Unidad 1 / Escenario 1

Lectura fundamental

Conceptos básicos de seguridad de la información

Contenido

Palabras clave: confidencialidad, integridad, disponibilidad, autenticación, autorización y no repudio.

1. Introducción

La seguridad en el ciclo de desarrollo del software, al igual que en otros componentes tecnológicos como las redes de datos, los servidores o las bases de datos, está enfocada en garantizar los pilares de la seguridad de la información.

En otras palabras, la seguridad en el ciclo de desarrollo de software busca que la información almacenada, transportada o procesada a través del software cuente con los niveles adecuados de confidencialidad, integridad y disponibilidad. Sin embargo, es necesario complementar esta definición básica de seguridad mediante la inclusión de otros tres conceptos básicos, los cuales son: autenticación, autorización y no repudio.

Las fallas de seguridad en el software siempre son asociables a uno o varios de los seis conceptos básicos, es decir a la confidencialidad, integridad, disponibilidad, autenticación, autorización y/o no repudio, por lo que estos son la base para entender que es seguridad en el ciclo de desarrollo de software, motivo por el cual en las siguientes secciones de la lectura profundizaremos cada uno de estos conceptos.

Figura 1. Conceptos de seguridad

Fuente: elaboración propia

2. Conceptos básicos de seguridad

2.1. Confidencialidad

El concepto

La confidencialidad es uno de los tres pilares básicos de la seguridad de la información junto con la integridad y la disponibilidad. Tiene como objetivo garantizar que la información únicamente sea accedida o esté disponible para los individuos, entidades o procesos autorizados.

Ejemplos

A lo largo de la historia se han conocido diferentes incidentes de seguridad de la información que claramente representan una pérdida o compromiso de la confidencialidad de la información, entre ellos:

- El muy sonado caso Wikileaks, un sitio web mediante el cual el periodista Julian Assange publicó en julio de 2007 documentos clasificados del gobierno de los Estados Unidos. La publicación de estos documentos representa una pérdida de confidencialidad ya que al ser publicados de manera libre en Internet son accesibles por cualquier persona, contrario a los que seguramente definió el gobierno de los Estados Unidos.
- En marzo de 2016, el FBI contrató a un hacker para desbloquear el teléfono celular del terrorista Syed Rizwan Farook, accediendo de esta manera a los mensajes, correos electrónicos y fotos almacenados en el dispositivo (Clarín, 2017). Más allá de la necesidad de acceder al teléfono para adelantar la investigación, lo que llama la atención es que ante la negativa de la compañía Apple por desbloquear el teléfono, el FBI accedió a una información que el ciudadano pretendía mantener en secreto, lo cual representó una pérdida de confidencialidad.
- En el ámbito empresarial existen muchos otros ejemplos de pérdida de confidencialidad, como los que se muestran a continuación y que no necesariamente implican medios tecnológicos:
    - El personal de nómina revela los salarios para los diferentes cargos y roles de la compañía de manera verbal.
    - Personal del área comercial de una compañía sostiene una conversación en un lugar público, como un ascensor, revelando los costos de un proyecto que la compañía tiene como objetivo.

- Un exempleado de una empresa revela la información de sus procesos, diseños y metodologías en su nuevo empleo, es decir se aprovecha del know-how de su antiguo empleador, una información que claramente debe ser confidencial.

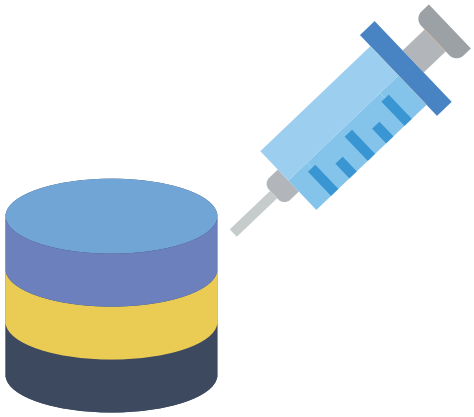

Figura 2. Representación de Inyección SQL
Fuente: elaboración propia

¿Sabía qué...?

Uno de los ataques más utilizados por los criminales para acceder sin autorización a los datos es la inyección de código o SQLInyection.

2.2. Integridad

El concepto

La integridad es uno de los tres pilares básicos de la seguridad de la información junto con la confidencialidad y la disponibilidad. Tiene como objetivo garantizar que la información se mantenga precisa y completa, lo que en otras palabras significa que no sea modificada sin autorización.

Ejemplos

Observemos algunos ejemplos de incidentes de seguridad de la información que claramente representan una pérdida o compromiso de la integridad de la información:

- En el año 2011, la página oficial del ejército colombiano sufrió un ataque por parte del grupo "Safety Last Group & Islam 47" (Semana, 2011). Como resultado, la página fue modificada sin autorización, pues una imagen de un soldado exhibiendo su lengua reemplazó los contenidos normales de la página.
- Stuxnet es un software malicioso creado para modificar sistemas de control industrial (SCI), como lo son plantas nucleares. En junio de 2010 este malware fue detectado en diferentes países, evidenciando su capacidad para modificar y reprogramar diferentes SCI (El País, 2010).
- En el ámbito empresarial existen muchos otros ejemplos de pérdida de integridad, como los que se muestran a continuación y que no necesariamente implican medios tecnológicos:
  - Un empleado expuso su portátil a un detector de metales o a radicación extrema, lo cual dañó algunos de los datos almacenados en el quipo, modificándolos y afectando la integridad de los mismos.
  - Un computador de la compañía se ha infectado por un malware o código malicioso que convierte todos los archivos en accesos directos.
  - Un estudiante de un colegio observó que su profesor se levantó de su computador, dejando abierto el sistema de ingreso de notas. El estudiante modificó sus notas a las máximas calificaciones posibles.

2.3. Disponibilidad

El concepto

La disponibilidad es uno de los tres pilares básicos de la seguridad de la información junto con la confidencialidad y la integridad. Tiene como objetivo garantizar que la información esté disponible cuando se necesite, garantizando que esta sea accesible y utilizable por demanda cuando así sea requerido.

Ejemplos

Observemos algunos ejemplos de incidentes de seguridad de la información que afectaron la disponibilidad de la información:

- En octubre de 2017 el sitio web del diario El País de España sufrió una serie de ataques que impidieron o "tumbaron" el servicio por más de dos horas, impidiendo así a sus miles de lectores acceder a sus noticias y contenidos (El Tiempo, 2017). Este incidente claramente representa una pérdida de disponibilidad de la información, pues esta no estaba accesible a sus usuarios finales.
- En mayo de 2017 múltiples empresas a nivel mundial fueron afectadas por un malware del tipo Ransomware llamado WannaCry, el cuál cifró los datos y solicitaba un pago a cambio de devolverlos (El País, 2017). Este tipo de malware, también conocido como "secuestrador" de datos, impide el acceso a la información, lo cual representa una pérdida de disponibilidad.
- En el ámbito empresarial existen muchos otros ejemplos de pérdida de disponibilidad, como los que se muestran a continuación y que no necesariamente implican medios tecnológicos:
  - Un empleado fue despedido de una empresa y como "venganza" ha decidido eliminar todos los datos que maneja, antes de que le deshabiliten sus usuarios de acceso a los sistemas de información.
  - El presidente de la compañía ha sido víctima del robo de su equipo portátil mientras realizaba un viaje de trabajo, desafortunadamente no contaba con copias de respaldo de la información allí almacenada.
  - Un incendio ha incinerado todos los servidores de la compañía, desafortunadamente el centro de datos no contaba con un sistema de detección y extinción de incendios.

¿Sabía qué...?

los ataques de denegación de servicio están orientados a comprometer la disponibilidad de las aplicaciones y por ende de la información.

Figura 3. Representación de una aplicación no disponible

Fuente: elaboración propia

2.4. Autenticación

El concepto

La autenticación consiste en verificar que alguien o algo es quien dice ser. Típicamente en las aplicaciones, la autenticación se realiza mediante la utilización de un usuario y contraseña, sin embargo existen otras formas de hacerlo, mediante la utilización de los 3 "Factores de Autenticación":

Figura 4. Factores de autenticación

Fuente: elaboración propia

La autenticación fuerte consiste en combinar al menos 2 de los 3 factores de autenticación.

Ejemplos

- Algo que se tiene y se carga: se refiere a objetos físicos con los que puede contar un usuario, como lo son:
  - Tokens físicos como los suministrados por los bancos para realizar transacciones financieras como pagos o transferencias de dinero.
  - Tarjetas de proximidad, típicamente utilizadas en control de acceso físico a edificios e instalaciones como centros de datos.
  - Teléfonos inteligentes con tecnología NFC o con tokens lógicos instalados.
- Algo que se es como persona: se refiere a las características biométricas de los usuarios, dentro de las que se encuentran:
  - Huella.
  - Iris.
  - Reconocimiento facial.
  - La forma de la mano.
  - Voz
  - Latidos del corazón.
- Algo que se conoce: se refiere a algo que saben los usuarios, como los son:
  - Contraseñas
  - Pines, por ejemplo, los de 4 dígitos utilizados como claves de tarjetas de débito.
  - Patrones de desbloqueo, como los utilizados en los teléfonos Android.
  - Respuestas a preguntas de seguridad.

¿Sabía qué...?

Las contraseñas siempre se pueden vulnerar, solo es cuestión de tiempo. Por eso es importante combinar 2 o más factores de autenticación para incrementar significativamente la seguridad en el acceso a las aplicaciones.

Figura 5. Autenticación representada con una huella digital

Fuente: elaboración propia

2.5. Autorización

El concepto

La autorización consiste en otorgar a los usuarios los permisos que requieren una vez se han superado la autenticación. En otras palabras, la autenticación son los perfiles de los usuarios, los cuales se deben construir basados en la regla o principio del menor privilegio, es decir que se les otorguen los permisos estrictamente necesarios para el desarrollo de sus labores.

Ejemplos

- En la plataforma educativa del Politécnico Gran Colombiano los estudiantes tienen acceso a leer las calificaciones, pero no a modificarlas. Los profesores y tutores pueden crear y modificar calificaciones, pues es una de las labores para las cuáles han sido contratados.
- Los perfiles de acceso se pueden diseñar utilizando matrices. Observemos un ejemplo de cómo se pueden diseñar los perfiles basados en las necesidades de sus roles:

Tabla 1. Matriz ejemplo de diseño de perfiles

	Funciones		
Nombre del perfil	**Ingresar notas**	**Leer notas**	**Modificar notas**
Tutor	Si	Si	Si
Estudiante	No	Si	No
Auditor	No	Si	No
Coordinador	No	Si	Si

Fuente: elaboración propia

- Uno de los controles más efectivos para la prevención de los fraudes financieros es la segregación de funciones, que no es más otra cosa que una adecuada selección de roles y permisos dependiendo de la necesidad de hacer/saber evitando que hayan conflictos de interés. Por ejemplo, el usuario que ingresa una factura, no debe ser la misma persona que apruebe su pago, pues de ser así podría cometer fraudes con facilidad. De igual manera, deberían existir diferentes personas que aprueben los pagos de las facturas dependiendo del monto, pagos muy grandes deberían ser aprobados por directores o inclusive por el gerente o presidente de la compañía.

2.6. No Repudio

El concepto

El no repudio es el último de los conceptos básicos de seguridad de la información, sin que esto quiera decir que es menos importante. El no repudio básicamente consiste en que un usuario de una aplicación no pueda negar (o repudiar) que ha realizado una acción. En otras palabras, es la capacidad de demostrar que un usuario ejecutó de manera inequívoca algo dentro de la aplicación, por lo que es información básica al momento de realizar investigaciones.

Figura 6. Datos bajo la lupa

Fuente: elaboración propia

Ejemplos

- Los logs o registros de auditoría almacenan la trazabilidad de las acciones ejecutadas. Un log debería contener al menos la siguiente información:
  - Quién: Usuario que ejecutó la acción.
  - Qué: Acción ejecutada.
  - Dónde: Dirección IP desde donde se ejecutó la acción.
  - Cuando: Fecha y hora en la que se ejecutó la acción.
- Los circuitos cerrados de televisión y las cámaras de video son controles que se implementan con el objetivo de evitar el no repudio, pues al final están registrando lo que hacen las personas. Claramente una investigación podrá avanzar en la medida en que sea posible observar el rostro de la persona en la grabación.

- Las firmas manuscritas son también utilizadas por los grafólogos para concluir que alguien certificó a través de su firma un documento o escrito.
- Las firmas digitales también están orientadas al no repudio, pues es responsabilidad de su dueño custodiarla de manera adecuada.

¿Sabía qué...?

RBAC (Role-basedAccess Control) es una de las técnicas más utilizadas para garantizar la autorización en las aplicaciones.

En síntesis...

Seguridad en el ciclo de desarrollo en más que confidencialidad, integridad y disponibilidad, también requiere de adecuados niveles de autorización, autenticación y no repudio.

Referencias

Clarín. (2017). *El FBI pagó 900.000 dólares para desbloquear el iPhone de un terrorista*. www.clarin.com. Recuperado de https://www.clarin.com/tecnologia/fbi-pago-900-000-dolares-desbloquear-iphone-terrorista_0_S1Bu7ryxW.html

Semana. (2011). *Hackean página del Ejército colombiano*. www.semana.com. Recuperado de http://www.semana.com/nacion/articulo/hackean-pagina-del-ejercito-colombiano/246019-3

El País. (2010). *Irán sufre un ataque informático contra sus instalaciones nucleares*. www.elpais.com. Recuperado de https://elpais.com/diario/2010/09/28/internacional/1285624808_850215.html

El Tiempo. (2017). *Página de El País de España fue hackeada durante dos horas*. www.eltiempo.com. Recuperado de http://www.eltiempo.com/mundo/europa/pagina-de-el-pais-de-espana-fue-hackeada-145038

El País. (2017). *El ciberataque: pulsar un botón y desenchufar el mundo*. www.elpais.com. Recuperado de https://elpais.com/internacional/2017/05/20/actualidad/1495291083_920693.html

INFORMACIÓN TÉCNICA

FACULTAD DE
INGENIERÍA, DISEÑO
E INNOVACIÓN

Módulo: Seguridad en el Ciclo de Desarrollo

Unidad 1: Conceptos básicos y modelos existentes

Escenario 1: Conceptos básicos de seguridad de la información

Autor: Miguel Ángel Zambrano Puentes

Asesor Pedagógico: Edwin Mojica Quintero

Diseñador Gráfico: Brandon Steven Ramírez Carrero

Asistente: Ginna Quiroga