Evaluación Multicriterio Sobre Herramientas de Análisis de Seguridad en Aplicaciones Web

Ayrton Marini, Enrique A. Miranda, Mario Berón, Miguel Bustos, Daniel Riesco, Pedro R. Henriques

Departamento de Informática/ Universidad Nacional de San Luis/ Argentina

Departamento de Informática/ Universidade do Minho/ Portugal

mariniayrtond@gmail.com, {eamiranda,mberon,mabustos,driesco}@unsl.edu.ar, prh@di.uminho.pt

Resumen

En la actualidad, la mayoría de los sistemas informáticos utilizan Internet como su medio de despliegue. Un factor crítico de éxito durante su desarrollo, es garantizar su seguridad. Para llevar a cabo esta tarea, dentro de las alternativas más utilizadas, se encuadran las herramientas de análisis estático y dinámico de software. No obstante, existe una gran variedad de analizadores los cuales poseen diversas características, convirtiendo al proceso de selección de una herramienta que mejor se adecue a una determinada situación, una tarea tediosa para el ingeniero de software. Es por esto que es de vital importancia proveer mecanismos sistematizados y eficaces para evaluar las distintas alternativas.

El presente trabajo propone una línea de investigación que tiene dos objetivos relacionados. Por un lado, el estudio de diferentes métodos de evaluación multicriterio y por otra parte, su aplicación a la evaluación de herramientas de análisis de la seguridad de aplicaciones web.

Palabras clave: Seguridad Informática, Evaluación Multicriterio de Software, Herramientas de Análisis.

Contexto

La línea de investigación descripta en este artículo se encuentra enmarcada en el contexto de dos proyectos. Uno de ellos (P-031516) denominado: Ingeniería de Software: conceptos, prácticas y herramientas para el desarrollo de software de calidad de la Universidad Nacional de San Luis. Y otro (PO/16/93) llamado: Fortalecimiento de la Seguridad de los Sistemas de Software mediante el uso de Métodos, Técnicas y Herramientas de Ingeniería Reversa. Un proyecto bilateral internacional que surge de la relación entre la Universidad Nacional de San Luis y la Universidade do Minho oriunda de Portugal.

Introducción

Las aplicaciones web son utilizadas en una amplia variedad de áreas, entre ellas: redes sociales, compras, actividad bancaria, sistemas de control, almacenamiento en la nube y demás. Inclusive desde el año 2011, el 75% de la distribución de aplicaciones por

categorías correspondía a aplicaciones web [1].

Para intentar satisfacer la incesante demanda de aplicaciones de este tipo, los usuarios ocasionalmente se ven rodeados de software que no fue desarrollado siguiendo un modelo adecuado, que no ha sido codificado de manera correcta, posee un diseño defectuoso, entre otros tantos factores que vuelven a los sistemas poco robustos y con grandes falencias en seguridad [2,3].

En un contexto de conectividad permanente entre los usuarios, el concepto de "seguridad" se vuelve un factor fundamental [4]. Este motivo, entre otros, es el principal desencadenante de una disciplina que se encuentra en auge en distintos contextos de la actualidad, la misma es conocida como: *seguridad informática*.

La noción de seguridad en los sistemas de información, la cual se extiende a diversos entornos como software embebidos, entornos móviles, aplicaciones web, entre otros; se define como un grupo de componentes vinculados y parcialmente superpuestos, de los cuales se pueden destacar las siguientes particularidades [5]:

Seguridad: envuelve características en concordancia con la protección del sistema, sus aplicaciones y los recursos compartidos. Incluye la prevención de la adquisición y modificación no autorizada de información, es decir, se intenta cubrir tanto la seguridad del sistema, como la de los datos del usuario.

Fiabilidad, disponibilidad y recuperación: indican, respectivamente, la exactitud de la seguridad del sistema y otras funciones del mismo, el soporte a través del tiempo de un sistema seguro y la capacidad de recuperación del mismo luego de haber sufrido un ataque o algún tipo de error/accidente.

Auditabilidad: implica el seguimiento de la continua existencia de seguridad y fiabilidad del sistema, incluyendo la detección de anomalías o un comportamiento amenazante.

Un camino factible para conseguir como producto final un software que provea mecanismos de seguridad adecuados, es seguir un enfoque correctivo [6]. Esto quiere decir, llevar a cabo la evaluación de la seguridad de los sistemas informáticos a posteriori de su desarrollo. En este sentido, es preciso hacer referencia a un conjunto de herramientas denominadas: "*Herramientas de Análisis de Seguridad de Software*".

El objetivo de dichas herramientas de análisis es encontrar aquellos puntos donde el sistema informático sufre problemas relacionados con la seguridad o inclusive, identificar vulnerabilidades que podrían ser potencialmente conflictivas [7,8]. Para llevar a cabo el proceso de análisis, estas herramientas hacen uso de diferentes técnicas, por lo general su modus operandi es simular ataques en contra de la aplicación en tiempo de ejecución y, acorde a las respuestas obtenidas, generar los reportes necesarios. No obstante, se dan situaciones donde para buscar falencias específicas, la herramienta también debe ser capaz de observar errores de codificación de software [9,10].

Sobre el marco de las observaciones realizadas, es inevitable pensar que existe un amplio abanico de posibilidades a la hora de elegir una

herramienta que mejor se ajuste en una situación en particular. Por lo tanto, se vuelve preponderante contar con mecanismos capaces de evaluar las distintas alternativas accesibles.

Líneas de Investigación y Desarrollo: Análisis Multicriterio y Herramientas de Análisis de Seguridad

El área de toma de decisiones bajo criterios múltiples, o *Multiple-criteria decision-making* en su traducción al inglés (MCDM), explora un conjunto de métodos y procedimientos mediante los cuales, contextos de conflictos de esta índole, pueden ser formalmente incorporados a un proceso analítico.

Dentro de esta área de investigación, se encuentra la evaluación multicriterio. La misma propone dar solución a problemas donde se involucran un número finito de alternativas explícitamente conocidas antes de comenzar el proceso. Este tipo de análisis, ofrece un modelo para plasmar la opinión del encargado de tomar la decisión de la forma más crítica posible, es por ello que la utilidad de la alternativa elegida debe quedar representada por su desempeño en los criterios seleccionados para la evaluación [11].

De acuerdo con Huang et al. [12] en la última década, dentro de los métodos más utilizados se encuentran: MAUT (*Multi-Attribute Utility Theory*), AHP (*Analytical Hierarchy Process*) y *Outranking Methods*. Donde este último grupo incluye: PROMETHEE (*Preference Ranking Organization Method for Enrichment Evaluation*) y ELECTRE (*ELimination and Choice Expressing Reality*).

Todas estas propuestas abordan el problema de toma de decisiones de una manera similar. Esto quiere decir hacen uso de elementos matemáticos para asignar valores a las comparaciones, se ponderan "pesos" y luego se combinan estos resultados parciales para producir un resultado final.

De cualquier forma, sin importar que medio se utilice para realizar la comparación, es importante sentar las bases de específicamente que características influyen en la elección de una herramienta de análisis de seguridad.

De acuerdo con el Instituto SANS [13], en el ámbito de aplicaciones web, estas herramientas se pueden clasificar, teniendo en cuenta la forma que utilicen para llevar a cabo sus procesos, en al menos tres categorías: i) bloqueo de ataques: basados en la red de datos y en el servidor, ii) eliminación de vulnerabilidades y iii) soporte seguro para usuarios autorizados.

Esto impulsa la idea de que existe una gran variedad de posibilidades (con distintas prestaciones) a la hora de seleccionar una herramienta que ejecute un proceso de análisis de seguridad para aplicaciones web y es la principal razón de que surja la necesidad de relevar el estado del arte en cuanto a la evaluación de analizadores. En este contexto, el objetivo es conseguir un conjunto de características que pueda representar el comportamiento deseable en este tipo de software. Para concluir esta sección cabe destacar que esta línea de investigación se divide en dos temáticas relevantes: i) el estudio y selección de un método de análisis multicriterio adecuado y ii) el análisis y formación de un conjunto de criterios que sirvan para englobar todos los atributos que se deben tener en cuenta

a la hora de llevar a cabo un proceso de evaluación sobre herramientas de análisis de seguridad.

Resultados Obtenidos y Objetivos

A continuación se mencionan los resultados obtenidos hasta el momento dentro del marco de la línea de investigación planteada.

Por un lado, dentro del estudio y selección de un método de evaluación, se optó por elegir el Proceso de Análisis Jerárquico, conocido por sus siglas AHP.

Para entrar un poco en contexto, AHP hace uso de comparaciones por pares de cada elemento del problema bajo la interrogativa de: ¿Qué tantas veces es más importante un elemento por sobre otro? Y como consecuencia, el procedimiento de comparación se vuelve más simple y flexible [14]. Además, proporciona métodos para computar que tan consistentes (o no) están siendo los resultados que se van obteniendo, lo que da como producto final del proceso, tanto prioridades globales para cada una de las alternativas (posibles candidatos) involucradas, como así también medidas de consistencia para los juicios realizados.

En síntesis, la elección del método AHP por sobre otros, se justifica bajo las siguientes características: i) garantiza el tratamiento de todas las aristas involucradas en el proceso, de forma centralizada e independiente, a través del uso de una jerarquía para organizar el problema, ii) brinda herramientas para la comprobación del nivel de consistencia de los juicios realizados y por lo tanto, la calidad de los resultados obtenidos, iii) es relativamente sencillo de implementar y no precisa de muchos cálculos para obtener resultados y por último, iv) es un método muy utilizado a la hora de llevar a cabo problemas de decisión bajo criterios múltiples.

Por otro lado, en cuanto a la selección de atributos deseables, se hizo un relevamiento del estado del arte respecto a la evaluación de herramientas de análisis de seguridad, a partir del cual se pudo construir un árbol de criterios. Es importante remarcar que el árbol construido es una adaptación de los criterios expuestos en el "*Web Application Security Scanner Evaluation Criteria*" [9], el cual sirvió de base para dar un enfoque claro a la evaluación de escáneres de vulnerabilidades. Tal y como se dijo anteriormente, estas características tienen como objetivo sintetizar, de la manera más completa posible, todos los puntos que debe cubrir un escáner de seguridad para que sea lo más eficaz y eficiente posible. A continuación se expone una breve descripción de cada una:

Soporte de Protocolos: para llevar a cabo un análisis, un escáner debe admitir todos los protocolos de comunicación son comúnmente utilizados por las aplicaciones web.

Autenticación: es necesaria la compatibilidad con métodos de autenticación estándar o ampliamente utilizados para poder probar de manera efectiva las aplicaciones que requieren autenticación.

Manejo de Sesiones: durante una búsqueda de vulnerabilidades web, es importante que los escáneres mantengan sesiones válidas con la aplicación en todo momento.

Buscador: este proceso consiste en recorrer recursivamente todos los enlaces que se vayan presentando a partir de la página principal de la aplicación. Los rastreadores le deben permitir al usuario definir una gran cantidad de criterios para garantizar una exploración exhaustiva y eficiente.

Parsing: para escanear completamente una aplicación web en busca de problemas de seguridad, un escáner primero debe ser capaz de reconstruir en una imagen los aspectos arquitectónicos y funcionales de la misma.

Testing: este criterio incluye los tipos de vulnerabilidades que un escáner de aplicaciones web debería ser capaz de detectar, así como las opciones de configuración y personalización relacionadas con las pruebas que debería proporcionar.

Reportes: lo que queda luego de un proceso de análisis son las conclusiones. Para conseguir un buen resultado, es necesario que los reportes que se produzcan de la forma más clara y concisa que se pueda.

Ya definido el árbol de criterios, en relación, tanto al estudio de la toma de decisiones multicriterio, como a la seguridad informática, en el marco de esta investigación se llevó a cabo el desarrollo de "*DAST: Decision Analysis Software Tool*", una aplicación web que implementa el Proceso de Análisis Jerárquico.

Esta herramienta ofrece prestaciones que le permiten resolver el problema de toma de decisión planteado, de forma semi-automática. Por un lado, teniendo disponible para el uso un árbol de criterios (detallado en la sección anterior) para evaluar herramientas de análisis de seguridad y por otra parte, simplificando la tarea de realizar los cálculos matemáticos subyacentes al método AHP. De cualquier forma, es importante remarcar que DAST está pensada para usuarios que deseen resolver un problema de toma de decisiones bajo múltiples criterios de cualquier índole, no sólo referido a analizadores de seguridad.

En cuanto a objetivos en el corto/mediano plazo, se pretende: i) dejar a DAST funcionando como una herramienta "*as a service*" y conseguir la fácil integración con otros sistemas que lo usen para resolver problemas de toma de decisión. Esta tarea implica definir una firma y dejar el sistema subido en producción para que pueda ser accedido por el público. ii) Mejorar el Árbol de Criterios para el Dominio de Escáneres de Seguridad incluyendo otros criterios importantes (veracidad, performance, entre otros). Y por último, iii) llevar a cabo evaluaciones sobre distintas herramientas de análisis de seguridad que se utilizan actualmente en la industria.

Formación de Recursos Humanos

Las tareas llevadas a cabo en la presente línea de investigación están siendo desarrolladas como parte de un Proyecto Final Integrador en Ingeniería en Informática en la Universidad Nacional de San Luis. Se pretende que los resultados obtenidos durante el desarrollo de las tesis den origen a estudios de posgrado de los integrantes del proyecto en el que se encuentra enmarcada dicha línea de investigación. Permitiendo, de esta manera, el crecimiento académico de los integrantes de la línea como así también la generación de proyectos de investigación basados en seguridad informática.

Bibliografía

[1] VERACODE. State of software security report. The Intractable Problem of Insecure Software. 2011.

[2] PRESSMAN, Roger S. Software engineering: a practitioner's approach. Palgrave Macmillan, 2005.

[3] BLACK, Paul E. Software Assurance Metrics and Tool Evaluation. En Software Engineering Research and Practice. 2005. p. 829-835.

[4] MITRE. The standard for information security vulnerability names. Common Vulnerabilities and Exposures, 2005.

[5] SONG, Jihong; HU, Guiying; XU, QuanSheng. Operating system security and host vulnerability evaluation. En 2009 International Conference on Management and Service Science. IEEE, 2009. p. 1-4.

[6] NEUMANN, Peter G. Computer system security evaluation. En National Computer Conference. 1978.

[7] WEB APPLICATION SECURITY CONSORTIUM, et al. Web application security scanner evaluation criteria. Version, 2009, vol. 1, p. 1-26.

[8] BLACK, Paul E., et al. Software assurance tools: Web application security scanner functional specification version 1.0. Special Publication, 2008, p. 500-269.

[9] ARTHO, Cyrille; BIERE, Armin. Combined static and dynamic analysis. Electronic Notes in Theoretical Computer Science, 2005, vol. 131, p. 3-14.

[10] GANDIBLEUX, Xavier (ed.). Multiple criteria optimization: state of the art annotated bibliographic surveys. Springer Science & Business Media, 2006.

[11] HUANG, Ivy B.; KEISLER, Jeffrey; LINKOV, Igor. Multi-criteria decision analysis in environmental sciences: Ten years of applications and trends. Science of the total environment, 2011, vol. 409, no 19, p. 3578-3594.

[12] VAIDYA, Omkarprasad S.; KUMAR, Sushil. Analytic hierarchy process: An overview of applications. European Journal of operational research, 2006, vol. 169, no 1, p. 1-29.

[13] HARDIKAR, A.; BAMBENEK, J. C. A. Malware 101—Viruses. SANS Institute InfoSec Reading Room, 2008.