Elaboración de Especificación de Requerimientos de Seguridad en el desarrollo de Sistemas de Información basado en la Modelización de Conocimientos.

Bajarlía, María Victoria Soledad [(1)] , Eterovic Jorge [(2)] , Ierache Jorge Salvador [(3)]

Escuela de Posgrado Facultad Regional Buenos Aires - Universidad Tecnológica Nacional
Castro Barros 91 (C1178AAA) C.A.B.A. Argentina . Tel: (54 11) 4983-8882
victoriabajarlia@hotmail.com [(1)] , jeterovic@hotmail.com [(2)], jierache@yahoo.com.ar[(3)]

Resumen

El objetivo del presente trabajo es expresar los aspectos fundamentales elegidos para proponer un modelo de un Sistema Basado en Conocimiento (SBC) aplicado al análisis de seguridad de aplicaciones, a través de la incorporación de los requerimientos funcionales y no funcionales en el contexto de un Framework que asista en el desarrollo de una especificación de requerimientos de software, en el aspecto especifico de la seguridad de aplicaciones.

1. Introducción

El aporte del presente trabajo es diseñar un sistema basado en conocimiento (SBC) aplicado al análisis de la seguridad de aplicaciones. La base de conocimiento será alimentada permanentemente por normas, estándares y mejores prácticas vigentes así como por aquellos informes de vulnerabilidades que tomen conocimiento público en la comunidad informática. El motor de inferencia, el cual trabajará sobre un universo abierto, tomará la información suministrada por la base de conocimiento para analizar la seguridad de una aplicación determinada. La solución del problema a través del método elegido comprenderá desde el análisis de seguridad de aplicaciones de gestión hasta el control de que las mismas cumplan con el marco regulatorio.

2. Líneas de investigación

El avance tecnológico y el desarrollo de aplicaciones informáticas para soportar las necesidades del negocio de una organización hace imperioso cruzar fronteras, por ejemplo acceder desde la Web hasta llegar a una base de datos que está gestionada por un software que corre sobre un equipo Mainframe. De este modo la explotación de la aplicación se realiza atravesando diversas capas e integrando diferentes plataformas existentes en la organización. Dado que las capas tienen distintas naturalezas de seguridad, es necesario implementar un mecanismo eficiente que permita que las aplicaciones sean realmente seguras cumpliendo con los estándares respectivos y permaneciendo altamente alineadas con la tecnología. [3] [4] [5] [6] [18] [19].

Para abordar esta problemática se propone un sistema basado en conocimientos (SBC) que asista a la elaboración de especificaciones de requerimientos de software (ERS) a fin de contribuir con el desarrollo de aplicaciones que contribuyan eficientemente a reducir las potenciales vulnerabilidades de las aplicaciones.

2.1 Áreas involucradas en el dominio del problema de estudio

Las áreas que participan en el contexto del tema de estudio propuesto involucran: (a) Seguridad de la Información (SI). Engloba la investigación del área de la seguridad de aplicaciones de gestión.

[22] [23] [24].(b) Ingeniería de Requerimientos (IR). Se basa inicialmente en el estándar IEEE-830 de Especificación de Requisitos de Software (ERS), sobre el cual se realizarán las aportaciones en función del modelo de conocimiento que se obtenga del trabajo con los expertos en el área de Seguridad de la Información, a partir de las consideraciones que surjan en relación a requerimientos funcionales y no funcionales. [10]. (c) Ingeniería de Conocimiento (INCO). Incorpora el marco metodológico y las técnicas aplicadas al desarrollo de un Sistema Basado en Conocimiento (SBC) en el contexto dado de la INCO. Quedará comprendido en la extracción de conocimientos y la educción de conocimientos con los expertos del área de seguridad. (d) Sistema basado en conocimiento (SBC), comprende la implementación de un Framework que asista a la elaboración de los aspectos de seguridad de la aplicación en el marco de una ERS, a través de la incorporación de los aspectos de la materia de estudio en el modelo de conocimiento del experto de campo. Por último, y como conclusión, abarcará la implementación de un prototipo de SBC para el análisis y evaluación de ERS en los aspectos de seguridad, desde el punto de vista de la IR.

Es importante señalar el mecanismo de interacción de las áreas involucradas, la integración de las mismas constituirá el SBC. En este orden se muestran en la figura 1 las interacciones entre las áreas: (a) **IR-SI**. Aporta la base metodológica para construir las Especificaciones de Requerimientos de Software de Seguridad en el aspecto especifico de Seguridad (ERSs) según el estándar IEEE-830. (b) **IR-INCO**. Aporta la metodología para el desarrollo del SBC en el contexto de la IR. (c) **SI-INCO**, aporta la conceptualizacion como producto de la extracción de conocimiento (marco regulatorio, mejores prácticas, etc.) y la educción de conocimiento (entrevistas con el experto y trabajo de campo),para la formalización e implementación del SBC. (d) como resultado de la interacción de las áreas involucradas se desarrollara un Framework de asistencia para la elaboración de FERSs sobre la base del SBC.

A modo de síntesis en el marco de la fundamentación del tema seleccionado se representan conceptualmente las áreas involucradas en el trabajo y su interacción en la figura 1. En concordancia con lo descripto anteriormente y su aportación en relación a la investigación en materia del estado del arte en SI y en el marco metodológico la aplicación de INCO, presentando como producto el desarrollo un prototipo de SBC.

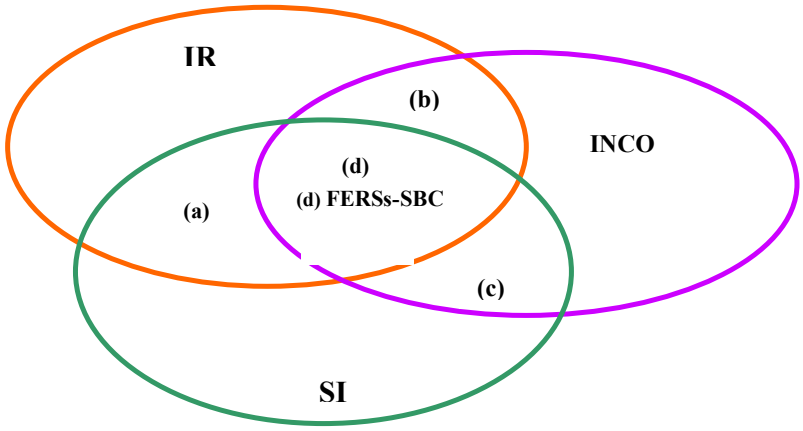

Figura 1 - Representación conceptual de las áreas involucradas.

2.2 Estado del arte de seguridad de la información

La situación actual demuestra que, si bien existe un importante nivel de madurez en materia de Seguridad de la Información respecto de la infraestructura tecnológica organizacional, no sucede lo mismo con las aplicaciones que son soportadas por dicha infraestructura. Esto conlleva a una falta de alineación entre los desarrolladores y los especialistas en el análisis de vulnerabilidades en aplicaciones. Finalmente esta falta de alineación puede poner en riesgo uno de los activos más importantes que tiene una organización: su información. [8] [11] [12] [13] [14] [15] [16] [17]

Como una evaluación preliminar del problema que origina este trabajo de investigación se hará una extracción y educción de expertos de conocimiento. Esto significa, en primer lugar, evaluar el tipo de seguridad que corresponde aplicar en cada una de las capas o layers que componen el desarrollo de un software. En segundo lugar se evaluará el trabajo de un experto en esta materia a fin de extraer el conocimiento necesario en relación a las posibles vulnerabilidades de software que pueden surgir con el crecimiento tecnológico.

2.3 Ingeniería de Conocimiento - Modelo del conocimiento de Seguridad de la Información

A fin de desarrollar un modelo del conocimiento de Seguridad de la Información resulta necesario adquirir y conceptualizar el conocimiento específico en este dominio formalizado a través de un SBC [7] [9] . El SBC que asistirá a la evaluación de ERS desde el punto de vista de los requisitos de Seguridad de la Información para aplicaciones a través de un Framework que contendrá los aspectos específicos para el desarrollo y evaluación de la ERSs.

3. Metodología de desarrollo

El desarrollo se articulara considerando las siguientes fases: Fase I (Identificación de la tarea) se consideran los objetivos del proyecto del Sistema Experto (SE). Involucra el proceso de **adquisición y extracción** de conocimiento. Aplicado al problema resolver, significará adquirir el conocimiento necesario en lo referente al marco regulatorio para Seguridad de la Información, así como hacer **educción** de expertos en esta materia. Fase II (Desarrollo del prototipo) se continuará con la adquisición de conocimientos, se evaluará la **viabilidad** del sistema y se llegará a la **conceptualización** y **formalización** de los conocimientos e **implementación** del prototipo que permitirá validar con el experto el modelo de SBC.

Como herramientas para desarrollo se utilizarán **Protégé** y **CLIPS**. La primera de ellas es una plataforma "open-source" que provee un conjunto de herramientas para construir modelos de dominio y aplicaciones basadas en conocimiento a través de ontologías. A su vez, Protégé implementa un amplio conjunto de estructuras de modelado del conocimiento así como acciones que soportan la creación, visualización y manipulación de ontologías en diversos formatos de representación. [1] [2] [21].

CLIPS se utilizará dado que se necesita una herramienta que permita, a través de su entorno de desarrollo, una forma rápida de realizar prototipos. De esta forma se pueden obtener aplicaciones que podrán ser reutilizadas en la manera que se incremente el conocimiento adquirido y así llegar a un desarrollo basado en prototipos incrementales.

4. Conclusiones y trabajo futuro

En virtud de que las amenazas y los ataques informáticos representan un problema constante y creciente se puede suponer que el SBC, a través del mantenimiento del conocimiento que lo mantendrá actualizado, podrá asistir a los especialistas en Seguridad de la Información, en el área de competencia, a la elaboración de ERS.

Se desarrollara un prototipo del SBC considerando las fases de adquisición de conocimientos, conceptualización, formalización, implantación y pruebas a fin de dar respuesta al problema planteado de manera eficiente. Se deberá asegurar que el desarrollo de aplicaciones permanezca alineado con la tecnología y cumpla con los estándares para seguridad de aplicaciones. La metodología para desarrollar el modelo incluye: la representación del conocimiento considerando el conocimiento fáctico, táctico, estratégico, su representación y síntesis a través del modelo estático y dinámico para brindar la síntesis final con el mapa de conocimiento que facilitará la formalización en **marcos** y reglas de producción para la construcción de:

- Una base de hechos a partir de normas, estándares, mejores prácticas e informes de vulnerabilidades.
- Una base de reglas con las acciones de seguridad a llevar a cabo a partir del análisis de vulnerabilidades
- La explotación de un motor de inferencia que active las reglas a partir de la información de la base de hechos.

Para la adquisición de conocimiento, además del marco teórico brindado por los estándares, mejores prácticas y otros aspectos relacionados con la Seguridad de la Información, se recurrirá al método de entrevistas con expertos en el dominio del problema. Este proceso, que se irá refinando a lo largo de toda la toma de datos, se formalizará a través de encuestas, observaciones del trabajo de campo y registración en contextos reales del problema. La parte experimental se basará en la elaboración de un prototipo, para probar el modelo propuesto.

Formación de recursos humanos

En el marco de formación de recursos humanos se encuentra en este momento en desarrollo una tesis de Magíster relacionada con la línea de investigación de este trabajo.

5. Referencias bibliográficas

[1] Fernández Galán, S., González Boticario, J., Mira Mira, J., "Problemas resueltos de Inteligencia Artificial Aplicada. Búsqueda y representación" (Addison-Wesley, 1998).

[2] Giarratano, J., Riley, G., "Sistemas Expertos Principios y Programación" (Thomson International, 2000).

[3] Harrison, R., "ASP/MTS/ADSI Web Security" (Longman, 1999).

[4] Jaworski, J., Perrone, P.J., "Seguridad en Java" (Prentice Hall, 2000).

[5] Kaeo, M., "Diseño de Seguridad en Redes" (Pearson Educación, 2003).

[6] Maiwald, E., "Fundamentos de la seguridad de redes. Conocimientos esenciales a tu alcance" (McGraw-Hill, 2005).

[7] Maté Hernández, J.L., Pazos Sierra J., "Ingeniería del Conocimiento. Diseño y construcción de sistemas expertos" (Sepa S.A.,1988).

[8] Piattini Velthuis, M., Del Peso Navarro, E., "Auditoría informática un enfoque práctico" (Alfaomega Grupo Editor Argentino S.A., 2001).

[9] Rusell, S.J., Norvig, P., "Inteligencia Artificial" (Pearson Educación, 2004).

[10] Sommerville , I., "Ingeniería de Software" (Addison Wesley, 2002).

[11] ISO/IEC 27001, 2006. Gestión de la Seguridad de la Información.

[12] Sarbanes-Oxley Act of 2002, SOX 404 IT. PUBLICLAW 107-204-july 30, 2002.

[13] Stallings, W., "Fundamentos de la seguridad en redes. Aplicaciones y estándares" (Pearson Educación, 2004).

[14] ArCERT (Coordinación de Emergencias en Redes Teleinformáticas de la Administración Pública), Subsecretaría de Gestión Pública) www.arcert.gov.ar. Consultado el 02/10/2006.

[15] HISPASEC SISTEMAS. www.hispasec.com . Consultado el 20/08/2007.

[16] IEEE (Institute of Electrical and Electronics Engineers), www.ieee.org. Consultado el 13/08/2006.

[17] ISO (International Organization for Standardization), www.iso.org. Consultado el 20/10/2007.

[18] ISECOM (Institute for security and open methodologies) www.isecom.org. Consultado el 01/09/2006.

[19] NIST (National Institute of Standards and Technology, Technology Administration U.S. Department of Commerce), www.nist.gov . Consultado el 20/08/2007.

[20] PKI (Public Key Infraestructure), Subsecretaría de Gestión Pública www.pki.gov.ar

[21] Protègè www.protege.stanford.edu . Consultado el 05/12/2006.

[22] Seguridad en Windows www.microsoft.com/security . Consultado el 10/03/2007.

[23] Seguridad en Java www.java.sun.com/products/jaas. Consultado el 10/03/2007.

[24] Universidad Nacional de Tucumán, Facultad de Ciencias Exactas y Tecnología www.herrera.unt.edu.ar/ingsoftware/CSHome/CSDocu. Consultado el 10/11/2007.