Asegurar Web Services no es Cuestión de Costos

Secure Web Services it is not a question of Costs

Marco Fidel Castellanos Bernal
Bogotá, Colombia
@mcastel_b
marcofcastellanos@gmail.com

Recibido / Received: 26-10-2016 – Aceptado / Accepted: 07-04-2017

Resumen

En la actualidad, el uso de componentes que permitan la integración e interacción entre diferentes sistemas de información, se hace necesario y evidente, ya que las organizaciones no logran mantenerse en una única línea de vida del *software*, que permita actualizar sus aplicaciones de modo tal que todas se mantengan con tecnología de punta, que soporte nuevas implementaciones y dinámicas del mercado. Esta convivencia entre diferentes tipos de aplicaciones, las cuales requieren comunicarse entre sí, ha llevado a la necesidad de contar con componentes *software* de comunicación que permitan, de forma inmediata, enviar y recibir información para lograr efectuar transacciones en línea primando la flexibilidad de los procesos.

Palabras clave: WebServices, WS-Security, Aseguramiento, DMZ, Desbordamiento de búfer.

Abstract

At present the use of components that allow the integration and interaction between different information systems becomes necessary and clear, since the organizations do not manage to be supported in the only line of life of the software, which allows to update its applications of a such way that they all are supported with technology of top, which supports new implementations and dynamics of the market. This one coexistence between different types of applications, which need to communicate between themselves, has led to the need to count with components software of communication that they should allow of immediate form to send and receive information to manage to carry deals out in line giving priority to the flexibility of the processes.

Keywords: WebServices, WS-Security, insurance, DMZ, Buffer overflow.

I. Introducción

Para lograr la flexibilidad, interacción e integración, se requiere la existencia de una arquitectura que preste estos servicios de interacción en distintas capas, para lo cual existe la arquitectura orientada a servicios (SOA Service Oriented Architecture) [1] que hace uso de los Servicios Web o Web Services [2], para lograr el objeto de la integración y flexibilidad de las aplicaciones.

Los WebServices (Web Services) permiten enlazar, mediante el uso de diferentes protocolos, cualquier tipo de tecnología o servicio en la web, logrando que aplicaciones legado se comuniquen con otras aplicaciones de una organización o de cualquier tercero.

La implementación de estos componentes, los Web Services, se ha masificado, siendo un importante punto de valor para las organizaciones, ya que allí confluyen varios núcleos de negocio por los cuales se transfiere información vital para las organizaciones, desde datos personales, información financiera, hasta todo tipo de información que pueda estar tipificada como confidencial.

Así, contar con un esquema de seguridad que propicie la confidencialidad, integridad y disponibilidad de la información que allí circula, no es en la actualidad el foco principal de las organizaciones. Como se mencionaba anteriormente, la evolución tecnológica no permite que los sistemas permanezcan en las últimas versiones de sus productos, sino que sobrevivan a los cambios cada vez más ágiles del mercado y cualquier componente que les permita mutar y adaptarse con el menor esfuerzo, les es de gran utilidad, como es el caso de los Web-Services.

Dependiendo el nivel económico, el estándar, la legislación o el lineamiento a cumplir, las organizaciones invierten o no en el aseguramiento de sus Web Services (bueno, en general de cualquier componente tecnológico), tema que no debería ser así; es cuestión simplemente de velar por minimizar el riesgo al que están expuestos los componentes tecnológicos que soportan los procesos de una empresa, a fin proteger la información tan sensible que puede llegar a ser transada por este medio, ante posibles ataques internos o externos que develen las falencias, fuga de información e incluso deterioro de los componentes de quien consume o expone estos servicios.

Muchas organizaciones cuentan con proxy´s [3] de web services o concentradores de servicios web, que permiten aplicar diferentes capas de seguridad, para proteger a quien expone con exigencias a quien consume el servicio, todo bajo estándares como WS-Security [4] que velan por el cumplimiento de la confidencialidad, integridad y disponibilidad de la información, usando diferentes herramientas como firmas digitales, certificados digitales, resúmenes criptográficos, protocolos de cifrado, mecanismos de autenticación, estructuras de sanitización de datos, entre otros.

Pero, todo esto no tiene por qué ser un armamento pesado, costoso y difícil de implementar en todo tipo de organización, existen caminos, arquitecturas y buenas prácticas que permiten lograr pasar de una simple configuración por defecto, a un conjunto de componentes de seguridad que le hagan un poco complicado o demorado el acceso a los delincuentes informáticos donde estos deban tomarse su tiempo para lograr efectuar algún tipo de "maleficio" sobre las fuentes de información llamadas Servicios web.

Así es como este documento y su resultado, pretende dar a conocer implementaciones que pueden llevar cualquier organización, a un nivel de aseguramiento que mitigue el nivel de riesgo, respecto a los servicios web que expone o que consume.

Con el ánimo de propender por la confidencialidad, integridad y disponibilidad de la información y de sus diferentes tipos de estado en almacenamiento, tránsito y procesamiento que proveen la interacción con diferentes tipos de sistemas de información y el constante desarrollo tecnológico, se ha obligado a que la industria se mueva rápidamente en la búsqueda de soluciones que permitan con el mínimo esfuerzo satisfacer las necesidades funcionales, dejando de lado los requerimientos no funcionales

asociados a seguridad. Pero este facilismo implícito ha permitido que, cada día, las implementaciones de nuevas tecnologías tengan graves falencias de seguridad y posean cada vez más el rótulo de "configuración por defecto".

Es aquí donde se expone la necesidad de contar con mecanismos de seguridad que provean el cumplimiento de las organizaciones respecto al correcto tratamiento de la información.

Así, el caso de los Web Services como mecanismos integradores de consumo y exposición de data, donde si no se cuenta con un correcto esquema de protección, dichos servicios pasarían de ser soluciones flexibles de integración, a puertas para la fuga de información.

Para lograr cumplir con dicha función, se requiere la existencia de una arquitectura que preste estos servicios de interacción en distintas capas, para lo cual existe la arquitectura orientada a servicios (SOA Service Oriented Architecture) [1] que hace uso de los Servicios Web o Web Services [2] , para lograr el objeto de la integración y flexibilidad de las aplicaciones.

II. Metodología

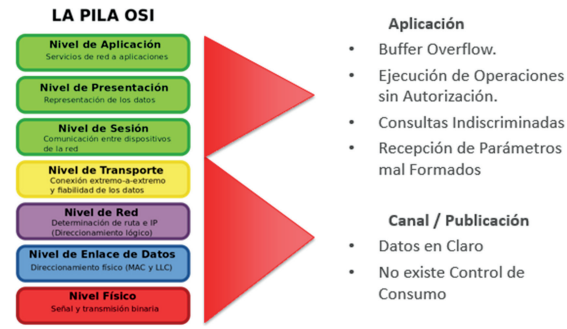
Artículo enmarcado dentro de la definición metodológica de un enfoque Explicativo.

Explicativa
Pretende sugerir una serie mejores prácticas a tener en cuenta dentro de la implementación de Web Services, permitiendo la mitigación de los riesgos asociados, sin incurrir en negligencia justificada en altos costos.

III. Contenido

Principales tipos de ataques a los web services: Los web services cuentan con diferentes vulnerabilidades que se han vuelto comunes a cualquier implementación, en la Fig. 1 se describen algunas de estas, según Panorama entorno Colombia:

A. A Nivel de Aplicación:



Fuente: autor.
Fig. 1. Vulnerabilidades Web Services Panorama Entorno Colombia.

Buffer Overflow [5]: sobre escritura de posiciones en memoria, todo producto de una mala validación de los tipos de datos y longitudes de los campos esperados en la capa de lógica del negocio, o en la pasarela que conecta al acceso a datos.

1) Ejecución de Operaciones Sin Autorización: dentro de la composición de los web services, es importante recordar el uso de operaciones y cómo cada una efectúa algún tipo de transacción. En varias implementaciones no se contempla el mínimo privilegio para la ejecución de cada operación, sino que se delega un único usuario para invocar cualquier tipo de operación para la que esté diseñando el web service, lo cual permite que un atacante libremente haga uso completo del servicio web.

2) Consultas Indiscriminadas: si el *web services* desarrollado no cuenta con parámetros de autenticación respecto al consumo del servicio y la operación que invoca, este podrá producir denegación de servicios respecto a las respuestas esperadas producto de sus consultas.

3) Recepción de Parámetros mal Formados: si el *web service* fue desarrollado bajo la premisa que el único consumidor iba a ser una aplicación, este podrá ser excitado de diferentes formas con parámetros

erróneos buscando comportamientos anómalos en el servicio.

B. A nivel de Canal y Publicación:

1) *Datos en Claro:* se requiere que se haga uso de un canal cifrado para la transmisión de datos.
2) *No existe Control de Consumo:* al igual que en la aplicación, se requiere un esquema de autenticación que autorice o no el consumo de los servicios expuestos.

C. Aseguramiento

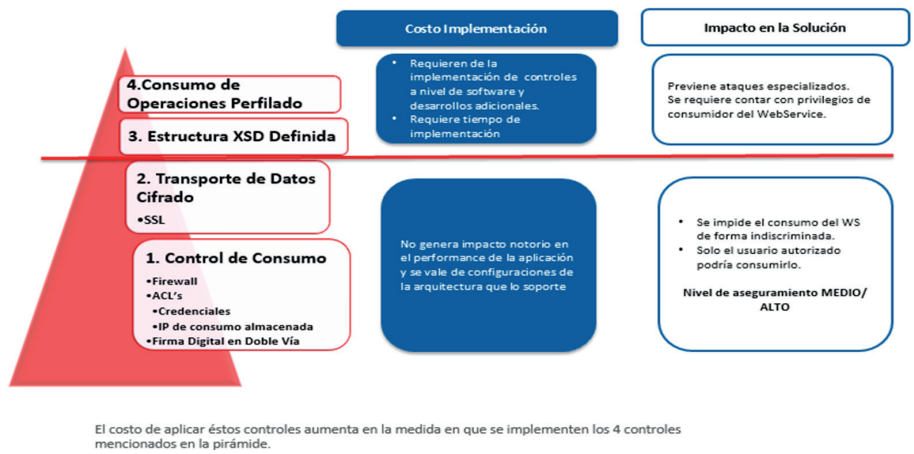
Dentro de los niveles de aseguramiento para *Web Services*, es posible efectuar una clasificación en tres niveles:

1) *El Mundo Ideal:* se cuenta con un concentrador de web Services, el cual es configurado usando WS-Security, así incluye firmas, certificados, autenticación por servicio, por métodos y por consumo, adicional cuenta con ACL's[6] de consumo. Adicional a los controles anteriores, a nivel de desarrollo, el *web service* cuenta con sanitización, hace uso de expresiones regulares, se cifran por *software* campos sensibles del servicio y cuenta con una estructura XSD [7] definida para limitar las posibles manipulaciones del servicio.

2) *El Mundo Real:* el *web services* se encuentra implementado y funciona, pero no cuenta con un esquema como WS-Security habilitado, no cuenta con firmas digitales, cuenta con certificados digitales pero los implementados para proveer autenticidad del sitio que los expone (esto en el mejor de los casos). El *web service* se dejó en la DMZ y está disponible para el consumo del cliente, no se estableció ningún tipo de control porque sencillamente el desarrollador indicó que solo iba a entender las peticiones del cliente que son originadas por una aplicación. Claramente, solo se esperan peticiones de la aplicación cliente, ¡qué gran error!

3) *El Mundo que Podemos Construir:* se debe mediar entre una implementación con componentes de seguridad tan robusta, que no sea sostenible ni económicamente ni a nivel de consumo de recursos tecnológicos por degradación del servicio.

Costos para el Aseguramiento de Web Services:
Se habla de cómo controles básicos con un mínimo de esfuerzo permiten mitigar riesgos y cerrar las brechas respecto a ataques más especializados en una implementación de Web Services. En la Fig. 2. se describe un comparativo entre el costo de implementación versus el impacto de la solución para asegurar las Web Services.



Fuente: El Autor, 2016

Fig. 2. Costo Vs. Impacto de soluciones de seguridad en Web Services

Como se observa en la imagen:

1) El costo de aplicar estos controles aumenta en la medida en que se implementen los 4 controles mencionados en la pirámide.

2) El costo debe estar desglosado en términos de:
   a) Riesgo reputacional al no lograr implementar controles y sufrir algún tipo de ataque.
   b) Cambios en la aplicación y soporte para las modificaciones.
   c) Tiempo de la implementación: Fuera de línea del servicio producto de un ataque o producto de la implementación de una solución.

IV. Conclusiones

Implementar controles de seguridad para mitigar los niveles de exposición al riesgo de los *web services*, es una tarea que no depende necesariamente de un presupuesto económico.

La implementación de controles puede ser progresiva, ya que existen controles que tienen mayor valor, respecto al nivel del riesgo que están cubriendo.

Es importante contar con un adecuado análisis de la necesidad durante la implementación del *web service*, para que se especifiquen todos los requerimientos no funcionales que propenderán por el endurecimiento de la solución, disminuyendo costos, respecto al costo de implementar controles una vez se encuentra en producción.

Los *web services* están por todos lados, son el "pasaje secreto" que unifica diferentes mundos de negocios; si no cuentan con un nivel de aseguramiento adecuado, continuarán siendo el túnel de obtención de información de muchos ciber criminales.

Referencias

[1] P. Bianco, K. Rick y M. Paulo, Software Engineering Institute, 2007. [En línea]. Available: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8443.

[2] M. Vera, Intelligence Bussines, 2014. [En línea]. Available: http://www.i2btech.com/blog-i2b/tech-deployment/que-se-entiende-por-soa-y-cuales-son-sus-beneficios/.

[3] Wikipedia [En línea]. Available: https://en.wikipedia.org/wiki/Proxy_server.

[4] Wikipedia [En línea]. Available: https://en.wikipedia.org/wiki/WS-Security.

[5] Buffer Overflow, 29 06 2016. [En línea]. Available: https://www.owasp.org/index.php/Buffer_Overflow.

[6] A. c. list. [En línea]. Available: https://en.wikipedia.org/wiki/Access_control_list.

[7] X. Schema. [En línea]. Available: http://www.w3schools.com/schema/schema_example.asp.