Seguridad en Transacciones Financieras y Detección de Intrusos en Internet

La seguridad de las operaciones en Internet es un aspecto que preocupa en gran medida a los usuarios de este medio, en particular en aquellos casos en los que se realizan transacciones financieras o se transmiten datos de carácter privado. Desde el momento en que una computadora se conecta a Internet, se abren ante los usuarios toda una nueva serie de posibilidades. Sin embargo, éstas traen consigo toda una serie de nuevos, y en ocasiones complejos, tipos de ataque o intrusiones. Por ejemplo, entre los *fraudes* o ataques más frecuentes de ingeniería social podemos citar: *Phishing* (suplantación de identidad, *p. ej. por correo-e,* para obtener información de la víctima), *Key Logger* (el delincuente graba de forma *invisible* todo lo que se escribe en el teclado), *Vishing* (llamadas telefónicas a la víctima para obtener información personal) y *Smishing* (mensajes de texto para engañar a la víctima).

Actualmente, los bancos tienen a su disposición plataformas digitales para que los usuarios, sin necesidad de ir al banco, puedan realizar sus *transacciones financieras* con *seguridad* vía Internet. Sin embargo, toda transacción segura por la red debe contemplar los aspectos de *autenticidad, integridad, confidencialidad y no repudio* (W. Stallings, 2016). Son varios los sistemas y tecnologías que se han desarrollado para intentar implementar estos aspectos en las transacciones financieras. De los métodos más utilizados, a la hora de proporcionar a un sitio Web medidas de seguridad adicionales (*p, ej.,* el protocolo *https (hypertext transfer protocol secure)*), es la utilización de los protocolos SSL (*Secure Sockets Layer*, 'SSL' por sus siglas en inglés) y TLS (Transport Layer Security, 'TLS' por sus siglas en inglés) su sucesor. TLS permite la confidencialidad y la autentificación en las transacciones financieras en Internet, siendo utilizado principalmente en aquellas transacciones en la que se intercambian datos sensibles, como números de tarjetas de crédito o contraseñas de acceso a sistemas privados. TLS es un sistema de protocolos de carácter general que está basado en la aplicación conjunta de criptografía simétrica, criptografía asimétrica (de llave pública), certificados y firmas digitales para conseguir un canal o medio seguro de comunicación vía Internet (W. Stallings, 2016). TLS funciona de forma que el navegador del consumidor cifra automáticamente la información de la orden de pago antes de enviarla al comercio. Una vez enviada, "únicamente el destinatario" podrá acceder a esta información que quedará protegida. La identidad del servidor Web seguro (y a veces también del usuario cliente) se consigue mediante un *certificado digital* correspondiente, del que se comprueba su validez antes de iniciar el

intercambio de datos sensibles (*autenticación*), mientras que de la seguridad de integridad de los datos intercambiados se encarga la firma digital mediante funciones *Hash* y la comprobación de resúmenes de todos los datos enviados y recibidos (W. Stallings, 2016).

Así mismo, existen otro tipo de ataques que se manifiestan como *anomalías* en el comportamiento usual del flujo de datos en una red de comunicaciones. Por lo tanto, prevención (antes), detección (durante) y reacción (después) constituyen tres conceptos clave en todo sistema de protección que pretenda ofrecer soluciones integrales de seguridad. Es por ello que es necesario no sólo contar con un buen *firewall* (*Un firewall es un elemento de hardware o software utilizado en una red de computadoras para permitir o denegar transmisiones de una red a la otra*) sino también con un sistema para detección de intrusos (*Intrusion Detection System, 'IDS' por sus siglas en inglés*) para reducir los posibles ataques a una red. Debido a que la seguridad de una red de comunicaciones es vulnerable a ataques e intrusiones, el uso de *firewalls* ya no es suficiente para frenar este fenómeno. Es por ello que se ha optado por el uso de sistemas capaces de observar y analizar el tráfico en una red de comunicaciones para la detección de intrusiones (D. Limon-Cantu y V. Alarcon-Aquino, 2021).

Los IDS tienen tres componentes principales: ***fuentes de información*** *(monitoreo de intrusiones),* ***análisis*** *(detección de intrusos - decisión) y* ***respuesta*** *(acciones).* De estos tres componentes la función de análisis es la que se encarga de decidir cuál de los eventos registrados es realmente una intrusión. Los métodos más comunes para realizar el análisis de intrusiones son el *de uso de firmas y la detección de anomalías* (D. Limon-Cantu y V. Alarcon-Aquino, 2021). El análisis de uso de firmas tiene la limitante de que únicamente puede ser capaz de detectar ataques conocidos y es la técnica más usada por la mayoría de los sistemas comerciales. Las firmas utilizadas en estos IDS usualmente son simples patrones que permiten detectar ataques previamente registrados. Mientras que la detección de anomalías, usada de forma limitada por un pequeño número de IDS, se centra en identificar comportamientos inusuales en una computadora o una red y funciona asumiendo que los ataques son diferentes a la actividad normal. Esto es, la detección de anomalías permite detectar ataques nuevos y totalmente desconocidos (D. Limon-Cantu y V. Alarcon-Aquino, 2021).

En el campo de detección de anomalías se han desarrollado distintos diseños que permiten trabajar de manera eficiente. Por ejemplo, recientemente se han desarrollado IDS basados en el comportamiento de sistemas inmunes artificiales (*Artificial Inmune Systems*, 'AIS' por sus siglas en inglés). Esto es, el sistema inmune humano se compone de un conjunto de órganos y células, cuya finalidad es proteger a nuestro cuerpo contra enfermedades, infecciones y el mal funcionamiento de otras células. En el caso de los IDS, el comportamiento de las células inmunes tiene la finalidad de observar el tráfico en el Internet y detectar anomalías de manera proactiva (D. Limon-Cantu y V. Alarcon-Aquino, 2021). Sin embargo, aún no se ha alcanzado un estado definitivo en el cual la detección de intrusos se lleve a cabo de forma confiable.

Es claro entonces que los sistemas informáticos no son todavía 100% seguros. Desde el punto de vista técnico, la seguridad está en manos de la dirección de las organizaciones y, en última instancia, en cada uno de nosotros. Por ello, es importante construir una *cultura de seguridad informática* en todos los usuarios del Internet. La seguridad siempre será relativa al tipo de servicios que se quieran ofrecer a los usuarios autorizados, según se establezca en la política de seguridad de la empresa.

Referencias:

- D. Limon-Cantu, V. Alarcon-Aquino (2021). Multiresolution Dendritic Cell Algorithm for Network Anomaly Detection, in PeerJ Computer Science. https://doi.org/10.7717/peerj-cs.749
- W. Stallings (2016), Cryptography and Network Security: Principles and Practices, 7th Edition, Pearson.

Sobre el autor:

Vicente Alarcón Aquino, Doctor en Ingeniería Eléctrica y Electrónica, por el Imperial College London (University of London), Londres, Inglaterra. Es Senior Member del IEEE, miembro de la Academia Mexicana de Ciencias y del Sistema Nacional de Investigadores (SNI) nivel 1. Profesor de tiempo completo en el departamento académico de computación, electrónica y mecatrónica de la Universidad de las Américas Puebla. Ha participado como revisor de artículos científicos para revistas indexadas y congresos internacionales. Fue Editor Huésped de la revista Journal of Universal Computer Science (Q2) y actualmente es Editor Asociado de la revista IEEE Access (Q1) y de la revista PeerJ Computer Science (Q1). Tiene más de 180 artículos en congresos y revistas científicas internacionales. Siendo sus líneas de investigación Ciberseguridad, monitoreo de redes, detección de anomalías, análisis con wavelets y aprendizaje automático.

Contacto: vicente.alarcon@udlap.mx