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

Seguridad

El concepto de seguridad en la información es mucho mas amplio que la simple a´ protección de los datos a nivel lógico. Para proporcionar una seguridad real hemos de tener en cuenta múltiples factores, tanto internos como externos. En primer lugar habría que caracterizar el sistema que va a albergar la información para poder identificar las amenazas, y en este sentido podríamos hacer la siguiente subdivisión:

1. *Sistemas aislados.* Son los que no están conectados a ningún tipo de red. De unos anos a esta parte se han convertido en minoría, debido al auge que ha experimentado Internet.

2. *Sistemas interconectados.* Hoy por hoy casi cualquier ordenador pertenece a alguna red, enviando y recogiendo información del exterior casi constantemente.Esto hace que las redes de ordenadores sean cada día mas complejas y supongan un peligro potencial que no puede en ningún caso ser ignorado.

En cuanto a las cuestiones de seguridad que hemos de fijar podríamos clasificarla de la siguiente forma:

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 de acceso físico a las computadoras unicamente a personas autorizadas.

2. *Seguridad de la información*. En este apartado prestaremos atención a la preservación de la información frente a observadores no autorizados. Para ello podemos emplear tanto criptografía simétrica como asimétrica, estando la primera unicamente indicada en sistemas aislados, ya que si la empleáramos en redes, al tener que transmitir la clave por el canal de comunicación, estaramos asumiendo un riesgo excesivo.

3. *Seguridad del canal de comunicación.* Los canales de comunicación rara vez se consideran seguros. Debido a que en la mayora de los casos escapan a nuestrocontrol, ya que pertenecen a terceros, resulta imposible asegurarse totalmente de que no están siendo escuchados o intervenidos.

4. *Problemas de autentificación*. Debido a los problemas del canal de comunicación,es necesario asegurarse de que la información que recibimos en la computadora viene de quien realmente creemos que viene, y que además no ha sido alterada.Para esto se suele emplear criptografía asimétrica en conjunción con funciones resumen (hash).

5. *Problemas de suplantación*. En las redes tenemos el problema añadido de que cualquier usuario autorizado puede acceder al sistema desde fuera, por lo quehemos de confiar en sistemas fiables para garantizar que los usuarios no estén siendo suplantados por intrusos. Para conseguir esto normalmente se emplean mecanismos basados en contraseñas.

6. *No repudio*. Cuando se recibe un mensaje no solo es necesario poder identificar de forma unívoca al remitente, sino que este asuma todas las responsabilidades derivadas de la información que haya podido enviar. En este sentido es fundamental impedir que el emisor pueda repudiar un mensaje, es decir, negar suautora sobre el.

7. *Anonimato*. Es, en cierta manera, el concepto opuesto al del no repudio. En determinadas aplicaciones, como puede ser un proceso electoral o la simple 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. Es una característica realmente difícil de conseguir, y desafortunadamente no goza de muy buena fama, especialmente en países donde prima la seguridad nacional sobre la libertad y la intimidad de los ciudadanos.