La Reunión Española sobre Criptología y Seguridad de la Información (RECSI) es el congreso científico español de referencia en el ámbito de la Seguridad en las Tecnologías de la Información. En septiembre de 2010 se celebra la undécima edición de este congreso en Tarragona. Las pasadas ediciones tuvieron lugar en Palma de Mallorca (1991), Madrid (1992), Barcelona (1994), Valladolid (1996), Torremolinos (1998), Santa Cruz de Tenerife (2000), Oviedo (2002), Leganés (2004), Barcelona (2006) y Salamanca (2008).

Estas actas contienen las contribuciones de la RECSI 2010, cuyas sesiones se organizan en los siguientes ámbitos temáticos: cifrado de flujo, clave pública, criptoanálisis, firmas digitales, privacidad, protocolos, RFID, seguridad, seguridad de redes, *watermarking* y *fingerprinting*.

ISBN 978-84-693-3304-4

SPONSORS/SUPPORTERS

UNESCO Chair in Data Privacy

[DΣIM]

Universitat Rovira i Virgili

Ajuntament de Tarragona

Diputació Tarragona

AGAUR Agència de Gestió d'Ajuts Universitaris i de Recerca

Gobierno de España · Ministerio de Ciencia e Innovación

[publicacions] urv

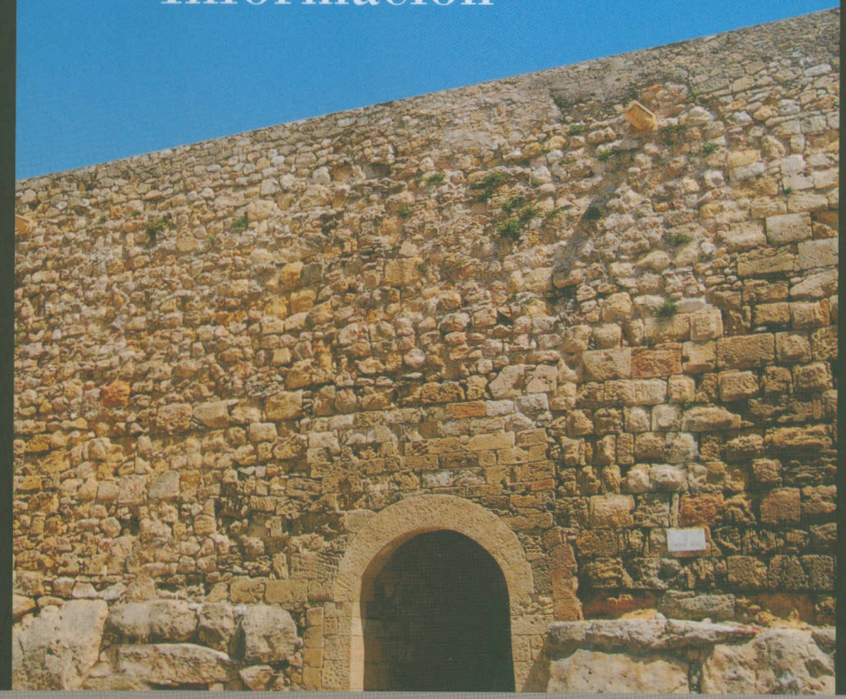
RECSI 2010 | XI Reunión Española sobre Criptología y Seguridad de la Información

RECSI 2010

Tarragona,
7–10 septiembre 2010

Coordinado por:
Josep Domingo Ferrer, Antoni Martínez Ballesté,
Jordi Castellà Roca, Agustí Solanas Gómez

XI Reunión Española sobre Criptología y Seguridad de la Información



[publicacions] urv

RECSI 2010

IX Reunión Española sobre Criptología y Seguridad de la Información

[publicacions] urv
Tarragona 2010

Edita:
Publicacions URV

1ª edició: juliol 2010

Impressió: Gràfiques Arrels, S. L.
Depòsit Legal: T-1099/2010
ISBN: 978-84-693-3304-4

Publicacions de la Universitat Rovira i Virgili:
Av. Catalunya, 35 - 43002 Tarragona
Tel. 977 558 474 - Fax: 977 558 393
www.urv.cat/publicacions
publicacions@urv.cat

Arola Editors: Polígon Francolí, parcel·la 3, nau 5 - 43006 Tarragona
Tel. 977 553 707 - Fax 977 542 721
arola@arolaeditors.com

Cossetània Edicions: C. de la Violeta, 6 - 43800 Valls
Tel. 977 602 591 - Fax 977 614 357
www.cossetania.com
cossetania@cossetania.com

RECSI 2010

IX Reunión Española sobre Criptología y Seguridad de la Información

Tarragona 7–10 de septiembre 2010

Coordinado por:
Josep Domingo Ferrer
Antoni Martínez Ballesté
Jordi Castellà Roca
Agustí Solanas Gómez

[publicacions] urv
Tarragona, 2010

Prefacio

Los grandes avances realizados en las tecnologías de la información y de las comunicaciones (TIC) han elevado nuestra capacidad de generar y compartir información hasta límites insospechados, y con esta capacidad también han aumentado los riesgos que ello supone.

El mundo electrónico-digital tiende a reemplazar a los antiguos sistemas, más lentos e ineficientes. Algunos ejemplos cotidianos los encontramos en el correo electrónico, el comercio electrónico, la votación electrónica, la administración digital, la televisión digital, etc. El mundo de lo electrónico y lo digital está llamado a ser el dominante y es por ello que resulta de vital importancia el estudio de teorías y métodos que permitan garantizar la privacidad y la seguridad de los usuarios en este nuevo contexto.

Con esta idea en mente, y con el objetivo de servir de foro de intercambio de conocimientos para los investigadores, en 1991 nació la Reunión Española sobre Criptología y Seguridad de la Información (RECSI), la cual en aquel entonces vino a llamarse Primera Jornada Española sobre Criptografía.

Este año, Tarragona acoge en septiembre la undécima edición de la RECSI, el congreso científico español de referencia en el ámbito de la seguridad en las tecnologías de la información. Las pasadas ediciones se realizaron en Palma de Mallorca (1991), Madrid (1992), Barcelona (1994), Valladolid (1996), Torremolinos (1998), Santa Cruz de Tenerife (2000), Oviedo (2002), Leganés (2004), Barcelona (2006) y Salamanca (2008).

La ciudad de Tarragona ha sido testigo de generaciones cuyas huellas han merecido el reconocimiento mundial. Como elemento representativo de esta RECSI hemos elegido la muralla, símbolo de los vestigios de la Tarragona Romana y uno de los muchos elementos patrimoniales que recomendamos visitar.

Estas actas contienen las 72 contribuciones de la RECSI 2010, cuyas sesiones se organizan en los siguientes ámbitos temáticos: cifrado de flujo, clave pública, criptoanálisis, firmas digitales, privacidad, protocolos, RFID, seguridad, seguridad de redes, watermarking y fingerprinting. Como conferenciantes invitados contamos con Ronald Cramer (Centrum Wiskunde & Informatica, Amsterdam) y Paulo Veríssimo (Universidad de Lisboa).

Desde la organización queremos expresar nuestro agradecimiento a todos los patrocinadores y colaboradores del evento, así como también a todos los ponentes, asistentes, miembros de los comités y revisores.

La compilación de las actas se realizado con LaTeX y el paquete 'confproc'.

Tarragona, septiembre de 2010

Josep Domingo Ferrer
Jordi Castellà Roca
Antoni Martínez Ballesté
Agustí Solanas Gómez

Comité de organización

Presidente

- Josep Domingo Ferrer (Universitat Rovira i Virgili)

Vicepresidentes

- Jordi Castellà Roca (Universitat Rovira i Virgili)
- Antoni Martínez Ballesté (Universitat Rovira i Virgili)
- Agusti Solanas Gómez (Universitat Rovira i Virgili)

Secretaría

- Jesús Manjón Paniagua (Universitat Rovira i Virgili)
- Gloria Pujol Crespo (Universitat Rovira i Virgili)

Comité científico

- Abascal Fuentes, Policarpo (Universidad de Oviedo)
- Álvarez Marañón, Gonzalo (C.S.I.C.)
- Amigó García, José María (Universidad Miguel Hernández)
- Areitio Bertolín, Javier (Universidad de Deusto)
- Borrell Viader, Joan (Universitat Autónoma de Barcelona)
- Bras Amorós, Maria (Universitat Rovira i Virgili)
- Caballero Gil, Pino (Universidad de La Laguna)
- Castellà Roca, Jordi (Universitat Rovira i Virgili)
- Climent, Joan-Josep (Universitat d'Alacant)
- Domingo Ferrer, Josep (Universitat Rovira i Virgili)
- Durán Díaz, Raúl (Universidad de Alcalá de Henares)
- Fernández-Medina Patón, Eduardo (Universidad de Castilla La Macha)
- Ferrer Gomila, Josep Lluís (Universitat de les Illes Balears)
- Fúster Sabater, Amparo (C.S.I.C.)
- González Vasco, Mª Isabel (Universidad Rey Juan Carlos)
- Gutiérrez Gutiérrez, Jaime (Universidad de Cantabria)
- Hernández Encinas, Luis (C.S.I.C.)
- Hernández Goya, Candelaria (Universidad de La Laguna)
- Herrera Joancomartí, Jordi (Universitat Autònoma de Barcelona)
- Huguet Rotger, Llorenç (Universitat de les Illes Balears)

- López Muñoz, Javier (Universidad de Málaga)
- Martín del Rey, Ángel (Universidad de Salamanca)
- Martínez López,Consuelo (Universidad de Oviedo)
- Megías, David (Universitat Oberta de Catalunya)
- Miret Biosca, José María (Universitat de Lleida)
- Morillo Bosch, Paz (Universitat Politècnica de Catalunya)
- Padró Laimon, Carles (Universitat Politècnica de Catalunya)
- Peinado Domínguez, Alberto (Universidad de Málaga)
- Ramió Aguirre, Jorge (Universidad Politécnica de Madrid)
- Ramos Álvarez, Benjamín (Universidad Carlos III de Madrid)
- Ribagorda Garnacho, Arturo (Universidad Carlos III de Madrid)
- Rifà Coma, Josep (Universitat Autònoma de Barcelona)
- Sáez Moreno, Germán (Universitat Politècnica de Catalunya)
- Salazar Riaño, José Luis (Universidad de Zaragoza)
- Sánchez Ávila, Carmen (Universidad Politécnica de Madrid)
- Sebé, Francesc (Universitat de Lleida)
- Sempere Luna, José María (Universitat Politècnica de València)
- Soriano Ibáñez, Miguel (Universitat Politècnica de Catalunya)
- Tena Ayuso, Juan (Universidad de Valladolid)
- Villar Santos, Jorge (Universitat Politècnica de Catalunya)
- Wu, Qianhong (Universitat Rovira i Virgili)
- Zurutuza, Urko (Universidad de Mondragón)

Programa de las sesiones

Cifrado de flujo

Clave pública

Criptoanálisis

Firmas digitales

Privacidad

Protocolos

RFID

Seguridad

Seguridad de redes

Watermarking y fingerprinting

Gestionando el riesgo de los activos de las PYMES

Luís Enrique Sánchez, Antonio Santos-Olmo
Departamento de I+D+i
SICAMAN Nuevas Tecnologías
Juan José Rodrigo, 4. Tomelloso, Ciudad Real, Spain
Email: {Lesanchez, Asolmo}@sicaman-nt.com

Eduardo Fernández-Medina, Mario Piattini
ALARCOS Research Group. TSI Department
Universidad de Castilla-La Mancha (UCLM)
Paseo de la Universidad, 4 13071 Ciudad Real, Spain
Email: {Eduardo.FdezMedina, Mario.Piattini}@uclm.es

***Resumen*—La sociedad de la información cada vez depende más de los Sistemas de Gestión y Análisis del Riesgo al que se encuentran sometidos sus principales activos de información, y poder disponer de estos sistemas ha llegado a ser vital para la evolución de las PYMES. Sin embargo, este tipo de compañías requiere que estos sistemas estén adaptados a sus especiales características. En este artículo se presenta el método propuesto para realizar un análisis de riesgos simplificado, que sea válido para las PYMES, y enmarcado dentro de la metodología de gestión de la seguridad en las pequeñas y medianas empresas (MSM2-PYME). Este modelo está siendo aplicado directamente a casos reales, consiguiendo así una constante mejora en su aplicación.**

***Palabras Clave*—PYMES; Análisis de riesgos, Activos; SGSI**

I. Introducción

Estudios realizados [1] han demostrado que para que las empresas puedan utilizar las tecnologías de la información y las comunicaciones con garantías es necesario disponer de guías, métricas y herramientas que les permitan conocer en cada momento su nivel de seguridad y las vulnerabilidades que aún no han sido cubiertas. El problema de conocer los riesgos a los que están sometidos sus principales activos se acentúa especialmente en el caso de las pequeñas y medianas empresas, que cuentan con la limitación adicional de no tener recursos humanos y económicos suficientes para realizar una adecuada gestión de sus activos [2]. Pero con la llegada de Internet, para las empresas es cada vez más critico implantar controles de seguridad que les permitan conocer y controlar los riesgos a los que pueden estar sometidas [3].

Algunos autores [4, 5] sugieren la realización de un análisis de riesgos como parte fundamental de la gestión de la seguridad en las PYMES, ya que los propietarios de estos activos deben tener en cuenta que el valor y la sanción de los datos robados o filtrados en una pequeña organización es el mismo que para una grande, y por tanto debe tener controlado el valor de los activos y los riesgos a los que están sometidos. Otros autores [6] proponen la necesidad de desarrollar un nuevo modelo de análisis de riesgos (AR) pero orientándolo directamente a las PYMES, dado que las características de éstas son diferentes que las de las grandes compañías, considerando que el uso de técnicas de análisis y gestión de riesgos, así como el papel de terceros, es necesario para poder garantizar la seguridad del sistema de información de las PYMES.

Estudios centrados en la evaluación de riesgos [7–9] realizados sobre organizaciones en Europa y los EE.UU, revelan que las PYMES se caracterizan por la falta de la dedicación necesaria a la seguridad de las tecnologías de la información, debido principalmente a la asignación de responsabilidades a personal sin la debida formación. Asimismo, la mayoría de las organizaciones carecen de políticas de seguridad y sistemas de evaluación del riesgo, llegando al caso en que el 73% de los encuestados de PYMES del Reino Unido dijo realizar en su casa la evaluación de riesgos. Menos del 10% de los encuestados afirmó usar una herramienta de análisis de riesgos, y ninguno utilizó una guía de referencia como podía ser la ISO/IEC17799 [10]. Esto plantea dudas sobre la manera exhaustiva o eficaz en que pueden haberse realizado dichos análisis.

Como tal, una de las cuestiones derivadas de las conclusiones es la necesidad de obtener nuevas metodologías y modelos de análisis y gestión del riesgo que se adapten a las características especiales de las PYMES [11], con el objetivo de eliminar (o al menos reducir) los inconvenientes y ayudar a estas compañías a evaluar los riesgos a los que sus activos están expuestos y a establecer los controles de seguridad adecuados.

Por lo tanto, y considerando que las PYMES representan una gran mayoría de empresas tanto a nivel nacional como internacional y son muy importantes para el tejido empresarial de cualquier país, [12] creemos que avanzar en la investigación para mejorar los procesos de análisis y gestión del riesgo para este tipo de empresas puede generar importantes aportaciones. Esto puede contribuir a mejorar no sólo la seguridad de las PYMES, sino también su nivel de competitividad. Por este motivo, a los largo de los últimos años hemos trabajado en elaborar un proceso simplificado que permita analizar y gestionar el riesgo de seguridad en las PYMES [13, 14] , y además hemos construido una herramienta que automatiza completamente este proceso [15] , y lo hemos aplicado en casos reales [16], lo que nos ha permitido validar tanto la metodología como la herramienta.

El artículo continúa en la Sección II, describiendo brevemente las metodologías y modelos existentes para el análisis y la gestión del riesgo de la seguridad y su tendencia actual. En la Sección III se introduce brevemente nuestra propuesta de metodología para el análisis y la gestión del riesgo de la seguridad orientada hacia las PYMES. Finalmente, en la

Sección IV concluimos indicando cuál será el trabajo que desarrollaremos en el futuro.

II. Related Work

Con el propósito de reducir las carencias mostradas en el apartado anterior con respecto a la gestión de la seguridad en la PYMES, ha aparecido un gran número de procesos, marcos de trabajo y métodos para la gestión del riesgo cuya necesidad de uso para proteger de forma eficaz los activos de una compañía está siendo cada vez más reconocida y considerada por las organizaciones, pero que no terminan de tener éxito en el caso de las PYMES.

A pesar de ello, la gestión de la seguridad no puede limitarse al análisis y la gestión del riesgo [17], sino que además de identificar y eliminar riesgos el proceso se ha de realizar de manera eficiente, obteniendo la compañía grandes ahorros de costes como consecuencia directa de una mejor gestión de la seguridad [18]. Gracias al análisis de riesgos se podrán identificar los activos y conocer el nivel de seguridad que se debe aplicar.

Los estándares de gestión de la seguridad más destacados han incorporado procesos para el análisis y la gestión del riesgo, pero estos se han mostrado difíciles de aplicar en el caso de las PYMES, ya que requieren una gran inversión y son difíciles de gestionar [19]. Entre las principales propuestas para el análisis y gestión del riesgo podemos destacar MAGERIT [20], OCTAVE [21]] o CRAMM [22].

Por otro lado, algunos de los principales estándares de gestión de la seguridad han intentando incorporar dentro de sus procesos el análisis y la gestión del riesgo:

- ISO/IEC27005 [23]: Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC27001 [24] y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.
- ISO/IEC21827/SSECMM [25]: El modelo de capacidad y madurez en la ingeniería de seguridad de sistemas describe las características esenciales de los procesos que deben existir en una organización para asegurar una buena seguridad en los sistemas, incluyendo en las fases previas un proceso orientado al riesgo, con 4 subprocesos: SSE-PA02 (Determinar el impacto), SSE-PA03 (Identificar los riesgos de seguridad), SSE-PA04 (Identificar las amenazas), SSE-PA05 (Identificar las vulnerabilidades).
- COBIT: Es una metodología para el adecuado control de los proyectos de tecnología, los flujos de información y los riesgos que implica la falta de controles adecuados. Incluye un proceso orientado a evaluar los riesgos, en el dominio PO9. Este proceso se centra principalmente en los criterios de confidencialidad, integridad y disponibilidad, y de forma secundaria en criterios de efectividad, eficiencia, cumplimiento y confiabilidad. Por último, este proceso involucra a diversos perfiles (RRHH, Sistemas de Información, Tecnología, Instalaciones y Datos) involucrados en el sistema de información.

Por otro lado, existe un pequeño conjunto de herramientas de análisis de riesgos. Actualmente las más utilizadas son PILAR y EAR, basadas en Magerit v2 [20]. Otras herramientas utilizadas son la propuesta por ENISA, que incluye un sistema de comparativas, OCTAVES y Octave Automated Tool, que implementan la metodología de evaluación de riesgos OCTAVE [21], CRAMM y COBRA.

El principal problema de estos procesos y herramientas es su complejidad para aplicarlos en el caso de las PYMES, ya que han sido concebidos para grandes empresas [26]. Se justifica en repetidas ocasiones [27, 28] que la aplicación de este tipo de procesos para las PYMES es difícil y costosa. Además, las organizaciones, incluso las grandes, tienden más a adoptar grupos de procesos relacionados como un conjunto que a tratar los procesos de forma independiente [29].

Por lo tanto, y como conclusión de este apartado, se puede decir que es pertinente y oportuno abordar el problema de desarrollar un nuevo proceso para el análisis y gestión del riesgo de la seguridad para los sistemas de información en las PYMES, así como una herramienta que soporte este proceso, tomando como base la problemática a que este tipo de compañías se enfrenta y que ha llevado a continuos fracasos [30] en los intentos de implantación de un SGSI en este tipo de empresas.

III. Gestión del Riesgo de los Activos en las PYMES

Para solucionar los problemas detectados en el análisis y gestión del riesgo a la hora de aplicarlo en las PYMES, se ha desarrollado un nuevo proceso orientado a gestionar el riesgo en este tipo de compañías denominado ARM-PYME, con dos premisas básicas: i) orientado a las PYMES; y ii) enfocado a reducir los costes de generación y mantenimiento del proceso de análisis y gestión del riesgo.

Este proceso se ha obtenido mediante la aplicación del método de investigación en acción [31] y se ha enmarcado dentro de la metodología (MSM2-PYME) [32] que acomete todos los aspectos relacionados con la gestión de la seguridad.

Dentro de la metodología, el proceso que se encarga del análisis y la gestión del riesgo esta formado por dos actividades:

- Actividad I: Se establece una estructura de relaciones entre los diferentes elementos involucrados en el análisis del riesgo y los controles necesarios para gestionar la seguridad. Estas relaciones se establecen mediante el conocimiento adquirido en las diferentes implantaciones, que es almacenado en una estructura denominada esquema para ser reutilizado con posterioridad, reduciendo los costes de generación de este proceso.
- Actividad II: Mediante la selección del esquema más adecuado y la identificación de un pequeño conjunto de los principales activos se obtiene un detallado mapa de la situación actual (análisis del riesgo) y un plan de recomendaciones de cómo mejorarlo (gestión del riesgo).

Para entender correctamente el proceso es importante conocer el concepto de Esquema. Se trata de una estructura formada por los principales elementos de un SGSI y las relaciones que se pueden establecer entre ellos, mediante el Know-How adquirido en diferentes implantaciones. Esta estructura puede ser reutilizada por un conjunto de compañías con características comunes (mismo sector y tamaño) a partir del conocimiento adquirido con la implantación de la metodología MSM2PYME y posteriores refinamientos.

Este apartado se divide en dos subapartados, que se corresponden con las dos actividades del proceso.

A. ARM-PYME Actividad 1: Análisis de riesgos como parte de un Esquema.

El principal objetivo de esta actividad es seleccionar los elementos necesarios para poder realizar, en actividades posteriores de la metodología, un análisis de riesgos básico y de bajo coste (que se adapte a los requerimientos de las PYMES) sobre los activos que componen el sistema de información de la compañía.

Esta actividad está basada en las conclusiones obtenidas durante la aplicación del método de investigación-acción [31] a diferentes casos de estudio, las cuales han permitido determinar que los elementos que participan en un análisis de riesgos y sus relaciones tienen un alto grado de coincidencia cuando se aplican en PYMES que tienen características parecidas (mismo sector y mismo tamaño), por lo que se pueden establecer dichas relaciones a priori eliminando el coste de tener que analizarlas una por una mediante una labor de consultoría en cada caso. Aún cuando existan diferencias entre unas y otras, éstas son irrelevantes con respecto a la configuración final del SGSI obtenido para el caso de las PYMES, dado que este tipo de empresas priorizan el coste a obtener un resultado con un alto grado de precisión.

En la Figura 1 se puede ver el esquema básico de entradas, tareas y salidas que componen esta actividad:

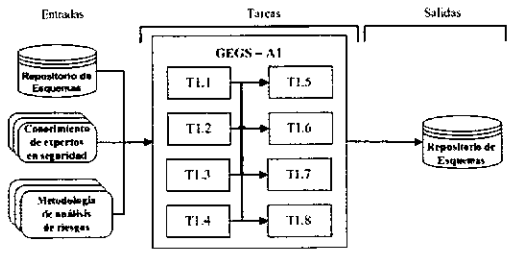


Fig. 1. Esquema simplificado a nivel de tarea de la actividad A1.

- *Entradas:* Como entrada se recibirá el conocimiento del grupo de expertos del dominio de seguridad (EGD) obtenido durante el proceso de implantación de SGSIs, así como un conjunto de controles para la gestión de seguridad que se encuentran almacenados en el repositorio de esquemas y un conjunto de elementos necesarios para elaboración del análisis de riesgos.
- *Tareas:* El subproceso estará formado por ocho tareas que se analizarán en detalle posteriormente.
- *Salidas:* La salida producida por este subproceso consistirá en un subconjunto de los elementos de entrada y las relaciones establecidas entre ellos, los cuáles se almacenarán en el repositorio de esquemas y que se corresponden con la tercera parte de los elementos de los que se compondrá el esquema que se quiere generar.

A continuación, se analizarán las diferentes tareas del proceso que involucran y manipulan los elementos del análisis de riesgos.

- *Tarea T1.1 Selección de tipos de activos:* Se ocupa de seleccionar el conjunto de tipos de activos que formarán parte del esquema que se está construyendo. Los tipos de activos se utilizarán posteriormente para diversas tareas: i) agrupar los activos del sistema de información; ii) se relacionarán con otros elementos del análisis de riesgos para facilitar la automatización del mismo.
- *Tarea T1.2 Selección de amenazas:* Se ocupa de seleccionar el conjunto de amenazas que formarán parte del esquema que se está construyendo. Una amenaza se define como un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos [20]. Estas amenazas se relacionarán en tareas posteriores con otros elementos del análisis de riesgos, con el objetivo de poder automatizar y reducir los costes a la hora de evaluar el riesgo al que están sometidos los activos de un sistema de información.
- *Tarea T1.3 Selección de vulnerabilidades:* Se ocupa de seleccionar el conjunto de vulnerabilidades que formarán parte del esquema que se está construyendo. Una vulnerabilidad se define como una debilidad o falta de control que permitiría o facilitaría que una amenaza actuase contra un activo del sistema que presenta la citada debilidad [20]. Estas vulnerabilidades se relacionarán en tareas posteriores con otros elementos del análisis de riesgos, con el objetivo de poder automatizar y reducir los costes a la hora de evaluar el riesgo al que están sometidos los activos de un sistema de información.
- *Tarea T1.4 Selección de criterios de riesgo:* Se ocupa de seleccionar el conjunto de criterios de riesgo que formarán parte del esquema que se está construyendo. Los criterios de riesgo se definen como aquellos criterios que permiten estimar el grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. Estos criterios de riesgo se relacionarán en tareas posteriores con otros elementos del análisis de riesgos, con el objetivo de poder automatizar y reducir los costes a la hora de evaluar el riesgo.
- *Tarea T1.5 Establecer relaciones entre tipos de activos y vulnerabilidades:* Se ocupa de establecer las relaciones existentes entre los elementos que componen el conjunto de tipos de activos y los elementos que componen el con-

junto de vulnerabilidades para un esquema determinado.

- *Tarea T1.6 Establecer relaciones entre amenazas y vulnerabilidades:* Se ocupa de establecer las relaciones existentes entre los elementos que componen el conjunto de amenazas y los elementos que componen el conjunto de vulnerabilidades para un esquema determinado.
- *Tarea T1.7 Establecer relaciones entre amenazas y controles:* Se ocupa de establecer las relaciones existentes entre los elementos que componen el conjunto de amenazas y los elementos que componen el conjunto de controles para un esquema determinado.
- *Tarea T1.8 Establecer relaciones entre tipos de activos, vulnerabilidades y criterios de riesgo:* Se ocupa de establecer las relaciones existentes entre los elementos que componen el conjunto de tipos de activos, los elementos que componen el conjunto de vulnerabilidades y los elementos que componen el conjunto de criterios de riesgo para un esquema determinado.

Las asociaciones de las tareas T1.5-8 se establecen por el grupo de expertos del dominio (EGD) en base al conocimiento adquirido en diferentes implantaciones del SGSI.

B. AGR-PYME Actividad 2: Aplicación del análisis de riesgos.

El principal objetivo de esta actividad es establecer una evaluación de los riesgos a los que se encuentran sometidos los principales activos del sistema de información de la compañía sobre la que se quiere implantar el SGSI, así como proponer un plan al responsable de seguridad (Cu/RS) para gestionar los riesgos de la forma más eficiente posible.

En la Figura 2 se puede ver el esquema básico de entradas, tareas y salidas que componen esta actividad:

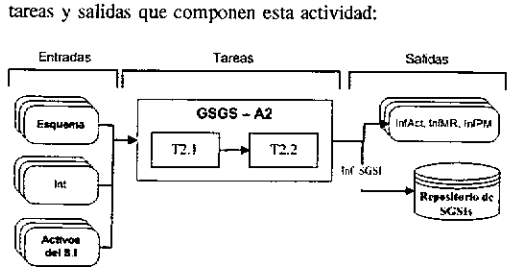


Fig. 2. Esquema simplificado a nivel de tarea de la actividad A2.

- *Entradas:* Como entrada se recibirá: i) un esquema de los existentes en el repositorio de esquemas, que será seleccionado por el consultor de seguridad (SCo) en base a las características de la compañía (sector y tamaño de la misma), del que se obtendrán los elementos necesarios para la realización del análisis de riesgos; ii) el interlocutor (Int) válido para la compañía, que se encargará de definir los activos; iii) un conjunto de activos del sistema de información, lo más generalistas posible (grano grueso).
- *Tareas:* El subproceso estará formado por dos tareas que se analizarán en detalle posteriormente.
- *Salidas:* La salida producida por este subproceso consistirá en una serie de entregables (informe de activos del sistema de información, matriz de riesgos a los que están sometidos los activos del sistema de información y plan de mejora recomendado por la metodología para afrontar las mejoras en la gestión de la seguridad del SGSI) para que el consultor de seguridad (SCo) pueda analizarlos.

El desarrollo de esta actividad está basado en la propuesta de Stephenson [33], que se centra en la sinergia entre la prueba técnica y el análisis de riesgos tomando como referencia la ISO/IEC 27002 [34] y en la metodología de análisis de riesgos Magerit v2 [20]. Estas metodologías suelen producir rechazo en el caso de las PYMES debido a que las perciben como demasiado complejas, a que requieren un enorme compromiso por parte de los miembros de la compañía y a que los costes asociados a los mismos no son aceptados por estas compañías. Por ello, la metodología MSM2PYME simplifica el proceso de evaluación del riesgo para adecuarlo a las PYMES.

Las principales bases sobre las que se define esta actividad son: flexibilidad, simplicidad y eficiencia en costes (humanos y temporales). Se trata, pues, de una actividad que pretende identificar con el menor coste posible los activos de la compañía y los riesgos asociados, usando para ello los resultados generados en las actividades anteriores y unos sencillos algoritmos.

La parte de análisis de riesgos de la metodología desarrollada toma algunos aspectos de Magerit v2 [20] y algunos aspectos de los análisis de riesgos clásicos, pero en todo momento tiende a la simplificación.

Para que esta actividad funcione de forma coherente se deben tener en cuenta las condiciones especiales de las PYMES, en las que los usuarios no suelen tener ni el tiempo ni los conocimientos adecuados para aplicar de forma eficiente metodologías de análisis de riesgos, ni para determinar de forma adecuada los activos de los sistemas de información.

Al igual que en la actividad anterior, cuando se trata de PYMES no se busca la opción óptima sino una opción razonablemente buena que permita grandes reducciones de tiempos a la hora de obtener el resultado.

Las tareas de esta actividad se apoyan principalmente en los datos que componen el esquema seleccionado, generado durante la actividad A1, y en una lista de controles de seguridad.

A continuación mostramos en detalle las tareas que componen la actividad:

- *Tarea T2.1 Identificación de activos:* El objetivo de esta tarea es obtener un conjunto de los activos que componen el sistema de información de la empresa. Los activos definidos son el objetivo principal hacia el que se enfoca el SGSI, ya que son los elementos que se pretenden proteger.
  Una de las diferencias principales que presenta el método para la evaluación del riesgo presentado en la metodología es que se busca que los activos sean lo más generales posible (grano grueso), frente a [20], que intenta identificarlos de forma clara y precisa (grano fino). En las PYMES se debe intentar definir un conjunto muy pequeño y básico de activos, ya que su sistema de información no permite la protección discriminada de activos de baja atomicidad ni puede soportar el coste de gestión de los mismos. Por lo tanto, en esta tarea se buscarán activos generales que se puedan valorar de forma sencilla tanto desde el punto de vista cuantitativo como cualitativo.
  En esta tarea el consultor de seguridad (SCo) deberá ayudar el interlocutor (Int) a identificar el conjunto de activos de valor que componen el S.I. de la compañía.
- *Tarea T2.2 Generación de matriz de riesgos y plan de mejora:* El objetivo de esta tarea es realizar una evaluación de los riesgos a los que están sometidos los activos de la empresa definidos en la tarea T2.1.
  Esta tarea requiere de los datos generados durante la actividad A1 y de los activos identificados en la tarea T2.1 para generar una matriz riesgos que muestre de forma detallada los riesgos a los que está sometido cada activo y un plan de mejora que determine cómo acometer estos riesgos.
  El plan de mejora se soporta sobre los resultados obtenidos de la matriz de riesgos. La matriz de riesgos y el plan de mejora son utilizados por el consultor de seguridad (SCo) para determinar y analizar medidas adicionales y urgentes que deban tomarse en la compañía para mitigar riesgos elevados sobre los activos de información de la misma.
  El primer objetivo de esta tarea es generar una matriz de riesgo que nos permita conocer los riesgos a los que está sometido cada activo de la compañía en cada nivel de madurez y para cada elemento del análisis de riesgos (amenazas, vulnerabilidades y criterios de riesgo). El resultado será una tabla con las siguientes columnas: i) Nivel de Madurez; ii) Nombre y descripción del activo; iii) Coste del activo; iv) Valor estratégico; v) Tipo de activo; vi) Amenaza; vii) Vulnerabilidad; viii) Criterios de riesgo; ix) Nivel de la amenaza (LT); x) Nivel de probabilidad (P); xi) Nivel de riesgo (RL); xii) Nivel de control o cobertura.

El valor obtenido en el nivel de riesgo (RL) se gestionará según la Tabla I y se moverá en un rango comprendido entre 1 (menor riesgo) y 7 (mayor riesgo). Se ha determinado que el nivel del riesgo residual (RRL), es decir, el que tiene actualmente la compañía, nunca debe ser superior al nivel de riesgo aceptable (ARL), que es al que debe tender la compañía. Para el proceso AGR-PYME se ha considerado que el ARL debe ser menor o igual a 3. Si el RL fuera superior al ARL, se procede a la selección de salvaguardas para la reducción del riesgo, realizando el proceso de forma recursiva hasta que el nivel de riesgo de la compañía sea el adecuado.

Para poder obtener de una forma sencilla el riesgo al que está sometido cada activo y el nivel de cobertura de cada

Tabla I
CUADRO PARA DETERMINAR EL NIVEL DE RIESGO.

ARL=<3	LT	Alto			Medio			Bajo		
								A		B
Valor	1	1	2	3	2	3	4	3	4	5
activo	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7

control se utilizará el algoritmo de Matriz de Riesgos (RMa).

Una vez que se ha obtenido la matriz de riesgos, se utilizará - junto con la información generada en las tareas anteriores - para obtener el plan de mejora, mediante la aplicación del algoritmo del Plan de Mejora (aPM). Este algoritmo funciona de forma recursiva, determinando el activo de mayor riesgo en el menor nivel de madurez, y aplicando el control que permita mejorarlo con el menor coste, para posteriormente recalcular todo el proceso y seleccionar el siguiente mejor, hasta llegar al nivel de gestión de seguridad óptimo.

IV. CONCLUSIONES

En este artículo se ha presentado la propuesta de un proceso para realizar el análisis y gestión del riesgo en las PYMES denominado ARM-PYME, que permite soportar los resultados generados durante la investigación y que cumple con los objetivos perseguidos.

Se ha definido cómo se puede utilizar este proceso y las mejoras que ofrece con respecto a otros modelos que afrontan el problema de una forma más precisa y detallada, pero también más costosa, lo que no los hace válidos para el caso de las PYMES.

Las características ofrecidas por el proceso y su orientación a las PYMES han sido muy bien recibidas, y su aplicación está resultando muy positiva ya que permite a este tipo de empresas realizar una adecuada gestión del riesgo al que están sometidos los activos de su sistema de información. Además, con este proceso se obtienen resultados a corto plazo y se reducen los costes que supone el uso de otros procesos, consiguiendo un mayor grado de satisfacción de la empresa.

El proceso ARM-PYME cumple con los objetivos propuestos, así como con los principios que según la Organización para la Cooperación y el Desarrollo Económico (OECD) [35] debe seguir todo proceso de evaluación del riesgo, según la cuál el sistema debe tener la capacidad de autoevaluar su riesgo de forma continuada en el tiempo, proponiendo medidas.

Finalmente, se considera que el trabajo realizado debe ser ampliado con nuevas especificaciones, nuevos esquemas, mejorando los algoritmos de análisis y gestión del riesgo de forma que puedan ofrecer planes más detallados y profundizando en el proceso con nuevos casos de estudio.

La mayor parte de las futuras mejoras del proceso se están orientando a mejorar la precisión del mismo, pero siempre respetando el principio de coste de recursos, es decir, se busca mejorar el proceso sin incurrir en costes de generación y mantenimiento del análisis de riesgos.

AGRADECIMIENTOS

Esta investigación es parte de los proyectos BUSINESS (PET2008-0136), concedido por el Ministerio de Ciencia e Innovación de España, SEGMENT (HITO-09-138) financiado por la Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha, SISTEMAS (PII2I09-0150-3135) financiado por la Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha MEDUSAS (IDI-20090557) financiado por el Centro para el Desarrollo Tecnológico Industrial. Ministerio de Ciencia e Innovación (CDTI).

REFERENCIAS

[1] Wiander, T. Implementing the ISO/IEC 17799 standard in practice: experiences on audit phases. in AISC '08: Proceedings of the sixth Australasian conference on Information security. 2008. Wollongong, Australia.
[2] Wiander, T. and J. Holappa, Theoretical Framework of ISO 17799 Compliant, Information Security Management System Using Novel ASD Method., in Technical Report, V.T.R.C.o. Finland, Editor. 2006.
[3] Dhillon, G. and J. Backhouse, Information System Security Management in the New Millennium. Communications of the ACM, 2000. 43(7): p. 125-128.
[4] Volonino, L. and S. Robinson. Principles and Practice of Information Security. in 1 edition, Anderson, Natalie E. 2004. New Jersey, EEUU.
[5] Michalson, L., Information security and the law: threats and how to manage them. Convergence, 2003. 4(3): p. 34-38.
[6] Spinellis, D. and D. Gritzalis. Information Security Best Practise Dissemination: The ISA-EUNET Approach. in WISE 1:First World Conference on Information Security Education. 1999.
[7] Dimopoulos, V., et al. Approaches to IT Security in Small and Medium Enterprises. in 2nd Australian Information Security Management Conference, Securing the Future. 2004b. Perth, Western Australia: 73-82.
[8] Holappa, J. and T. Wiander, Practical Implementation of ISO 17799. Compliant Information Security Management System Using Novel ASD Method., in Technical Report, V.T.R.C.o. Finland, Editor. 2006.
[9] Livonen, L. Information Security Management in Finnish SMEs. in 5th European Conference on Information Warfare and Security National Defence College. 2006. Helsinki, Finlan: 1-2 June 2006.
[10] ISO/IEC17799, ISO/IEC 17799, Information Technology - Security Techniques - Code of practice for information security management. 2000.
[11] Taylor, M. and A. Murphy, SMEs and eBusiness. Small Business and Enterprise Development, 2004. 11(3): p. 280-289.
[12] Tawilch, A., J. Hilton, and S. McIntosh, Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach, in ISSE/SECURE 2007 Securing Electronic Business Processes, Vieweg. Editor. 2007. p. 331-339.
[13] Sánchez, L.E., et al. Security Management in corporative IT systems using maturity models, taking as base ISO/IEC 17799. in International Symposium on Frontiers in Availability, Reliability and Security (FARES06) in conjunction with ARES. 2006. Viena (Austria).
[14] Sánchez, L.E., et al. Developing a model and a tool to manage the information security in Small and Medium Enterprises. in International Conference on Security and Cryptography (SECRYPT07). 2007a. Barcelona, Spain.: Junio.
[15] Sánchez, L.E., et al. SCMM-TOOL: Tool for computer automation of the Information Security Management Systems. in 2nd International conference on Software and Data Technologies (ICSOFT07). . 2007c. Barcelona-España Septiembre.
[16] Sánchez, L.E., et al. Practical Application of a Security Management Maturity Model for SMEs Based on Predefined Schemas. in International Conference on Security and Cryptography (SECRYPT08). 2008. PortoPortugal.
[17] Siegel, C.A., T.R. Sagalow, and P. Serritella, Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security. Security Management Practices, 2002. sept/oct: p. 33-49.
[18] Garigue, R. and M. Stefaniu, Information Security Governance Reporting. Information Systems Security, 2003. sept/oct: p. 36-40.
[19] Bohemer, W. Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001. in SECURWARE '08: Proceedings of the 2008 Second International Conference on Emerging Security Information, Systems and Technologies. 2008.
[20] MageritV2, Methodology for Information Systems Risk Analysis and Management (MAGERIT version 2). 2006, Ministerio de Administraciones Públicas (Spain).
[21] Alberts, C.J. and A.J. Dorofee, Managing Information Security Risks: The OCTAVE Approach., ed. A.-W.P. Co. 2002.
[22] CRAMMv5.0, CRAMM v5.0, CCTA Risk Analysis and Management Method. 2003.
[23] ISO/IEC27005, ISO/IEC 27005, Information Technology - Security Techniques - Information Security Risk Management Standard (under development). 2008.
[24] ISO/IEC27001, ISO/IEC 27001, Information Technology - Security Techniques Information security management systemys - Requirements. 2005.
[25] ISO/IEC21827, ISO/IEC 21827:2002, Information technology - Systems Security Engineering - Capability Maturity Model (SSE-CMM). 2002, ISO/IEC. p. 123.
[26] Batista, J. and A. Figueiredo, SPI in very small team: a case with CMM. Software Process Improvement and Practice, 2000. 5(4): p. 243-250.
[27] Hareton, L. and Y. Terence, A Process Framework for Small Projects. Software Process Improvement and Practice, 2001. 6: p. 67-83.
[28] Tuffley, A., B. Grove, and M. G, SPICE For Small Organisations. Software Process Improvement and Practice, 2004. 9: p. 23-31.
[29] [29] Mekelburg, D., Sustaining Best Practices: How Real-World Software Organizations Improve Quality Processes. Software Quality Professional, 2005. 7(3): p. 4-13.
[30] Fomin, V.V. and H. Vries. ISO/IEC 27001 Information Systems Security Management Standard: Exploring the reasons for low adoption. in EuroMOT 2008 - The Third European Conference on Management of Technology. 2008. Nice, France.
[31] Kock, N., The three threats of action research: a discussion of methodological antidotes in the context of an information systems study. , in Decision Support Systems. 2004. p. 265-286.
[32] Sánchez, L.E., et al. MMISS-SME Practical Development: Maturity Model for Information Systems Security Management in SMEs. in 9th International Conference on Enterprise Information Systems (WOSIS07). 2007b. Funchal, Madeira (Portugal). June.
[33] Stephenson, P., Forensic Análisis of Risks in Enterprise Systems. Law, Investigation and Ethics, 2004. sep/oct: p. 20-21.
[34] ISO/IEC27002, ISO/IEC 27002, Information Technology - Security Techniques - The international standard Code of Practice for Information Security Management. 2007.
[35] OECD, OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security., O.f.E.C.-o.a.D. (OECD). Editor. 2002: Paris.

An operational research approach to feature selection for network-based intrusion detection

Hai Nguyen
NISlab, Department of Computer Science
and Media Technology, Gjøvik University College
Email: hai.nguyen@hig.no

Slobodan Petrović
NISlab, Department of Computer Science
and Media Technology, Gjøvik University College
Email: slobodan.petrovic@hig.no

***Abstract*—The goal of the feature selection process in network intrusion detection is to determine the minimal set of network traffic features that ensures accurate intrusion detection in the most efficient way. Obtaining automatically a good set of such features is a great research challenge. The problem is in a huge cardinality of the power set of the full feature set. In this paper, we transform the correlation feature selection (CFS) problem into a polynomial mixed 0-1 fractional programming problem and by solving that problem we get the globally optimal solution of the CFS problem. We describe a sequence of transformations of the original optimization problem into a program with the number of constraints that is linear in the number of full set features. Our feature selection algorithm was compared experimentally with the best-first-CFS and the genetic-algorithm-CFS methods regarding the feature selection capabilities. The classification accuracy obtained after the feature selection by means of the C4.5 and the BayesNet machines over the KDD CUP99 IDS benchmarking data set was also tested. Experiments show that our feature selection method outperforms the best first and the genetic algorithm search strategies by removing much more redundant features and still keeping the classification accuracies or even getting better performances.**

I. INTRODUCTION

Network-based intrusion detection systems (IDS) gather and analyze information from networks in order to identify suspicious activities and generate alerts for an operator. Such a task is often analyzed as a pattern classification problem - an IDS has to tell normal from abnormal activities in networks. The theoretical models of IDS (see for example [4], [6]) usually include the representation algorithm (for representing incoming data in the space of selected features) and the classification algorithm (for mapping the feature vector representation of the incoming data to elements of a certain set of values, e.g. normal or abnormal etc.) Some IDS models, like those presented in [6], also include the feature selection algorithm, which determines the features to be used by the representation algorithm. Even if the feature selection algorithm is not included in the model directly, it is always assumed that such an algorithm is run before the very intrusion detection process.

The goal of the feature selection algorithm is to determine the most relevant features of incoming traffic, whose monitoring ensures reliable detection of abnormal behaviour. Since the effectiveness of the classification algorithm heavily depends on the number of features, it is of interest to minimize the cardinality of the set of selected features without dropping potential indicators of abnormal behaviour. Obviously, determining a good set of features is not an easy task. The most of the work in practice is still done manually and the feature selection process depends too much on expert knowledge. Automatic feature selection for intrusion detection remains therefore a great research challenge.

In this paper, we approach the problem of feature selection for intrusion detection from the operational research point of view. We propose an automatic feature selection procedure based on so-called filter method [7], [10] used in machine learning. The filter method directly considers statistical characteristics of the data set, such as correlation between a feature and a class or inter-correlation between features, without involving any learning algorithm. We focus on one of the most important filter methods, the Correlation Feature Selection (CFS) measure proposed by M. Hall [8]. The CFS measure is combined with some search strategies, such as brute force, best first search or genetic algorithm, in order to find the most relevant subset of features. The brute force method can only be applied when the number of features is small. In other cases, a more intelligent optimization algorithm in the feature selection process is needed. With the best first search or the genetic algorithm, we can deal with high dimensional data sets, but these methods usually give locally optimal solutions. To get the globally optimal feature set, we formulate the problem of feature selection by representing the CFS measure as a polynomial mixed 0 - 1 fractional programming (P01FP) problem. We improve the Changs method [1], [2] in order to equivalently reduce this P01FP to a mixed 0 - 1 linear programming (M01LP) problem [1]. Finally, we propose to use the branch-and-bound algorithm to solve this M01LP, whose optimal solution is also the globally optimal subset of relevant features by means of the CFS measure.

Any feature selection algorithm selects relevant traffic features based on labelled data. We used the KDD CUP99 [9] data set for this purpose. The full feature set assigned to this data set consists of 41 features. For evaluating the performance of our feature selection approach, two available feature selection methods based on the CFS measure were implemented [3]. The first one was the best-first-CFS method using the best-first search strategy to find the locally optimal subset of features by means of the CFS measure. The second one