Seminario – Seguridad en desarrollo del Software

Tema: Comercio electrónico

Autor: Leudis Sanjuan

Seminario (seguridad en desarrollo del software)

¿Qué es el comercio electrónico?

Se denomina e-commerce o comercio electrónico a la forma de realizar transacciones de bienes y servicios por medio del uso de medios electrónicos; por ejemplo, a través de Internet.

[1]Por medio del comercio electrónico se pueden ofrecer los siguientes servicios:

- La contratación de bienes o servicios por vía electrónica.
- La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.
- La gestión de compras en red por grupos de personas.
- El envío de comunicaciones comerciales.
- El suministro de información por vía telemática.
- El vídeo bajo demanda, como servicio en el que el usuario puede seleccionar a través de la red, tanto el programa deseado como el momento de su suministro y recepción y, en general, la distribución de contenidos previa petición individual.

Por otro lado, el comercio electrónico dependiendo del participante se puede clasificar en:

- Empresa-Empresa: Conocido como B2B (business to business), que es lo mismo que relación electrónica entre dos empresas.

[1] Tomado de : http://guia.mercadolibre.com.co/1-concepto-general-comercio-electronico-4964-VGP

- Empresa-Consumidor: Conocido como B2C (business to consumer), que es lo mismo que comercio entre empresas y consumidores finales.
- Empresa-Administración: Conocido como B2A (business to administration). Se conoce también como Empresa-Gobierno y cubre las relaciones entre las empresas y organizaciones gubernamentales.
- Consumidor-Administración: Conocido por C2A (consumer to administration) y cubre las relaciones entre individuos y gobierno.
- Consumidor-Empresa: Conocido por C2B (consumer to business) y en este caso es el cliente individual quien inicia la relación comercial con la empresa.
- Consumidor-Consumidor: Conocido como C2C (consumer to consumer) y se trata de una relación comercial entre dos personas naturales.

Estándares usados para el intercambio de datos en el comercio electrónico

Para que pueda darse el comercio electrónico entre dos entidades es necesario definir reglas o estándar para el intercambio de datos. A continuación se mencionan lo más utilizados:

EDI: Es un conjunto coherente de datos para la transmisión por medios electrónicos, estructurados conforme a normas de mensajes acordadas, preparados en un formato capaz de ser leído por un computador y de ser procesado automáticamente y sin ambigüedad.

EDI ofrece intercambio electrónico de datos; es decir, intercambio entre sistemas de información, por medios electrónicos, de datos estructurados de acuerdo con normas de mensajes acordadas. A través del EDI, las partes involucradas

cooperan sobre la base de un entendimiento claro y predefinido acerca de un negocio común, que se lleva a cabo mediante la transmisión de datos electrónicos estructurados.

En el EDI, las interacciones entre las partes tienen lugar por medio de aplicaciones informáticas que actúan a modo de interfaz con los datos locales y pueden intercambiar información comercial estructurada. El EDI establece cómo se estructuran, para su posterior transmisión, los datos de los documentos electrónicos y define el significado comercial de cada elemento de datos. Para transmitir la información necesita un servicio de transporte adicional (por ejemplo, un sistema de tratamiento de mensajes o de transferencia de archivos). Debe destacarse que el EDI respeta la autonomía de las partes involucradas, no impone restricción alguna en el procesamiento interno de la información intercambiada o en los mecanismos de transmisión.

Para mayor información, visitar: http://www.monografias.com/trabajos/edi/edi.shtml

XML (Extensible Markup Language): es un metalenguaje extensible de etiquetas desarrollado por el World Wide Web Consortium (W3C). XML no es realmente un lenguaje en particular, sino una manera de definir lenguajes para diferentes necesidades.

XML es un estándar que se utiliza para el intercambio de información estructurada entre diferentes plataformas. Por esa razón es uno de los estándares usados en el comercio electrónico.

Para mayor información, visitar: http://es.wikipedia.org/wiki/Extensible_Markup_Language

XML/EDI

Durante los últimos años se ha puesto en evidencia que las empresas están en continua evolución y necesitan adaptarse a los nuevos mercados y tecnologías. Concretamente, Internet está obligando a reescribir las reglas sobre cómo comprar y vender, cómo cambiar bienes y servicios, etc.. Se están cambiando también las formas tradicionales de relación consumidor-proveedor, así sea el consumidor un comprador final, una organización, otra empresa o una organización gubernamental.

El ciclo original para procesar documentos debe estar constituido por: crear, transmitir, recibir, procesar usando programas individuales; esto se está reemplazando por el concepto de **objetos activos**, que tienen procesos asociados con ellos, dependiendo de la información que contengan. Por ejemplo, una factura no sólo contiene una copia de los datos almacenados en la base de datos, contiene un indicador que apunta al lugar de donde podemos obtener los datos y estos datos son buscados en su lugar de origen cada vez que la factura es procesada.

El simple hecho de redefinir el formato de los mensajes EDI para adecuarlo a Internet no es suficiente. XML/EDI busca definir un nuevo marco para el desarrollo del comercio electrónico. XML/EDI es la unión de cinco tecnologías. Cada componente añade la tecnología necesaria en la que el resto se apoya. Los componentes son:

- XML: proporciona la base.
- EDI. Proporciona todo lo desarrollado hasta el momento y la experiencia necesaria.
- Plantillas. Son reglas que hacen que el proceso de intercambio de información se pueda realizar. Las plantillas van incluidas dentro del documento XML como una sección especial y pueden ser fácilmente leídas e interpretadas. Se apoyan en los DTD's y definen qué operaciones realizar con los datos.

- Agentes. Interpretan las plantillas para realizar el trabajo necesario e interactúan con las transacciones y el usuario creando nuevas plantillas para cada tarea específica. Buscan y aplican la plantilla adecuada para los trabajos existentes. También utilizan los DTD's para determinar la forma de visualizar los datos en los correspondientes formularios. Principalmente los agentes son creados utilizando tecnologías como Java o ActiveX.

- Directorios. XML/EDI utiliza el concepto de directorios globales en Internet de forma automática. Este componente proporciona la base semántica para las transacciones comerciales y apoya a los agentes para realizar de forma automática y correcta la referencia a las entidades. En el directorio se incluyen también los DTD's. Los objetivos de los directorios son: ser un campo dentro de una determinada industria, compartir objetos, compartir DTD's y proporcionar una interfase para recuperar información. La combinación de estos cinco componentes proporciona un sistema que comunica información y no sólo datos, junto con las reglas para el procesamiento lógico.

Para mayor información, visitar: http://www.monografias.com/trabajos25/xml-edi/xml-edi.shtml

Seguridad y comercio electrónico

A continuación se enumeran varios aspectos relacionados con la seguridad y el comercio electrónico:

ISO 8730: se trata de la norma más antigua y más extendida en el tema de seguridad para las transferencias bancarias. La norma ISO 8730, utiliza cifrado de clave simétrica (DES) para autenticar transferencias. Los mecanismos de distribución de claves están regulados por la norma ISO 8732. Según ISO 8730 varios de los campos que integran una transferencia interbancaria deben estar incluidos en el mensaje de autenticación. Estos campos son:

- MAC: código de autenticación del mensaje, que consta de 8 dígitos hexadecimales.
- DMC: fecha en que se calculó la MAC
- IDA: identificador para que el receptor utilice la clave de autenticación
- MID: identificador del mensaje. Se trata de un número generado por el emisor a partir de DMC e IDA para protección contra la duplicación o la perdida del mensaje.
- Elementos específicos en el texto del mensaje, como valor de la transacción, entidades participantes, beneficiarios, etc..

Para mayor información, visitar: http://www.cosic.esat.kuleuven.be/publications/article-260.pdf

SWIFT (*Society for Worldwide Interbank Financial Telecommunication*): es una organización que tiene a cargo una red internacional de comunicaciones financieras entre bancos y otras entidades financieras. Ofrece un servicio para

transferencias de pagos con varios mecanismos de seguridad, como son el cifrado de líneas, la protección de acceso a la red mediante códigos y la posibilidad de cifrado en las conexiones usuarios-red.

Se utiliza para realizar operaciones de gran volumen: pago de nóminas, pago de pensiones; SWIFT ha creado la transferencia de archivos interbancarios (IFT). Los servicios de seguridad que este ofrece son: integridad del contenido, autenticación del mensaje original y confidencialidad. Se pueden usar varios algoritmos de clave simétrica o asimétrica, para lo que el emisor genera un "*token*" que contiene un identificador del algoritmo seleccionado. IFT ofrece funciones de seguridad extremo a extremo. La elección de los algoritmos de la gestión de claves no depende de SWIFT.

Para mayor información, visitar: http://www.swift.com/

ETEBAC 5: es un protocolo diseñado para su utilización en la banca francesa, que permite realizar de forma segura operaciones de cierta envergadura entre instituciones financieras y sus clientes. ETEBAC 5 utiliza un protocolo de transferencia de archivo llamado PeSIT. Este acepta criptografía con clave simétrica o asimétrica, DES y RSA respectivamente.

Entre los servicios de seguridad ofrecidos por ETEBAC 5 están la autenticación recíproca entre el banco y el cliente, la integridad de los datos con una MAC, el no repudio recíproco y la confidencialidad de la transferencia con DES.

ETEBAC 5 contiene muchos elementos que proporcionan gran flexibilidad y seguridad para los servicios ofrecidos. Por ejemplo, no sólo se firma el contenido del archivo, sino también el MAC del identificador del archivo. ETEBAC 5 ha sido el primer estándar especificado en incluir RSA como criptografía de clave pública.

Para mayor información, visitar: http://www.etebac.com/US/Etebac_5.htm

Seminario (seguridad en desarrollo del software)

PCI DSS: *Payment Card Industry Data Security Standard* (PCI DSS), es un estándar de seguridad que define el conjunto de requerimientos para gestionar la seguridad, definir políticas y procedimientos de seguridad, arquitectura de red, diseño de software y todo tipo de medidas de protección que intervienen en el tratamiento, procesado o almacenamiento de información de tarjetas de crédito. Su finalidad es la reducción del fraude relacionado con las tarjetas de crédito e incrementar la seguridad de estos datos.

PCI DSS es el resultado del esfuerzo del *PCI Security Standards Council* (PCI SSC) formado por las principales compañías emisoras de tarjetas de crédito (Visa, Mastercard, American Express, JCB y Discover), para forzar y facilitar a comercios, proveedores de servicios y bancos a reducir el riesgo de fraude con tarjetas de crédito, mediante la protección de las infraestructuras que procesan, transmiten o almacenan datos relativos a tarjetas de crédito.

Toda empresa u organización (centros comerciales, empresas de comercio electrónico que operan por Internet, entidades financieras y las empresas que gestionan medios de pago, etc.) que almacene, procese o transmita datos de tarjetas de crédito deben cumplir este estándar.

El estándar está compuesto por seis categorías o secciones, en los que se definen doce requisitos para construir una infraestructura confiable para el procesado de transacciones mediante tarjetas de pago. A continuación se menciona cuales son las secciones y los requisitos:

Seminario (seguridad en desarrollo del software)

PSI DSS	
Secciones	**Requerimientos**
Construir y Mantener una red segura.	Instalar y mantener un cortafuegos y su configuración para proteger la información de tarjetas.
	No emplear parámetros de seguridad y usuarios del sistema por defecto.
Protejer los datos de las tarjetas.	Proteger los datos almacenados de las tarjetas.
	Cifrar las transmisiones de datos de tarjetas en redes abiertas o públicas.
Mantener un programa de Gestión de vulnerabilidades.	Usar y actualizar regularmente el software antivirus.
	Desarrollar y mantener de forma segura sistemas y aplicaciones.
Implementar medidas de control de acceso.	Restringir el acceso a la información de tarjetas según la premisa " need-to-know".
	Asignar un único ID a cada persona con acceso a computadores.
Monitorizar y testear regularmente las redes.	Restringir el acceso físico a la información de tarjetas.
	Auditar y monitorizar todos los accesos a los recursos de red y datos de tarjetas.
Mantener una política se seguridad de la informacón.	Testear de forma regular la seguridad de los sistemas y procesos.
	Mantener una política que gestione la seguridad de la información.

Figura 1: Requerimientos y categoría de PSI DSSS. Tomado de: http://www.avisortech.com/pci_dss_services.asp

Para mayor información, visitar: http://www.shopfactory.com/contents/es/p779_-PCI-CISP-what-is-it.html

Recomendaciones del manejo de pagos en el comercio electrónico

A continuación mencionaremos las recomendaciones de OWAPS para el desarrollo de aplicaciones que utilizan pagos electrónicos:

- Procese las transacciones en línea inmediatamente o pase el procesamiento a una tercera parte competente.
- Nunca almacene ningún número de tarjeta de crédito. Si deben almacenarse, debe seguir las directivas de PCI al pie de la letra. Sin embargo, le recomendamos que en la medida de lo posible, no almacene datos de tarjetas de crédito.
- Si usted usa un servidor compartido para su sitio, no puede cumplir con las directivas PCI. Debe tener su propia infraestructura para cumplir con las directivas PCI.

Números de autorización

Después del procesamiento correcto de una transacción a usted se le asigna un número de autorización. Este es único por transacción y no tiene un valor propio intrínseco. Es seguro almacenar este valor, escribirlo en logs, o enviarlo a través de e-mail al cliente.

Manejando devoluciones de pagos

La única razón de negocio para almacenar números de tarjetas de crédito son las devoluciones de pagos. Sin embargo, tiene diversas responsabilidades si facilita devoluciones de pagos:

- Debe seguir los términos del acuerdo de su comercio. La mayoría de los acuerdos de comercio requieren que usted tenga las autorizaciones firmadas de derechos originales de sus usuarios de tarjetas de crédito. Este papel firmado le ayudará en caso de algún problema de cobros con el cliente.
- Es una buena práctica cifrar los números de tarjetas de crédito. Este es un requisito obligado en las directivas PCI.
- Se debe limitar los términos de la devolución de pagos a menos de un año.
- Se debe eliminar los detalles de la tarjeta de crédito tan pronto como el acuerdo haya finalizado.
- El problema con el cifrado es que usted debe ser capaz de descifrar los datos posteriormente en los procesos del negocio. Cuando se elige un método para almacenar las tarjetas de forma cifrada, recuerde que no hay ninguna razón por la cual el servidor Web front-end necesite ser capaz de descifrarlas.

Mostrando partes de la tarjeta de crédito

PCI sólo permite la presentación de los primeros seis dígitos (BIN) o los últimos cuatro de las tarjetas de créditos. OWAP recomienda no almacenar la tarjeta de crédito de ninguna manera. A continuación se enumeran las razones:

- Si su empresa envía la factura por correo electrónico, es posible que envié con la factura el número de la tarjeta de crédito. Esta situación puede ser utilizada por su atacante al interceptar el correo electrónico con la factura.
- Si su empresa utiliza un *call center* para verificar una transacción, es posible que los trabajadores de esta oficina (por lo general, personal contratado temporalmente) conozca el número de la tarjeta de crédito sólo revisando la información consignada en el sistema.

- Si su empresa guarda en un log las transacciones electrónicas, y en este queda registrado el número de la tarjeta de crédito de los compradores, es posible que un atacante ingrese a ese log y obtenga toda la información de las tarjetas de crédito.
- En países con pequeña cantidad de instituciones bancarias, los números institucionales BIN están limitados. Por lo tanto, es posible adivinar números BIN válidos y reconstruir el número de la tarjeta incluso si gran parte del número de la tarjeta se ha ocultado.

Corrección y mantenimiento

PCI exige que a más tardar al mes de la publicación de un parche, este sea aplicado. Igualmente exige tener antivirus con versión actualizada.

Revocaciones

Hay dos fraudes potenciales en las revocaciones: un usuario malintencionado poniendo dinero de la cuenta de la organización a una tercera parte y un atacante que ha descubierto con éxito como usar un proceso automático de revocación para “reembolsar” dinero que no le pertenece, por ejemplo usando números negativos.

Las revocaciones deberían siempre realizarse a mano; además, deberían ser firmadas por dos empleados distintos. Esto reduce el riesgo de fraude interno y externo.

Es esencial asegurarse de que todos los valores estén dentro de los límites y la autoridad de firma está asignada apropiadamente.

Devolución de cobros

Si el sistema que está desarrollando contempla la opción de devolución, tenga en cuenta las siguientes recomendaciones:

- El dinero no es negativo. Use una función para validar cifras positivas o ingreso del número cero.
- Todas las devoluciones y revocaciones requieren registros, auditorias y autorizaciones manuales.
- No debería haber códigos en su sitio Web para revocaciones o devoluciones.
- No envíe el material hasta que no tenga un código de autorización de la pasarela de pago.
- Gran parte de las tarjetas de crédito tienen una fuerte relación entre los números BIN y el país de la institución que la emitió. Considere firmemente el no enviar materiales a tarjetas con BIN fuera-del-país
- Para bienes de gran valor, considere realizar una confirmación de la compra antes de debitar.
- Registre todas las transacciones y publique en su sitio una nota que indique que cuenta con toda una infraestructura para detectar fraudes en las transacciones.

Bibliografía

Serra, Artur. Next Generation Community Networking. En “Digital Cities”. Toru Ishida., Katherine Isbister Ed., Springer, 2000

HAMMER/OWENS, “Promoting Tax Competition”, Tax Notes International,vol.22, nº11, 2001.

Lizama P. L., León R. Comercio Electrónico Seguro. Memoria Electrónica del Primer Congreso Nacional de Informática y Sistemas. México.2004

http://www.monografias.com/trabajos/edi/edi.shtml

http://es.wikipedia.org/wiki/Extensible_Markup_Language

http://www.monografias.com/trabajos25/xml-edi/xml-edi.shtml

http://www.cosic.esat.kuleuven.be/publications/article-260.pdf

http://es.wikipedia.org/wiki/ISO_9362

http://www.swift.com/

http://www.etebac.com/US/Etebac_5.htm

http://www.shopfactory.com/contents/es/p779_-PCI-CISP-what-is-it.html