Un Modelo para la Evaluación de la Seguridad en Sistemas Informáticos

Aristides Dasso, Ana Funes

SEG / Departamento de Informática / Facultad de Ciencias Físico-Matemáticas y Naturales / Universidad Nacional de San Luis
Ejército de los Andes 950, D5700HHW San Luis, Argentina
+54 (0) 266 4520300, ext. 2126
{arisdas, afunes}@unsl.edu.ar

Resumen

Dentro del contexto de desarrollo de modelos de evaluación de sistemas complejos, esta investigación tiene como objetivo el concretar un modelo que permita evaluar el nivel de seguridad de sistemas informáticos. Para ello, comenzamos por establecer un conjunto de características (los requisitos de seguridad) en formato jerárquico, tomado de la norma ISO 2700, para luego, aplicando el método de evaluación Logic Scoring of Preference (LSP), construir un modelo adecuado que permita obtener un resultado numérico final entre 0 y 100 el cual indique claramente cuál es el grado de seguridad del sistema bajo evaluación.

Palabras clave: Seguridad de Sistemas Informáticos. Evaluación de la Seguridad de Sistemas Informáticos. Métodos de Evaluación. Logic Scoring of Preference (LSP).

Contexto

Este trabajo de investigación se viene llevando a cabo dentro del SEG (Software Engineering Group), en el ámbito de la Universidad Nacional de San Luis y se encuentra enmarcado dentro de una de las líneas de investigación del Proyecto de Incentivos código 22/F222 “Aspectos de alta sensibilidad en el ejercicio de la profesión de Ingeniero de Software” (Director: Daniel Riesco, Co-Director: Roberto Uzal. Acreditado con evaluación externa. Financiamiento: Universidad Nacional de San Luis).

Introducción

La construcción de modelos de evaluación de sistemas complejos, entre los que se encuentran los sistemas de seguridad informática, constituye una necesidad primordial para garantizar que las medidas, herramientas, métodos, etc., tomadas en ese sentido sean las más adecuadas en un entorno dado.

Existen propuestas, no sólo de cómo organizar e implementar la seguridad de sistemas informáticos, sino también de cómo se puede certificar la seguridad de los mismos. Por ejemplo Common Criteria Schemes [13][14]es un método que armoniza criterios sobre seguridad de productos de software y hardware que se aplica en varios países. Ha recibido algunas críticas ya que las certificaciones que otorga pueden ser parciales (ver por

ejemplo [15], [16]).

Se encuentran, además, en la literatura, en empresas y en organismos gubernamentales, numerosas referencias a modelos, métricas, y sistemas de evaluación de la seguridad (ver por ejemplo [17], [18], [19], [20], [21]).

Cabe aclarar que el método LSP (Logic Score of Preferences) [1], [6], [7], [8], que adoptamos para construir nuestros modelos de evaluación, es un método que se basa en el empleo de una lógica continua, que permite la creación de funciones complejas de evaluación y su aplicación en la evaluación y comparación de sistemas de índole general, permitiendo la creación de modelos precisos y fácilmente adaptables a las necesidades del usuario, en este caso las necesidades de Seguridad de un sistema informático.

El proceso general propuesto por el método LSP es mostrado en la Figura 1. El desarrollo e identificación de la lista de características principales a tener en cuenta (requisitos) corresponde al primer nivel del *árbol de requerimientos* que el método prescribe construir en una de sus etapas.

Cada una de estas características del primer nivel comprende varios ítems o categorías más específicas de acuerdo con propiedades similares, tales que las mismas puedan ser razonablemente agrupadas, y así sucesivamente, llegando hasta ítems que no se desagregan, donde encontramos las 'hojas' del árbol de requerimientos, llamadas *variables de performance*.

Las hojas del árbol de preferencias son empleadas para construir una *estructura de agregación* junto con los operadores de Lógica Continua provistos por el método. Estos operadores o funciones GCD (Generalized Conjunction Disjunction) nos permiten agregar los valores observados de cada una de las variables de performance, previamente mapeados a valores en el intervalo [0, 100] llamados *preferencias elementales*, por medio de funciones llamadas *criterios elementales*. Las preferencias elementales representan el grado de cumplimiento con un requisito del sistema bajo evaluación.

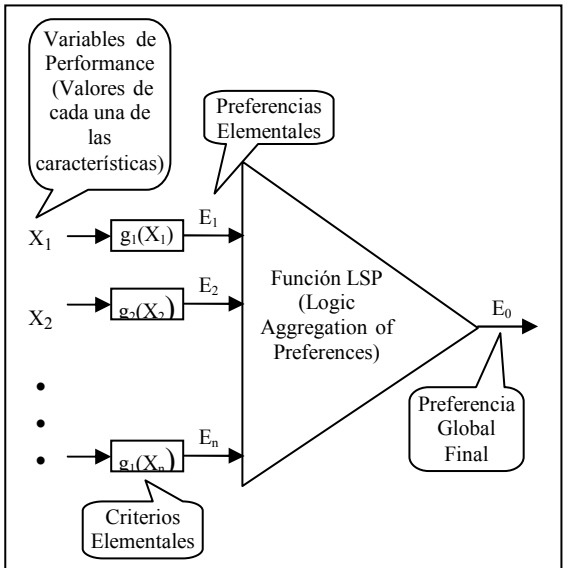

Figura 1. Una visión genérica del proceso de evaluación de LSP.

La estructura de agregación tiene como objetivo obtener, como resultado final un único valor (preferencia global final E_0 en la Figura 1) entre 0 y 100 que representa el grado de adecuación o de satisfacción de todas las características consideradas para el sistema bajo evaluación.

Así, por ejemplo, para alguna de las características que un sistema debería poseer, el valor asignado a la correspondiente variable de performance corresponderá a la valoración que se haga del mismo; dicho valor se trasformará, con el correspondiente criterio elemental, en un valor del intervalo [0,100]. La relación entre el valor asignado a la variable y el intervalo será justamente propia de la elección del criterio elemental por parte de quienes construyan

el modelo.

Líneas de Investigación, Desarrollo e Innovación

La línea de investigación en la que se enmarca el trabajo presentado, es parte de una línea de investigación sobre el tema de la construcción de modelos de evaluación de sistemas complejos y que viene desarrollándose desde hace tiempo en el ámbito del SEG (Software Engineering Group), donde se han obtenido resultados plasmados en diversas publicaciones (ver por ejemplo [2], [3], [4], [10], [11], [12]).

Resultados y Objetivos

En una primera etapa nos encontramos desarrollando un modelo de evaluación que sigue de manera general las directivas establecidas en la norma ISO/IEC 27002. "Information technology - Security techniques - Code of practice for information security controls" [5]. Esta norma establece, como el título sugiere, un código de prácticas. El estándar tiene catorce cláusulas que en total establecen treinta y cinco categorías principales y ciento catorce controles.

Tanto las cláusulas, como las categorías y los controles tienen definidos sus objetivos y condiciones de ejecución e implementación, además de otra información útil para su ejecución.

En la Figura 2 mostramos, a modo de ejemplo, un árbol de preferencias parcial construido a partir de una de las catorce cláusulas, en este caso la cláusula "5. Access control", la que ha sido desagregada en sus cuatro categorías. Hay que remarcar que cada una tiene sus correspondientes controles (que no se muestran aquí por razones de espacio).

5. Access control.
   - 5.1. Business requirements of access control.
   - 5.2. User access management.
     - 5.2.1. User registration and de-registration.
     - 5.2.2. User access provisioning.
     - 5.2.3. Management of privileged access rights.
     - 5.2.4. Management of secret authentication information of users.
     - 5.2.5. Review of user access rights.
     - 5.2.6. Removal or adjustment of access rights.
   - 5.3. User responsibilities.
   - 5.4. System and application access control.

Figura 2. Variables de performance para la cláusula 5 [5].

Notemos que el árbol de preferencias y las variables de performance consideradas es una elección de quién o quienes construyen el modelo sobre la base de las necesidades del usuario.

A partir de un árbol de requerimientos, se pueden generar diversas estructuras de agregación como modelos de evaluación, previa clasificación de los distintos aspectos que el usuario considere mandatarios, opcionales y deseables para un sistema de seguridad. En la Figura 3 mostramos la estructura de agregación para el ítem "5.2. User access mangement."

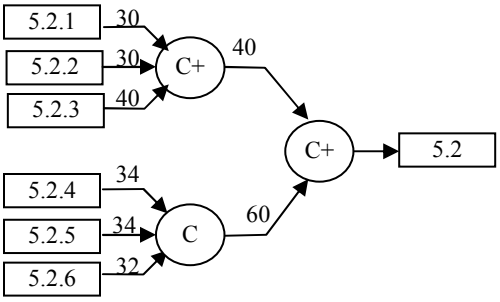

Figura 3. Estructura de agregación para el requisito 5.2. User access mangement.

Para asignar un valor a cada una de las variables de performance se sigue lo

prescripto por la norma en cada ítem (ver para este caso [5], págs. 21 y siguientes).

Como parte del trabajo futuro, esperamos, en una etapa siguiente, calibrar los modelos producidos, además de aplicarlos a casos reales. Asimismo, creemos que el modelo debería incluir la evaluación de los costes económicos de los aspectos de seguridad de los sistemas. Establecer el coste/beneficio de la seguridad es un aspecto sumamente importante para los usuarios.

También nos encontramos trabajando en la generación de un cuestionario para las empresas proveedores de sistemas de seguridad informática en todos sus niveles, con el objeto de obtener mayor información sobre las características de los sistemas ofrecidos, con el objeto de ampliar y/o mejorar nuestros modelos.

Formación de Recursos Humanos

Dentro del SEG (Software Engineering Group), en el ámbito de la Universidad Nacional de San Luis, en el que se realiza el Proyecto de Incentivos código 22/F222 "Aspectos de alta sensibilidad en el ejercicio de la profesión de Ingeniero de Software", se han llevado a cabo numerosas tesis de grado y de posgrado.

Entre otros, nos hemos concentrado en la evaluación de sitios de gobierno electrónico lo que ha dado como resultado una tesis de maestría en 2010; mientras que hay otras dos en preparación. La construcción del modelo aquí expuesto, también, tiene como objetivo ser motivo de tesis, como lo han sido la construcción de otras herramientas en el ámbito del proyecto.

Referencias

[1] Jozo J. Dujmovic, "Continuous Preference Logic for System Evaluation", IEEE Transactions on Fuzzy Systems, Vol. 15, Nº 6, December 2007

[2] A. Dasso, A. Funes, M. Peralta, C. Salgado, "Una Herramienta para la Evaluación de Sistemas", Workshop de Investigadores en Ciencias de la Computación, WICC 2001, Universidad Nacional de San Luis, San Luis, Argentina, May 2001.

[3] Ana Funes, Aristides Dasso, "Web Application Frameworks Evaluation", CONAIISI 2014, 13 y 14 de noviembre de 2014, San Luis, Argentina. pp. 1063-1070. ISSN: 2346-9927.

[4] Ana Funes, Aristides Dasso, Carlos Salgado, Mario Peralta, "UML Tool Evaluation Requirements". Argentine Symposium on Information Systems ASIS 2005. Rosario, Argentina. September 29-30, 2005.

[5] ISO/IEC 27002. "Information technology - Security techniques - Code of practice for information security controls". Second edition, 2013-10-01. Reference number ISO/IEC 27002:2013(E)

[6] J. J. Dujmovic and A. Bayucan, "Evaluation and Comparison of Windowed environments", Proceedings of the IASTED Interna Conference Software Engineering (SE'97), pp 102-105, 1997.

[7] J. J. Dujmovic, "A Method for Evaluation and Selection of Complex Hardware and Software Systems", The 22nd International Conference for the Resource Management and Performance Evaluation of Enterprise Computing Systems. CMG96 Proceedings, vol. 1, pp.368-378, 1996.

[8] J. J. Dujmovic, "Quantitative Evaluation of Software", Proceedings of the IASTED International Conference on Software Engineering, edited by M.H. Hamza, pp. 3-7, IASTED/Acta Press, 1997.

[9] M. Castro, A. Dasso, A. Funes. "Modelo de Evaluación para Sitios de Gobierno Electrónico". 38 JAIIO/SIE 2009, Simposio de Informática en el Estado 2009, Mar del Plata, Argentina, August 26-28, 2009.

[10] N. Debnath, A. Dasso, A. Funes, G. Montejano, D. Riesco, R. Uzal, "The LSP Method Applied to Human Resources Evaluation and Selection", Journal of Computer Science and Information Management, Publication of the Association of Management/International Association of Management, Volume 3, Number 2, 2000, ISBN 1525-4372, pp.1-12.

[11] N. Debnath, A. Dasso, A. Funes, G.

Montejano, D. Riesco, R. Uzal, "The LSP Method Applied to Human Resources Evaluation and Selection", Journal of Computer Science and Information Management, Publication of the Association of Management/International Association of Management, Volume 3, Number 2, 2000, ISBN 1525-4372, pp.1-12.

[12] Narayan Debnath, Aristides Dasso, Ana Funes, Roberto Uzal, José Paganini. "E-government Services Offerings Evaluation Using Continuous Logic". 2007 ACS/IEEE International Conference on Computer Systems and Applications, AICCSA '2007, Amman, Jordan. Sponsored by IEEE Computer Society, Arab Computer Society, and Philadelphia University, Jordan. May 13-16, 2007.

[13] The Common Criteria http://www.commoncriteriaportal.org/ (Recuperado marzo 2015)

[14] The National Information Assurance Partnership/Common Criteria Evaluation and Validation Scheme (NIAP/CCEVS) https://www.niap-ccevs.org/ (Recuperado marzo 2015)

[15] Wikipedia http://en.wikipedia.org/wiki/Common_Criteria#Criticisms (Recuperado marzo 2015)

[16] William Jackson, "Under attack". GCN. 2007. http://gcn.com/articles/2007/08/10/under-attack.aspx (Recuperado marzo 2015)

[17] Barabanov, Rostyslav; Kowalski, Stewart; Yngström, Louise. "Information Security Metrics: State of the Art". DSV Report series No 11, 2011. http://www.diva-portal.org/smash/get/diva2:469570/FULLTEXT01.pdf (Recuperado marzo 2015)

[18] Department of Homeland Security (DHS) Control Systems Security Program (CSSP. Cyber Security Evaluation Tool. https://ics-cert.us-cert.gov/sites/default/files/documents/DHS_CyberSecurity_CSSP-CSET-v4.pdf (Recuperado marzo 2015)

[19] Payment Card Industry Security Standards Councilhttps://www.pcisecuritystandards.org/security_standards/role_of_pci_council (Recuperado marzo 2015).php

[20] LeMay, E.; Ford, M.D.; Keefe, K. ; Sanders, W.H. ; Muehrcke, C. "Model-based Security Metrics Using ADversary VIew Security Evaluation (ADVISE)". Eighth International Conference on Quantitative Evaluation of Systems (QEST), 5-8 Sept. 2011, Publisher: IEEE. Print ISBN: 978-1-4577-0973-9

[21] Andy Ju An Wang. "Information security models and metrics". ACM-SE 43 Proceedings of the 43rd annual Southeast regional conference – Volume 2, Pages 178-184. ACM New York, NY, USA ©2005 ISBN:1-59593-059-0