UNIVERSIDAD NACIONAL DE LA MATANZA

Departamento de Ingeniería e Investigaciones Tecnológicas

Seguridad y Calidad en Aplicaciones Web

Unidad N° 0: Anexo Seguridad

Fuente: "Criptografía y Seguridad en Computadoras", Manuel José Lucena López. Capitulo 2.6, Seguridad en sistemas informaticos

Seguridad en sistemas informáticos

Todo sistema que procese, almacene o transmita información tiene que cumplir una serie de requisitos. En primer lugar, ha de preservar la información frente a alteraciones tanto fortuitas como deliberadas, debidas a fallos en el software o en el hardware, provocadas por agentes externos —incendios, interrupciones en el suministro eléctrico, etc.— o por los propios usuarios. En segundo lugar, es necesario evitar accesos no autorizados tanto al sistema como a su contenido. Finalmente, el sistema debe garantizar que la información esté disponible cuando sea necesario. Estos tres requerimientos quedan recogidos en los conceptos de integridad, confidencialidad y disponibilidad de la información respectivamente, y son los que hacen que podamos considerar seguro a un sistema.

Por lo tanto, garantizar la seguridad de un sistema informático es un objetivo mucho más amplio y complejo que la simple protección de los datos mediante técnicas criptográficas. De hecho, hemos de tener en cuenta múltiples factores, tanto internos como externos. En esta sección comentaremos algunos de los más relevantes, de manera no exhaustiva.

Quizás la primera pregunta que haya que responder a la hora de identificar los requerimientos de seguridad de un sistema sea la siguiente: ¿está conectado con el exterior? En este sentido podemos hacer la siguiente subdivisión:

1. Sistemas aislados. Son los que no tienen acceso a ningún tipo de red. De unos años a esta parte se han convertido en minoría, debido al auge que han experimentado las redes, especialmente Internet. En ellos suele ser suficiente la implementación de mecanismos de control de acceso físico —cerraduras, videovigilancia, etc.—, junto con protocolos adecuados de gestión de los privilegios de cada usuario, si es que hay más de uno.

2. Sistemas interconectados. Constituyen el caso más general y extendido. De hecho, hoy por hoy casi cualquier ordenador está conectado a alguna red —y cada vez más dispositivos de uso cotidiano son auténticas computadoras: consolas de videojuegos, teléfonos celulares, reproductores multimedia, etc.—, enviando y recogiendo información del exterior casi constantemente. Esto hace que las redes de ordenadores sean cada día más complejas, y presenten auténticos desafíos de cara a gestionarlos adecuadamente.

En cuanto a las cuestiones de seguridad propiamente dichas, citaremos algunas de las más relevantes:

1. Seguridad física. Englobaremos dentro de esta categoría a todos los asuntos relacionados con la salvaguarda de los soportes físicos de la información, más que de la información propiamente dicha. En este nivel estarían, entre otras, las medidas contra incendios y sobrecargas eléctricas, la prevención de ataques terroristas, las políticas de copias de respaldo (*backups*), etc. También se suelen tener en cuenta dentro de este punto aspectos relacionados con la restricción del acceso físico a las computadoras.

2. Seguridad de los canales de comunicación. Los canales de comunicación rara vez se consideran seguros. Debido a que normalmente escapan a nuestro control, ya que pertenecen a terceros, resulta imposible asegurarse de que no están siendo escuchados o intervenidos. En la inmensa mayoría de los casos tendremos que establecer mecanismos de protección de la información capaces de cumplir su cometido en canales manipulados, e incluso hostiles.

3. Control de acceso a los datos. Como ya hemos dicho, un sistema informático debe permitir acceder a la información únicamente a agentes autorizados. Generalmente, diferentes usuarios tendrán acceso a distinta información, por lo que una simple restricción del acceso al sistema no será suficiente, sino que habrá que establecer privilegios individualizados, así como mecanismos que, como el cifrado, permitan preservar la confidencialidad incluso frente a accesos físicos a los dispositivos de almacenamiento.

4. Autentificación. Para garantizar su correcto funcionamiento, es necesario poder verificar de forma fiable la autenticidad de los distintos elementos que interactúan en un sistema informático: la información que se recibe, envía y almacena, los usuarios que acceden a él, y eventualmente los dispositivos que se comunican con el mismo. En los dos últimos casos, hemos de evitar a toda costa que se produzcan problemas de *suplantación de identidad*.

5. No repudio. Cuando se recibe un mensaje no sólo es necesario poder identificar de forma unívoca al remitente, sino que éste asuma todas las responsabilidades derivadas de la información que haya podido enviar, por ejemplo en la firma de un contrato o en una transacción comercial. En este sentido es fundamental impedir que el emisor pueda *repudiar* un mensaje, es decir, negar su autoría sobre el mismo.

6. Anonimato. Es, en cierta manera, el concepto opuesto al de no repudio. En determinadas aplicaciones, como puede ser un proceso electoral o la denuncia de violaciones de los derechos humanos en entornos dictatoriales, es crucial garantizar el anonimato del ciudadano para poder preservar su intimidad y su libertad. Sin embargo, el anonimato también puede ser empleado para practicar actividades delictivas con total impunidad, lo cual lo convierte en una auténtica arma de doble filo. En cualquier caso, se trata una característica realmente difícil de conseguir, y que no goza de muy buena fama, especialmente en países donde prima la *seguridad nacional* sobre la libertad y la intimidad de los ciudadanos. Si a eso le sumamos el interés que para muchas empresas tiene conocer los perfiles de actividad de sus clientes, de cara a personalizar sus ofertas, entenderemos por qué apenas hay iniciativas serias en la industria para proporcionar servicios de este tipo.