. Lo importante es que se consigan mecanismos judiciales de respaldo de las transacciones que se realizan. Lo que se vaya desarrollando en Europa tendrá que estar en la misma línea, allí está más evolucionado. PKI, como tecnología de entornos cerrados, en entornos maduros y operativos es muy interesante. En entornos de B2B es básico. Cuando los contratos entre las partes se reconozcan la firma mutuamente, son acuerdos válidos. Esta tecnología PKI se puede utilizar en relaciones empresariales sin complicaciones, pero es más complicado en abierto.

Arturo Ribagorda. En PKI, la existencia de una clave privada garantiza aún más el procedimiento, facilita las cosas en los grupos de B2B. Es una relación de confianza mutua, como tantos mecanismos contractuales. Es fácil si funciona como una relación entre amigos. El problema es al abrir el ámbito a gran escala.

Julián Inza. Un aspecto delicado de las jerarquías de certificación, cuando tienen alcance



Arturo Ribagorda: "El problema es que la seguridad no es demostrable, sólo se demuestra a "posteriori" la inseguridad"

Café de redacción

multinacional es que la seguridad de la autoridad de certificación raíz es especialmente importante, ya que afecta a la de todo el sistema, por lo que pueden plantearse conflictos de soberanía, si la seguridad de los sistemas de un país depende de la custodia de datos que están en otro.

En cuanto al comercio electrónico en España ¿cómo va, qué peligro hay de que se ralentice la sociedad de la información junto con su puesta en marcha, qué pasa con el B2B?

Arturo Ribagorda. Llegan las tecnologías tan deprisa que es necesario digerirlas. Si estableces una relación con una serie de proveedores, utilizas este tipo de comunicación. La tecnología IP agiliza el envío de documentos, facturas, albaranes. Cuando no hay una relación previa, es necesario recurrir a una firma electrónica que respalde la fiabilidad de las relaciones, tanto entre empresas como entre cliente y empresa. Las relaciones del cliente y banco cuentan con la seguridad que da el banco, es quien lo respalda. El cliente siempre puede reclamar a su banco.

José Antonio Mañas. Si el banco ve una posibilidad comercial, no quiere renunciar a ello. El B2B es fácil, el problema surge cuando es una relación efímera, si el B2B no está registrado.

Con UMTS ¿qué pasará con los datos móviles?

José Antonio Mañas. La tecnología trabaja en contra de la seguridad, ese es el problema. Pero lo que se establece es una fir-



Julián Inza: "El móvil se ha convertido en un dispositivo de confianza que está 'bajo control exclusivo de su titular' "

ma digital, un contrato de carácter vinculante, a través del móvil, entre origen y destino del mensaje. Está la parte de confianza con lo que está al otro lado de la línea telefónica. En definitiva, la seguridad tiene tres fases: preventiva, detectiva y reactiva. Se debe evitar pasar a las distintas fases, pero lo mejor es no pasar de la primera.

Julián Inza. El móvil se beneficia de un ritmo rápido de mejora de tecnologías, y con ello de mejora de seguridad. Además se ha convertido en un dispositivo de confianza que está "bajo control exclusivo de su titular" requisito que señala la ley de firma electrónica para los dispositivos de firma. Cada vez incluye más usos como elemento de

uso inmediato y cotidiano. Es cierto que a veces se critica la robustez del cifrado en la última milla, lo que puede justificarse en algunas ocasiones por criterios legales, pero eso no afecta a la capacidad de autenticación del teléfono que está fuera de toda duda.

A veces se confunden las funciones de confidencialidad y autenticación, aunque están claras desde un punto de vista académico. Por ejemplo, con las tarjetas de crédito, dado que el número identifica la tarjeta, se ha protegido este número mediante cifrado, cuando el objetivo era autenticar. En realidad, la autenticación debería hacerse por otro procedimiento y esto es lo que permite la telefonía móvil.

Arturo Ribagorda. No se va a mejorar la seguridad de la última milla con sistemas criptográficos fuertes, las fuerzas de seguridad no lo van a permitir, por muchas razones. El usuario, por otra parte, no tiene por qué saber qué sistema de seguridad tiene. Si usa un buen aparato, contará ya con ello, como con los coches. Hay un tema que me parece importante destacar y es que nuestros datos personales están fuertemente expuestos en nuestras sociedades de la información, pues son fáciles de recabar, cotejar y acumular para obtener perfiles de nuestra salud, creencias, ideologías, etc. Es conveniente tenerlo en cuenta y concienciar a la sociedad sobre ello. Si hay dos polos que preocupen son los de seguridad en el comercio electrónico y la seguridad de nuestros datos personales.