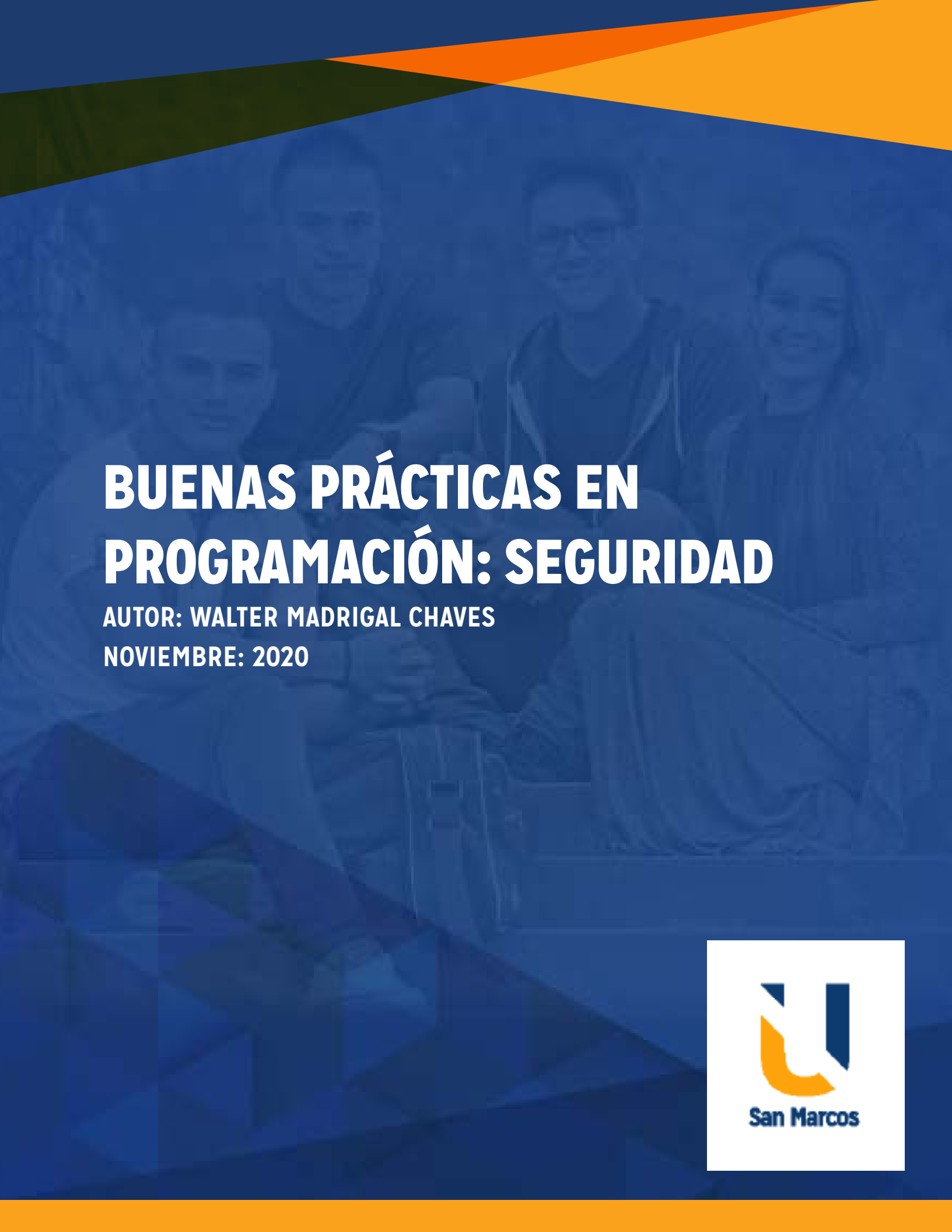

BUENAS PRÁCTICAS EN PROGRAMACIÓN: SEGURIDAD

AUTOR: WALTER MADRIGAL CHAVES

NOVIEMBRE: 2020

San Marcos

Contenido

Introducción

En un mundo bastante globalizado en que se vive, la tecnología y en particular el uso de internet al interior de diversos dispositivos es el pan de cada día, nace la imperiosa necesidad de generar entornos seguros que faciliten el intercambio de información de forma eficiente y segura para quienes interactúan.

Día a día múltiples desarrolladores generan soluciones de software que ágilmente llevan a cabo las tareas para las cuales fueron diseñados, sin embargo, no todas abordan con suma seriedad el tema de seguridad, que es bastante relevante, sobre todo en una época en que la información es el tesoro primordial para una persona u organización.

Es importante entonces abordar el tema de seguridad con seriedad y no solo desde la perspectiva de quien accede o no a una aplicación bajo esquemas tradicionales de usuarios y contraseñas, sino cómo hacer para mantener esa información de tal manera que genere confianza para los usuarios que utilizan soluciones de software.

Tipificación de ataques

Cuando las organizaciones exponen uno o más servicios a internet, deben proteger sus recursos y datos. Cabe mencionar que existen sistemas más críticos que otros, por ejemplo, las entidades bancarias tienen que prestar una mayor atención en temas de seguridad ya que los datos que administran son de tipo monetario. Aun así, las aplicaciones web deben resguardarse y asegurarse ante cualquier eventualidad de ataque.

Por lo general, se puede hacer referencia a tres tipos de ataques:

- **Ataques anónimos:** Aquí el objetivo principal es obtener información de índole confidencial, analizando la continua comunicación entre dos equipos de cómputo. Este análisis es conocido como sniffing. Una forma eficiente de prevenir este tipo de ataques es a través de la encriptación de los datos que son transmitidos. Algunas instituciones hacen uso del protocolo HTTPS para el despliegue de sus aplicaciones web.

- **Ataques a la integridad:** Estos ataques buscan alterar la información en tránsito con fines netamente maliciosos. Para evitar esto, se debe hacer uso de métodos como la criptografía de llaves públicas.

- **Ataques para la denegación de servicios:** Toma una plataforma e intenta inundarla de peticiones falsas, haciendo que se muestre como no disponible en las verdaderas solicitudes. Por lo general, este tipo de ataques suelen prevenirse a través del uso de firewalls, cuya tarea es bloquear el tráfico de red en aquellos puertos que no se utilizan normalmente.

Algunos tipos de ataques se enfocan a:

- **Autenticación:** Por lo general es realizado a través del login: usuario y contraseña.

- **Autorización:** Hace referencia a las acciones que puede llevar a cabo el usuario en el sistema, después del proceso de autenticación.

- **Integridad de los datos:** Hace referencia a los momentos en los que los usuarios realizan alguna operación al interior del sistema. La información resultante de dichas operaciones no debe ser cambiada o saboteada.

- **Confidencialidad:** El usuario que ha sido autorizado para ingresar al sistema debe acceder a la información sensible de forma exclusiva. Varía de acuerdo con la autorización debido a que el objetivo de la confidencialidad es garantizar que los datos, si llegan a caer en manos indebidas, no puedan utilizarse.

Es importante tener en cuenta que las aplicaciones web son de alcance público y pueden ser atacadas con facilidad. Estas pueden ser vulneradas por distintas personas y por diversos motivos. Por ejemplo, un hacker podría vulnerar por simple diversión, o una persona que ha sido despedida tendría motivos para querer tomar venganza.

A través de la definición de servlets se pueden crear métodos que contribuyan a la implementación de parámetros de seguridad al interior de las aplicaciones.

Mecanismos de autenticación

Existen 4 mecanismos a través de los cuales se logra implementar la autenticación a partir de la definición y el uso de servlets. Estos son:

1. HTTP basic.
2. HTTP digest.
3. HTTPS client.
4. Autenticación HTTP que se basa en formularios.

Estas técnicas se basan en el uso de usuario, contraseña y un servidor web que

logra mantener el respectivo listado de usuarios y sus contraseñas.

HTTP basic: es de los mecanismos más usados para la protección de los recursos, debido a su sencillez. Se compone de una ventana tipo pop up, que solicita un usuario y la respectiva contraseña. Una deficiencia es la no encriptación de la información y el no poder personalizar dicho pop up.

HTTP digest: este mecanismo es similar al anterior, con la diferencia de que hace uso del método de encriptación MD5. Aun así, una gran falencia es que solo es soportado por Internet Explorer y algunos de los contenedores de servlets no pueden gestionarlo.

HTTPS client: hace referencia a HTTP sobre SSL. La información que viaja entre el servidor y el cliente va encriptada, haciendo uso del método de criptografía de llave pública. Este lo soportan gran variedad de los navegadores y es el más seguro frente a otros métodos. Como desventaja puede mencionarse el hecho de que requiere un aval por parte de una entidad certificadora y, además, el costo de implementación y soporte es elevado.

SSL
Es un protocolo diseñado para permitir que las aplicaciones que transmitan información de manera segura de ida y hacia atrás. Las aplicaciones que utilizan el protocolo Secure Sockets Layer están capacitadas para dar y recibir claves de cifrado de otras aplicaciones,
así como la manera de cifrar y descifrar los datos enviados (digicert.com, s.f.).

Autenticación HTTP a partir del uso de formularios: Tiene un comportamiento parecido al que posee HTTP basic, aunque este hace uso de formularios HTML para el ingreso del usuario y la respectiva contraseña. Tiene características de fácil implementación y en general la mayoría de los navegadores lo soportan. Una gran desventaja es que no es lo suficientemente seguro ya que la información no viaja encriptada y además requiere el soporte de cookies.

Implementación de mecanismos de seguridad en TOMCAT

Tomcat, y específicamente su servidor, establece un modelo de seguridad que se basa en la definición de roles. Un usuario bajo ese modelo estará asignado mínimo a un rol y los correspondientes permisos le serán asignados al respectivo rol en vez del usuario. De esta manera se flexibiliza el modelo ya que pueden tenerse varios usuarios con el mismo rol, de igual forma un usuario puede tener distintos roles manteniendo en su definición la sumatoria de todos los roles establecidos.

Definición de dominios de seguridad

Estos hacen referencia a mecanismos del Tomcat que son usados para la protección de los recursos que tiene la aplicación web. Esto brinda una gran capacidad para proteger un recurso a partir de una o varias restricciones de seguridad predeterminadas para más adelante definir cuáles roles pueden acceder al recurso que se ha protegido.

La interfaz org.apache.catalina.realm, del servidor de Tomcat, hace que sea posible dicha funcionalidad. Esta ofrece un mecanismo en el que se integran el listado de roles, usuarios y sus respectivas contraseñas.

Tomcat establece 2 tipos de dominios de seguridad:

- Dominio basado en el archivo tomcat-users.xml.
- Dominio basado en fuentes JDBC.

En ambos casos, el mecanismo y su configuración de seguridad es definida en elweb.xml de la correspondiente aplicación web. Una distinción radica principalmente en el origen (donde se obtienen) los usuarios, roles y contraseñas. Para el primer caso, los usuarios a los que se les ha permitido entrar a una determinada aplicación se han de guardar en el documento DIRECTORIO_TOMCAT/conf/tomcat-users.xml. Para el caso número dos, se

obtendrán de una base de datos.

La seguridad en la arquitectura de referencia de un servicio web

A continuación, se hace una breve descripción acerca de los requerimientos de seguridad que son enumerados dentro de la arquitectura que aquí se menciona.

Servicios básicos de seguridad: Un componente relevante en el ámbito del aseguramiento de calidad dentro de un servicio web es la seguridad. Los servicios de seguridad básicos que por lo general se deben tener en cuenta son la integridad, la confidencialidad, la autenticidad de origen, el no repudio y el control de acceso.

Autenticación de los participantes: Los servicios web son muy heterogéneos, esto lleva a los sistemas de autenticación a un alto grado de flexibilidad. Por ejemplo, si hay servicios web que requieren establecer comunicación con otros servicios, estos podrían realizar una solicitud al demandante y solicitar las respectivas credenciales junto a una breve corroboración de que es el dueño de estas.

Es bastante importante establecer un estándar de los formatos y los protocolos a usar. Una gran dificultad es tener que establecer modelos de autenticación de tipo Single Sign-On, de tal manera que si hay servicios que requieren la comunicación con otro u otros servicios, no tengan que autenticarse continuamente y pueda terminar satisfactoriamente el proceso de negocio en el tiempo necesario.

Autorización: Frecuentemente surge la necesidad de aplicar ciertos criterios que ayuden a establecer controles de acceso a los distintos recursos. Es necesaria la definición de los usuarios que estén en capacidad de realizar acciones sobre todos los recursos. Al combinarse con la autenticación, facilita a las identidades conocidas la realización de las acciones para las que les han asignado permisos. Frecuentemente se establecen normas de acceso con base

a jerarquías.

Confidencialidad: Aquí hay una imperiosa necesidad de garantizar que el contenido que se incluye en los mensajes intercambiados se mantenga a manera de datos confidenciales. Es común utilizar mecanismos de cifrado para esa tarea. Es obvio que la confidencialidad debe ir más allá del establecimiento de un canal para la correspondiente transmisión.

Integridad: Este atributo garantiza que la información que se recibe es la misma que la enviada por el cliente.

No repudio: Al establecer comunicaciones en las que se llevan a cabo operaciones es muy importante el registro de la producción de estas y su correspondiente autor-ejecutor. Para el caso de un servicio web, se debe trasladar esa norma al uso del servicio. Por ejemplo, al comprobar que cierto cliente hizo uso de un servicio a pesar de que este fue negado se conoce como no repudio del solicitante; de igual forma, se puede probar si la ejecución se ha llevado a cabo, lo que comúnmente se denominada no repudio del receptor.

Disponibilidad: Dentro de los ataques que se encuentran con más frecuencia en las aplicaciones, los más populares son aquellos basados en la denegación de servicios. Suelen hacerse varias peticiones falsas para colmar los servicios y generar su respectiva caída. Se debe entonces tener en cuenta la disponibilidad como una referencia relevante en la configuración de los servicios web, puesto que permitiría cierto grado de redundancia en el sistema.

Auditabilidad: Registrar las acciones al interior de un servicio web ayuda a mantener una traza de ellas, de tal forma que los datos pueden ser analizados posteriormente con facilidad.

Seguridad de extremo a extremo: Cuando se ejecutan los servicios es

importante que se garantice la seguridad de estos en el tiempo que dure el recorrido de los mensajes. Lo anterior debido a que, por lo general, hay routers que hacen las veces de intermediadores de comunicaciones, generando el crecimiento de las políticas de seguridad que garanticen la realización del transporte de manera segura y logren confirmar la seguridad de los respectivos intermediarios.

Se hace relevante poder contar con un entorno de seguridad que tenga el canal de comunicación adecuado. Aquí se hace necesario aplicar múltiples operaciones criptográficas en el origen de la información. Así se pueden evitar dependencias con la seguridad configurada por detrás de la capa de aplicación y se tiene garantía de los respectivos servicios de seguridad.

Requerimientos de seguridad

Es importante concebir un entorno para que los procesos y transacciones naveguen en un ambiente de seguridad total. De igual forma, es importante que se garantice la seguridad de la información en el momento en que se lleve a cabo la comunicación, ya sea a través de intermediarios o sin ellos. También se requiere el aseguramiento de la seguridad de los datos al interior de las respectivas actividades de almacenamiento.

Mecanismos de autenticación

Un proceso de autenticación se hace necesario para mantener el debido control, así como poder verificar la identidad de proveedores y solicitantes. Muchas veces es necesario establecer una autenticación tanto del proveedor como del solicitante, ya que podría suceder que quienes participan no se encuentren en conexión directa. Aun así, pueden existir intermediarios que logren retransmitir la debida comunicación.

Independiente de las políticas de seguridad adoptadas se hace necesario autenticar al solicitante y al proveedor. Pueden emplearse métodos que estén

basados en certificados o contraseñas para la formalización de la autenticación. Si el proceso está basado en el uso de contraseñas, será necesario utilizar políticas pertinentes para el caso.

Pueden usarse técnicas basadas en normas de transporte como el SSL/TLS X509 Certificate y el HTTP autentication. Estos se hacen válidos solamente en el momento en que exista una conexión directa entre el proveedor y el consumidor de los servicios, ya que, si los mensajes SOAP viajan a través de distintos endpoints mucho antes de la llegada a su destino, las respectivas credenciales del usuario se pierden en el primer endpoint.

De igual manera podrían emplearse técnicas basadas en tokens incluidos en el interior del mensaje. WS-Security es el estándar que tiene una amplia variedad de tokens que pueden ser utilizados, por ejemplo, X509 Certificate, username token, SAML assertions. Esa técnica de autenticación no posee las dificultades en los mecanismos que se basan en el transporte, debido a que las credenciales podrían transportarse entre los diferentes endpoints hasta llegar a su respectivo destino.

Al usarse esta técnica, es importante que los mensajes se transmitan de manera segura con el fin de evitar ataques tipo replay. Esto se puede conseguir a través de la firma del token al interior del mensaje SOAP, asociado a un IDMessage o TimeStamp, aquí se recomienda incluir en la firma la cabecera de WS-Addressing. En escenarios cerrados podría usarse de igual forma SSL para la transmisión de los mensajes con tokens de manera segura.

Autorización: La autorización es relevante para ejercer control sobre el acceso a los recursos. Después de la autenticación del usuario y conociendo por defecto su identidad, se utilizan las técnicas de autorización para la realización de las respectivas validaciones y el aseguramiento del acceso al recurso por parte del usuario.

Deben crearse normas que determinen los respectivos privilegios de quienes participan. A través de la administración de la confianza, se autoriza una interoperabilidad entre un proveedor y un solicitante, sin que haya referencias previas, pero que teniendo en cuenta las credenciales intercambiadas logren determinar niveles de confianza asumibles por los dos. Así, de esta forma, es permitido el proceso para autenticarse sin que haya necesidad de revelar la identidad de quienes participan en la actividad.

Confidencialidad e integridad de los datos

La actividad de mantener de forma íntegra la información debe garantizar que los datos que han sido enviados no han tenido modificaciones sin que se hayan detectado.

Para esto, es la confidencialidad la que establece y garantiza los principios de intimidad de la respectiva información. Esto es, que solo es permitido acceder a los datos de los usuarios que tengan credenciales para hacerlo. A menudo se utilizan mecanismos de cifrado para tareas y actividades de alta confidencialidad y, además, una firma digital para todo lo que tiene que ver con integridad.

No repudio: Como se ha mencionado anteriormente, el objetivo primordial de estas técnicas es el registro de la participación de los distintos interlocutores en una transacción y así blindarlo de posibles denegaciones por parte de un interlocutor que niega que la transacción haya ocurrido o que haya participado allí.

Si lo que se busca es que el no repudio haga parte de las comunicaciones por servicios web, los debidos mensajes SOAP que se intercambian deben identificarse de manera exclusiva a través del uso de la definición WS-Addressing. Un mensaje SOAP, junto a su cabecera, debe ser firmado teniendo en cuenta los procedimientos obtenidos en la definición WS-Security. Del mismo

modo, es importante mencionar que un mensaje debe ser almacenado en archivos de logs para posteriores consultas.

Rastreabilidad: Es clave realizar un ajuste de trazas que asegure el conocimiento de los datos de acceso una vez que este se establezca y validar el comportamiento que haya podido tener el usuario al acceder al sistema. Es de gran importancia para la verificación de la integridad del sistema.

Por lo general, las trazas son generadas por los denominados agentes de auditoría, los cuales se encargan de monitorear, vigilar recursos y validar cómo se comportan otros agentes, así como también el cumplimiento de las normas establecidas. A menudo es casi imposible prevenir que se vulneren las distintas tareas, pero si, por ejemplo, dos agentes de auditoría evidencian una brecha podrían iniciar un plan de repulsión o definir otro tipo de tareas.

Llevar a la práctica de forma distribuida las políticas de seguridad

Cuando se establecen las arquitecturas que se basan en un servicio web, estas deben facilitar la definición de normas de seguridad y validar que se lleven a cabo en las diferentes plataformas, teniendo en cuenta los múltiples cambios para acceder al servicio.

Seguimiento de las políticas:

Un mensaje que es enviado a través de la comunicación de uno o varios servicios web atraviesa un cortafuegos y puede ser cambiado a través de los distintos protocolos y puertos que existen. Con el fin de que se asegure la calidad de seguridad en un servicio web es necesario crear normas corporativas que se integren con las diferentes políticas que tienen los proveedores y, de igual manera, con la administración de la confianza planeada.

Políticas distribuidas:

A menudo, las normas de seguridad se asocian a los clientes, los proveedores

o mecanismos de descubrimiento. Son usados para establecer un control y la definición de una metodología de acceso de las solicitudes y las correspondientes respuestas dadas por quienes intervienen en la comunicación. Esas normas se validan en ejecución en el ámbito de la comunicación. Las partes involucradas deben llevar a cabo la correspondiente validación de sus normas.

Normas de confianza:

Las normas o políticas de confianza deberían ser políticas distribuidas que aseguren a dos entidades que buscan afrontar interacciones sin conocerse en primera instancia. A través de la utilización de credenciales, toman los niveles de seguridad que les es posible soportar. Algunas veces, el establecimiento de las políticas involucra a terceros que de manera recursiva repercuten en las decisiones.

Mecanismo de descubrimiento seguro

El objetivo principal de este mecanismo es controlar las apariciones y publicaciones de un servicio. En el momento en que aparecen los servicios, se hace relevante la realización de una evaluación de las normas de publicación de este, a excepción de aquellas situaciones que suponen un servicio de descubrimiento entre nodos. Si el cliente es quien lleva a cabo el descubrimiento, puede asignarle identidad o no al servicio en mención. En este caso se hace referencia a un descubrimiento anónimo.

Confianza y descubrimiento

Al pensar en situaciones donde los clientes descubren la existencia de servicios web necesarios para ellos, y quien los provee es una entidad desconocida, se debe preguntar cuál es el nivel de confianza que le puede asignar el solicitante a ese servicio. Aquí es bastante relevante en el caso que se estén administrando datos muy sensibles, ya que se estaría corriendo un grave riesgo.

Privacidad

Esta puede expresarse a través de diferentes protocolos definidos por los distintos dueños de la información. A menudo, estos dueños son quienes hacen uso de uno o varios servicios web. Es importante garantizar que los privilegios de los usuarios se respeten

Fiabilidad de los servicios web

Es inevitable que aparezcan errores, sobre todo cuando se considera que el contexto asocia a múltiples servicios interconectados a través de una red mundial que hacen parte de varias clases de entidades y personas. La eliminación de errores no es completa, así que la principal meta es la disminución de la tasa de errores que se muestran al máximo nivel.

Amenazas de seguridad

Si se analiza la definición de amenaza de seguridad, se tiende a asumir que pueden existir intentos de acceso y usos errados de los diferentes servicios. Debido a esto se debe definir un esfuerzo para establecer controles sobre los accesos que no se encuentran permitidos. Si se realiza una clasificación de las amenazas más relevantes, se tiene lo siguiente:

- Acceso no permitido llevado a cabo por entidades sin identificación. Se requiere de forma confiable la identificación de la identidad de servicios, proveedores, entre otros.
- Alteración de los datos en el canal de comunicación. Se requiere garantizar la integridad de los datos enviados.
- Se debe garantizar el acceso a los datos. Solo pueden acceder las partes que se deseen. Debe mantenerse la integridad del contenido y obviamente que la comunicación ha tenido lugar.
- El acceso no apropiado a los recursos. En lo posible debe garantizarse

que las acciones y los recursos no son accedidos por aquellos que no han sido autorizados. Nuevamente, este hecho podría extenderse al simple conocimiento de que el recurso en sí existe, es decir, de alguna manera se podría impedir que personas no autorizadas conozcan la existencia de algunos servicios o recursos.

- Denegación de servicio. Los clientes no deben tener la posibilidad de acceder a uno o varios servicios.

Tipos de ataques

Modificación de los mensajes

Este se centra sobre la estructura de un mensaje. Su principal objetivo es alterar el contenido del mensaje de forma parcial o total. Si el atacante tuviese el control del canal de comunicaciones entre servicios, tendría la capacidad de modificarlos, eliminarlos, tomarlos y enviarlos nuevamente.

Que un mensaje tenga alta integridad puede darse a través de la firma digital del respectivo archivo xml junto con tokens de seguridad que aseguren que el mensaje se transmite sin alteración alguna. La técnica de integridad está construida con el fin de soportar distintas firmas a través de múltiples actores y puede extenderse para soportar nuevas técnicas de firma. Al integrar xmlsignature, se disminuyen las consecuencias de dichos ataques.

Ataques a la confidencialidad

Se centran en la captación de los datos contenidos en los mensajes. Algunas veces puede existir información altamente sensible como datos económicos, médicos, financieros, entre otros.

Hombre en el medio

Hace referencia a la infiltración por parte de un ente que ataca en medio de

quienes participan en una comunicación. Por lo general, intercepta la comunicación y suplanta a los participantes de tal forma que estos creen que realmente se están comunicando entre sí, cuando realmente lo están haciendo con el atacante.

Los ataques de intermediarios siguen siendo un gran problema en cuanto a seguridad se refiere, aún para distintos sistemas criptográficos que se basan en una clave pública. En la actualidad se pueden encontrar varios tipos de defensa contra los ataques que emplean mecanismos de autenticación basados en:

- Contraseñas de tipo público.
- Autenticación y validación mutua de tipo fuerte.
- Contraseñas secretas con alta y baja entropía.
- Reconocimiento de voz y distintas alternativas con atributos biométricos.

Se debe asegurar la integridad de las llaves públicas, aunque estas no requieren ser secretas, en cambio, los passwords y las claves de secreto compartido tienen el requisito de la confidencialidad. Una clave pública puede verificarse a través de una autoridad de certificación, la cual posee una clave pública distribuida a través de un canal de forma segura, para el caso podría integrarse en el navegador o en la instalación del respectivo sistema operativo.

Suplantación de identidad

También conocido como spoofing, hace referencia a un ataque que se encuentra orientado a los niveles de confianza que están establecidos en la comunicación. Cuando un atacante suplanta la identidad de uno de los que participan en una relación de confianza, por lo general intenta comprometer al destinatario de la comunicación. Se hace útil el uso de una autenticación robusta que fortalezca el servicio ante los ataques en mención.

Para evitar este tipo de ataques se pueden tomar distintas medidas preventivas; en primera instancia, se hace evidente que un gran apoyo es el refuerzo de la secuencia de predicción de números de secuencia

TCP. También se tiene como alternativa la eliminación de las relaciones de confianza que se basan en la dirección IP o el nombre de los equipos, cambiándolas por relaciones que se basen en claves criptográficas; el filtrado y el cifrado de las conexiones que aceptan las máquinas de igual forma son alternativas de seguridad bastante relevantes.

Denegación de servicio

La principal tarea es ofrecer un servicio activo para que los usuarios que son legítimos puedan acceder a él. Por lo general, los ataques están centrados en la destrucción de la disponibilidad de un servicio. Su principal meta es bloquear las operaciones de un servicio desconectándolo por completo Se debe entonces tomar la configuración del servidor y adaptarla a las necesidades de autenticación, siguiendo recomendaciones, teniendo en cuenta el tamaño de mensajes aceptados y el control de distribución correspondiente de mensajes para reducir al máximo este tipo de ataques.

Ataque de repetición

En esta situación un atacante tiene la capacidad de interceptar un mensaje logrando que se reenvíe más tarde cuantas veces quiera al servicio para el que era destinatario. Este problema se solventa utilizando mecanismos de autenticación junto con técnicas de sellado de números y tiempos de secuencia.

Frameworks y estándares actuales que abordan la seguridad en un servicio web

Este esquema tiene unos atributos de acceso a los datos sobre su intercambio y acerca de la autonomía de la información que difieren de lo establecido en los

modelos tradicionales de seguridad. De hecho, esto genera el desafío y la necesidad de modificar técnicas que afectan la confidencialidad e integridad de los datos enviados a través del canal del servicio web. Si se analiza la estructura de los sistemas de seguridad perimetrales, estos no están preparados para el aseguramiento de arquitecturas SOA.

Estas son dinámicas transmitidas mediante protocolos no asegurados como HTTP. Si se aplican criterios que controlan la comunicación punto a punto (TLS y SSL), no son válidos ya que no aseguran que su aplicación sea completa.

La tarea de procesar SOA se basa en comunicaciones soportadas en mensajes SOAP y documentos XML. Se hace necesario el aseguramiento de transmisiones por medio de una infraestructura de conectividad. Los estándares que están siendo desarrollados por W3C y otras entidades, que se basan en XML, intentan asegurar la integridad, confidencialidad y disponibilidad de un servicio web.

XML Digital Signature

Su principal objetivo es la creación de una serie de técnicas que permitan la generación y administración de firmas digitales que se basen en XML. Este es un estándar de firmas, desarrollado para el establecimiento de un esquema que permita la interpretación del resultado obtenido de las firmas digitales para aplicarlas sobre la información.

Al interior del esquema se evidencia el no repudio de las transacciones, la integridad de los datos y los criterios de autenticación sobre la transmisión.

De igual manera permite firmar de forma parcial el código XML y no obliga a que la firma sea aplicada a la totalidad de un documento, también permite firmar distintos tipos de recursos al interior de estos fragmentos de código, como información XHTML, datos en formatos en XML nativo y datos en formatos binarios. Para validar la firma se requiere que sea accesible el objeto que fue

firmado. La firma XML muestra la localización del objeto original, referenciándola a través de una URI con la respectiva firma XML.

XML Encryption

En este hay un framework que se utiliza para el cifrado de documentos XML. En el ejemplo siguiente se muestra cómo debe usarse este estándar asociado a llaves simétricas.

Imagen 1 Seguridad con XML Encryption

```
<?Xml version='1.0'?>
<Metodopago xmlns='http://madeja/ejemplo">
  <Nombre>Desarrollador</Nombre>
    <CreditCard Limite='10000' Moneda='EU'>
      <Numero>222 111 333 444</Numero>
      <Issuer>BanJuntaAndalucia</Issuer>
    <Caducidad>10/10</Caducidad>
  </CreditCard>
</Metodopago>
```

Fuente: elaboración propia

XML Key Management

Se orienta a la obtención de datos de certificados y claves. Permite el manejo de los procesos de revocación y registro del servicio. A través del uso de este protocolo se logra el intercambio y el registro de claves públicas. Se compone de dos importantes elementos: el registro (X-RKSS) y la información (X-KISS) de la clave pública.

Estos dos estándares están definidos del siguiente modo: XML Key Information Service Specification (X-KISS). Su objetivo es la creación de protocolos para el

procesamiento de los datos asociados a las claves de una firma XML y el contenido de estas, ya sean privadas o públicas.

XML Key Registration Service Specification (X-KRSS). Está dirigida al registro de un conjunto de claves que facilitan la realización de gestiones sobre la arquitectura privada o pública. Su principal objetivo es brindar una administración global de las actividades de intercambio de claves.

Oasis Security Service TC-SAML (Security Authorization Markup Language)

Se deriva de XML y está diseñado para el intercambio de autorización de datos y de autenticación. Dicho framework permite infraestructuras de llave pública que facilitan la realización de intercambios de autorizaciones y autenticaciones. Su principal objetivo es la creación de un conjunto de procesos que faciliten la realización de forma segura de un canje de la información relacionada con la identidad y privilegios de los usuarios.

Estos datos de seguridad se materializan a manera de afirmaciones establecidas por una autoridad SAML sobre un sujeto. Dicho sujeto es aquella entidad-objeto de las afirmaciones que se han realizado por la autoridad SAML.

Las afirmaciones tienen varios tipos de datos. Pueden brindar información sobre la autenticación, sobre un atributo o acerca de las respectivas decisiones de autorización. Si se analiza el tipo de declaraciones que se emiten, pueden definirse tres tipos de autoridades como son: autoridad de atributos, autoridad de autenticación y puntos de decisión de políticas.

Afirmaciones SAML

Estas por lo general se transfieren por los proveedores de identidad a los proveedores de servicios. Las afirmaciones tienen declaraciones que los proveedores de servicios usan para la toma de decisiones de control de accesibilidad. Hay tres tipos de declaraciones que proporciona SAML:

- Las declaraciones de autenticación se encargan de afirmar que el proveedor de servicios realmente se autenticó con el proveedor de identidad en determinado momento a través de un mecanismo de autenticación.

- Una declaración de atributo sostiene que un sujeto se asocia con ciertas características. Un atributo hace referencia a un par valor-nombre. Estas confían en la utilización de los atributos para la toma de decisiones de control de acceso.

- La declaración de decisión para la respectiva autorización sostiene que a un sujeto se le permite realizar una acción en un determinado recurso presentando pruebas para ello. La expresividad de los estados de decisión para la autorización en SAML se limitan de gran manera.

Platform for Privacy Preferences

Conocida también como P3P, es una especificación que ha sido propuesta por el consorcio de W3C con la tarea clara de indicar la política de privacidad de los participantes de forma estándar. En la especificación se define la forma de interpretar los datos referentes a la privacidad. Incluye una recomendación para la generación de varios archivos destinados al manejo de normas.

Ventajas de P3P

P3P se utiliza para el desarrollo de servicios y herramientas que ofrezcan a los usuarios un mayor control sobre la información personal que se administra en internet y, al mismo tiempo, el aumento de la confianza entre los usuarios y los servicios web.

De igual forma, mejora sustancialmente el control del usuario al establecer políticas de privacidad donde los usuarios las pueden encontrar en un formato de fácil comprensión y, sobre todo, con la posibilidad de que el usuario logre actuar sobre lo que ven. Se puede concluir que proporciona a los usuarios web una gran facilidad a la hora de decidir si quieren o no, y obviamente bajo qué

circunstancias, si se revelan sus datos personales.

Funcionamiento de P3P

Les permite a los sitios web el traslado de sus prácticas de privacidad a formatos estandarizados y procesados por dispositivos que pueden ser recuperados de forma automática y además pueden ser interpretados con facilidad por los navegadores de los usuarios.

Es importante comprender la importancia que tienen los componentes de seguridad al incluirlos dentro las aplicaciones que se desarrollan. Ningún parámetro estará de sobra y siempre se debe estar al tanto de nuevas formas de intrusión, así como también de métodos que contrarresten el impacto de las prácticas malintencionadas.

Aunque no existen soluciones informáticas que aborden 100% las necesidades de los clientes, se debe procurar blindar de manera óptima las aplicaciones que se generen para diversos objetivos.

Conclusiones y recomendaciones

- La seguridad es sin duda un elemento muy importante en desarrollo de software, el proteger la información es un deber que debe tomarse en cuenta al momento de diseñar y desarrollar proyectos informáticos.
- La variedad de ataques informáticos crece día a día, es importante para un programador renovar constantemente conocimientos, verificar soluciones que el mercado ofrece y siempre poner en práctica las buenas prácticas recomendadas en este apartado.
- No se puede escatimar en recursos para el diseño e implementación de la protección de datos, es importante asegurar a los involucrados la integridad y confidencialidad de la información.
- Es transcendental utilizar herramientas que aseguren la seguridad de la información, los distintos framework son excelentes opciones para implementa en los proyectos, ya que estos tienen estructuras robustas y ampliamente probadas.

Referencias bibliográficas

Junta de Andalucía. (s.f.). Conceptos de seguridad en los servicios web. Recuperado de http://www.juntadeandalucia.es/servicios/madeja/contenido/recurso/211

Martínez, F. (2013). Seguridad en aplicaciones web (I). Recuperado de https://www.portantier.com/seguridad-en-aplicaciones-web-i.html

Netuniversecorp. (2017). Seguridad de sitios web: problemas, peligros y amenazas. Recuperado de https://www.netuniversecorp.com/seguridad-en-web/

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica