VIII Jornadas de Ciencia e Ingeniería de Servicios

Sistedes 2012

JISBD | PROLE | ACTAS JCIS

Sistedes
Sociedad de Ingeniería de Software y Tecnologías de Desarrollo de Software

IN LUMINE SAPIENTIA · UNIVERSITAS ALMERIENSIS

Almería, 17 al 19 de Septiembre

Editores: Mª Valeria de Castro | José Manuel Gómez | Luis Iribarne

M.V. de Castro, J.M. Gómez, L. Iribarne (Eds.): Actas de las "VIII Jornadas de Ciencia e Ingeniería de Servicios (JCIS'2012)", Jornadas Sistedes'2012, Almería 17-19 sept. 2012, Universidad de Almería.

JCIS 2012

VIII Jornadas de Ciencia e Ingeniería de Servicios (JCIS)

Almería, 17 al 19 de Septiembre de 2012

Editores:
Ma. Valeria de Castro
José Manuel Gómez
Luis Iribarne

Actas de las "*VIII Jornadas de Ciencia e Ingeniería de Servicios (JCIS)*"
Almería, 17 al 19 de Septiembre de 2012
Editores: Ma. Valeria de Castro, José Manuel Gómez, Luis Iribarne
http://sistedes2012.ual.es
http://www.sistedes.es

ISBN: 978-84-15487-26-5
Depósito Legal: AL 672-2012

Prólogo

El presente volumen contiene los artículos seleccionados para presentación en las *VIII Jornadas de Ciencias e Ingeniería de Servicios* (JCIS 2012) celebrado en Septiembre de 2012 en Almería, España.

El principal objetivo de las Jornadas es proporcionar un foro de discusión e intercambio de conocimiento y experiencias en el ámbito de la Ciencia de Servicios. El interés no sólo se centra en los nuevos avances científicos, sino también en las tecnologías existentes en torno a la computación orientada a servicios y los procesos de negocio, las nuevas prácticas de ingeniería de servicios y las lecciones aprendidas por medio de experiencias reales. Las JCIS, que celebran este año su octava edición, son el resultado de la integración de las Jornadas Científico-Técnicas en Servicios Web y SOA (JSWEB) y el Taller sobre Procesos de Negocio e Ingeniería de Servicios (PNIS). Seguir contando después de ocho años, y en el contexto de crisis en el que nos encontramos actualmente, con un foro de encuentro que nos permita intercambiar conocimiento y experiencias entre grupos de investigación de distintas Universidades españolas y profesionales de la Administración Publica y de la Industria, es sin duda un triunfo de nuestra comunidad que debemos y queremos destacar.

En esta edición se han recibido 22 contribuciones para su revisión, de las cuales 4 eran artículos publicados ya previamente en congresos y revistas de reconocido prestigio. Todos las contribuciones fueron revisadas por, al menos, dos miembros del comité de programa. Como resultado de este proceso de revisión, se seleccionaron 14 trabajos largos para su presentación en las jornadas y otros 3 como trabajos cortos. Los trabajos han sido organizados en seis sesiones temáticas dobles que se presentarán a lo largo de dos días de jornadas de los siguientes temas: “SOA, Tecnologías para Servicios Web y Aplicaciones”, “Ingeniería de Servicios” y “Procesos de Negocio”.

Nos gustaría agradecer a todos aquellos que de un modo u otro han contribuido a la organización de estas Jornadas. En primer lugar, a todos los autores de los artículos enviados a JCIS 2012, y a los miembros del Comité de Programa por su disponibilidad y dedicación a la hora realizar las revisiones. Agradecer además a nuestros colaboradores: SRII (Service Research & Innovation Institute), ATI, Novática, INES y la Red Científico-Tecnológica en Ciencias de los Servicios financiada por el Ministerio de Economía y Competitividad. Finalmente, agradecemos a la Sociedad de Ingeniería del Software y Tecnologías de Desarrollo del Software (SISTEDES) y a la organización por parte de los miembros de la Universidad de Almería. Conocemos la dificultad de la organización de este tipo de eventos, y máxime en la situación de crisis económica en la que nos encontramos, por lo que destacamos y agradecemos enormemente vuestro esfuerzo y dedicación en la realización de estas Jornadas.

Gracias a todos y esperamos que disfrutéis de las Jornadas y de vuestra estancia en Almería.

Almería, Septiembre 2012
Ma. Valeria de Castro y José Manuel Gómez
Presidentes del Comité científico

Prologo de la Organización

Las jornadas SISTEDES 2012 son un evento científico-técnico nacional de ingeniería y tecnologías del software que se celebra este año en la Universidad de Almería durante los días 17, 18 y 19 de Septiembre de 2012, organizado por el Grupo de Investigación de Informática Aplicada (TIC-211). Las Jornadas SISTEDES 2012 están compuestas por las XVII Jornadas de Ingeniería del Software y de Bases de Datos (JISBD'2012), las XII Jornadas sobre Programación y Lenguajes (PROLE'2012), y la VIII Jornadas de Ciencia e Ingeniería de Servicios (JCIS'2012). Durante tres días, la Universidad de Almería alberga una de las reuniones científico-técnicas de informática más importantes de España, donde se exponen los trabajos de investigación más relevantes del panorama nacional en ingeniería y tecnología del software. Estos trabajos están auspiciados por importantes proyectos de investigación de Ciencia y Tecnología financiados por el Gobierno de España y Gobiernos Regionales, y por proyectos internacionales y proyectos I+D+i privados. Estos encuentros propician el intercambio de ideas entre investigadores procedentes de la universidad y de la empresa, permitiendo la difusión de las investigaciones más recientes en ingeniería y tecnología del software. Como en ediciones anteriores, estas jornadas están auspiciadas por la Asociación de Ingeniería del Software y Tecnologías de Desarrollo de Software (SISTEDES).

Agradecemos a nuestras entidades colaboradoras, Ministerio de Economía y Competitividad (MINECO), Junta de Andalucía, Diputación Provincial de Almería, Ayuntamiento de Almería, Vicerrectorado de Investigación, Vicerrectorado de Tecnologías de la Información (VTIC), Enseñanza Virtual (EVA), Escuela Superior de Ingeniería (ESI/EPS), Almerimatik, ICESA, Parque Científico-Tecnológico de Almería (PITA), IEEE España, Colegio de Ingenieros Informática de Andalucía, Fundación Mediterránea, y a la Universidad de Almería por el soporte facilitado. Asimismo a D. Félix Faura, Director de la Agencia Nacional de Evaluación y Prospectiva (ANEP) de la Secretaría de Estado de I+D+i, Ministerio de Economía y Competitividad, a D. Juan José Moreno, Catedrático de la Universidad Politécnica de Madrid, presidente de la Sociedad de Ingeniería y Tecnologías del Software (SISTEDES), a D. Francisco Ruiz, Catedrático de la Universidad de Castilla-La Mancha, y a D. Miguel Toro, Catedrático de la Universidad de Sevilla, por su participación en la mesa redonda "*La investigación científica informática en España y el año Turing*"; a Armando Fox de la Universidad de Berkley (EEUU) y a Maribel Fernández del King's College London (Reino Unido), como conferenciantes principales de las jornadas, y a los presidentes de las tres jornadas por facilitar la confección de un programa de *Actividades Turing*. Especial agradecimiento a los voluntarios de las jornadas SISTEDES 2012, estudiantes del Grado de Ingeniería Informática y del Postgrado de Doctorado de Informática de la Universidad de Almería, y a todo el equipo del Comité de Organización que han hecho posible con su trabajo la celebración de una nueva edición de las jornadas JISBD'2012, PROLE'2012 y JCIS'2012 (jornadas SISTEDES 2012) en la Universidad de Almería.

Luis Iribarne
Presidente del Comité de Organización
@sistedes2012{JISBD;PROLE;JCIS}

Comité Científico

Presidentes del Comité Científico:

Ma. Valeria De Castro (Universidad Rey Juan Carlos)
José Manuel Gómez (ISOCO)

Coordinador de artículos ya publicados:

Marcos López Sanz (Universidad Rey Juan Carlos)

Miembros del Comité Científico:

Antonio Ruiz Cortés (Universidad de Sevilla)
Antonio Vallecillo (Universidad de Málaga)
Carlos Bobed (Universidad de Zaragoza)
Carlos Rodríguez Fernández (Universidad Complutense Madrid)
Diego López (Red Española de I+D, RedIRIS)
Daniel González Morales (Ag. Canaria de Inv., Innovación y Soc. de la Inf.)
Enrique Beltrán (Software AG)
Esperanza Marcos (Universidad Rey Juan Carlos)
Félix García (Universidad de Castilla-La Mancha)
Francisco Almeida Rodríguez (Universidad de La Laguna)
Francisco Javier Fabra (Universidad de Zaragoza)
Francisco Ruiz (Universidad de Castilla-La Mancha)
Guadalupe Ortiz Bellot (Universidad de Cádiz)
Jaime Cid (Oracle)
Jesús Arias Fisteus (Universidad Carlos III de Madrid)
Jesús Gorroñogoitia (Atos Origin)
Joan Pastor (Universitat Oberta de Catalunya)
Jordi Marco (Universidad Politécnica de Cataluña)
José Emilio Labra (Universidad de Oviedo)
José Hilario Canós (Universidad Politécnica de Valencia)
José M. López Cobo (Playence KG)
José Raúl Romero (Universidad de Córdoba)
Juan De Lara (Universidad Autónoma de Madrid)
Juan Hernández (Universidad de Extremadura
Juan José Moreno Navarro (Universidad Politécnica de Madrid)
Juan Manuel Murillo (Universidad Extremadura)
Juan Pavón (Universidad Complutense de Madrid)
Leire Bastida (Tecnalia)
Manuel Lama (Universidad de Santiago de Compostela)
Manuel Resinas (Universidad de Sevilla)
Marcos López Sanz (Universidad Rey Juan Carlos)
María del Carmen Penadés (Universidad Politécnica de Valencia)
María-Ribera Sancho (Universidad Politécnica de Cataluña)
Marta Patiño (Universidad Politécnica de Madrid)
Martín Álvarez Espinar (W3C Spain)
Mercedes Ruiz (Universidad de Cádiz)
Óscar Corcho (Universidad Politécnica de Madrid)
Pedro Alvarez (Universidad de Zaragoza)
Pere Botella (Universidad Politécnica de Cataluña)
Rafael Corchuelo (Universidad de Sevilla)
Santi Ristol (Atos Origin)
Silvia Acuña (Universidad Autónoma de Madrid)
Vicente Pelechano (Universidad Politécnica de Valencia)
Víctor Acinas (Inabensa)
Víctor Ayllón (Novayre)

Comité de Organización

Presidente:

Luis Iribarne (Universidad de Almería)

Miembros:

Alfonso Bosch (Universidad de Almería)
Antonio Corral (Universidad de Almería)
Diego Rodríguez (Universidad de Almería)
Elisa Álvarez, Fundación Mediterránea
Javier Criado (Universidad de Almería)
Jesús Almendros (Universidad de Almería)
Jesús Vallecillos (Universidad de Almería)
Joaquín Alonso (Universidad de Almería)
José Andrés Asensio (Universidad de Almería)
José Antonio Piedra (Universidad de Almería)
José Francisco Sobrino (Universidad de Almería)
Juan Francisco Inglés (Universidad Politécnica de Cartagena)
Nicolás Padilla (Universidad de Almería)
Rosa Ayala (Universidad de Almería)
Saturnino Leguizamón (Universidad Tecnológica Nacional, Argentina)

Colaboradores JCIS

Índice de Contenidos

Chala Invitada

"Crossing the Software Education Chasm using Software-as-a-Service and Cloud Computing", Armando Fox (Univ. Berkeley, USA). *183*

Sesión 1: SOA, Tecnologías para Servicios Web y Aplicaciones
Chair: Dr. José Manuel Gómez

Ruediger Gad, Juan Boubeta-Puig, Martin Kappes and Inmaculada Medina-Bulo. *Leveraging EDA and CEP for Integrating Low-level Network Analysis Methods into Modern, Distributed IT Architectures*..... *13-26*

Sergio Hernández, Javier Fabra, Pedro Álvarez and Joaquín Ezpeleta. *Una solución SOA para ejecutar workflows científicos en entornos Grid heterogéneos* *27-40*

Ricardo Jiménez, Marta Patino and Iván Brondino. *CumuloNimbo: Una Plataforma como Servicio con Procesamiento Transaccional Altamente Escalable*. *41-47*

Sesión 2: Ingeniería de Servicios
Chair: Dr. Pedro Alvarez

Antonio García and Inmaculada Medina. *Un Método de Generación de Pruebas de Rendimiento para Múltiples Tecnologías desde Modelos UML con Anotaciones MARTE* *51-64*

Juan Carlos Castillo Cano, Francisco Almeida, Vicente Blanco and María Carmen Ramírez Castillejo. *Plataforma de computación genérica basada en servicios web para problemas de conteo de células* *65-76*

Jorge Moratalla and Esperanza Marcos. *Definición y Aplicación de un proceso de Modernización y Evolución al Sistema de Gestión de Nombres de Dominios ".es"* *77-80*

Miguel A. González-Serrano, Diana Perez-Marin and Miren Idoia Alarcón. *Clasificación de los Servicios Web de Negocio Corporativos basada en la Funcionalidad Horizontal de las Organizaciones* *81-87*

Sesión 3: Procesos de Negocio
Chair: Dr. Inmaculada Medina

Laura Sánchez González, Francisco Ruiz and Félix García. *Guías para el Modelado de Procesos de Negocio* *91-104*

Andrea Delgado, Barbara Weber, Francisco Ruiz and Ignacio García-Rodríguez de Guzmán. *A proposal on service execution measures for the improvement of business processes realized by services* *105-110*

Clara Ayora, Victoria Torres and Vicente Pelechano. *Feature Modeling to deal with Variability in Business Process Perspectives* *111-124*

Adela Del Río Ortega, Cristina Cabanillas Macías, Manuel Resinas Arias de Reyna and Antonio Ruiz Cortés. *PPINOT: A Tool for the Definition and Analysis of Process Performance Indicators* *125-128*

Sesión 4: Ingeniería de Servicios II
Chair: Dr. Vicente Pelechano

Jenifer Verde, Juan Manuel Vara, Veronica Andrea Bollati and Esperanza Marcos. *Desarrollo de puentes tecnológicos para soportar el modelado de interfaces de servicio* *131-144*

Rubén Casado, Javier Tuya and Muhammad Younas. *An Abstract Transaction Model for Testing the Web Services Transactions* *145-146*

José María García, David Ruiz, and Antonio Ruiz-Cortés. *A Model of User Preferences for Semantic Services Discovery and Ranking* *147-148*

M.Carmen De Castro, Azahara Camacho-Magriñán and Inmaculada Medina-Bulo. *Aplicación de la técnica de las pruebas metamórficas a una composición de servicios: Metasearch* *149-154*

Sesion 5: SOA, Tecnologías para Servicios Web y Aplicaciones II
Chair: Dr. Víctor Ayllón

Carlos Müller, Marc Oriol Hilari, Marc Rodríguez, Xavier Franch, Jordi Marco, Manuel Resinas and Antonio Ruiz-Cortés. *SALMonADA: A Platform for Monitoring and Explaining Violations of WS-Agreement-Compliant Documents* *157-160*

José María García, David Ruiz and Antonio Ruiz-Cortés. *SOA4All Integrated Ranking: A Preference-based, Holistic Implementation* *161-164*

José A. Martin, F. Martinelli and Ernesto Pimentel. *Synthesis of Secure Adaptors* *165-166*

Jose A. Dorado, Juan Boubeta-Puig, Guadalupe Ortiz and Inmaculada Medina-Bulo. *Detección de Ataques de Seguridad mediante la Integración de CEP y SOA 2.0* *167-172*

Sesion 6: Procesos de Negocios II
Chair: Dr. Juan Manuel Vara

Cristina Cabanillas, Adela Del-Río-Ortega, Manuel Resinas and Antonio Ruiz-Cortés. *RAL Solver: a Tool to Facilitate Resource Management in Business Process Models* *175-178*

Cristina Cabanillas, Manuel Resinas, and Antonio Ruiz-Cortés. *Defining and Analysing Resource Assignments in Business Processes with RAL* *179-180*

Detección de Ataques de Seguridad mediante la Integración de CEP y SOA 2.0

Jose Antonio Dorado Cerón, Juan Boubeta Puig, Guadalupe Ortiz e Inmaculada Medina Bulo

Departamento de Ingeniería Informática, Universidad de Cádiz,
C/Chile 1, 11002 Cádiz, España
jose.doradoce@alum.uca.es
{juan.boubeta,guadalupe.ortiz,inmaculada.medina}@uca.es

Resumen La seguridad informática cada día cobra mayor importancia debido al incremento de ataques que se realizan tanto para intentar acceder a los datos críticos como para detener procesos esenciales en los sistemas. Así pues, la detección temprana de estos ataques es fundamental para asegurar la integridad, disponibilidad y confidencialidad de la información. En este artículo desarrollamos un sistema que integra SOA 2.0 junto con un motor de procesamiento de eventos complejos (CEP) y un sistema de detección de intrusiones (IDS) para detectar inmediatamente las amenazas de seguridad que se produzcan en sistemas complejos y heterogéneos, así como ponerlas en conocimiento a los responsables de seguridad. Estos tomarán las medidas oportunas para reducir el impacto de estas situaciones. Los resultados experimentales obtenidos demuestran que nuestro enfoque, que integra SOA 2.0 con CEP e IDS, es una buena alternativa para el campo de la seguridad informática.

Keywords: CEP, seguridad, amenaza, IDS, Snort, SOA 2.0.

1. Introducción

Actualmente, el campo de la seguridad informática cobra cada día mayor importancia, y eso es debido a que cada vez son más los sistemas de información que almacenan datos críticos para sus usuarios. Esto tiene como consecuencia un significativo incremento del número de atacantes. Por ello es necesario buscar una nueva solución capaz de hacer frente a esta problemática.

En el campo de la seguridad es imprescindible minimizar el tiempo de respuesta a los posibles ataques, debido a que una respuesta fuera de los plazos permisivos puede suponer, en la mayoría de los casos, el éxito del atacante.

Así pues, la tecnología que se ha decidido utilizar atendiendo a los requisitos mencionados es el procesamiento de eventos complejos o *Complex Event Processing* (CEP) [5,8]. Gracias a CEP vamos a poder procesar y analizar en tiempo real una gran cantidad de eventos, además de correlacionarlos entre sí y así poder responder a las situaciones críticas producidas en los sistemas de información. El software que se utilizará es un motor CEP denominado Esper [2,9] que provee

M.V. de Castro, J.M. Gómez, L. Iribarne (Eds.): JCIS'2012, pp. 167-172, ISBN:978-84-15487-26-5.
Jornadas Sistedes'2012, Almería 17-19 sept. 2012, Universidad de Almería.

un lenguaje de procesamiento de eventos o *Event Processing Language* (EPL) para definir los patrones de eventos que detectarán las situaciones críticas.

A la hora de escoger el enfoque en el que nos vamos a basar, tenemos que tener muy en cuenta que, como afirma Boubeta et al. [6], las arquitecturas orientadas a servicios o *Service-Oriented Architecture* (SOA) [14] no son adecuadas, por sí mismas, para el tratamiento de grandes cantidades de eventos en tiempo real. Por tanto, vamos a hacer uso de la arquitectura alternativa propuesta en ese mismo artículo: una integración de las arquitecturas dirigidas por eventos o *Event-Driven Architecture* (EDA) [12] y SOA, combinada con el uso de CEP. Además, vamos a utilizar un bus de servicios empresariales o *Enterprise Service Bus* (ESB) [13] que nos va a permitir llevar a cabo la integración de las diferentes arquitecturas y tecnologías, además de ofrecer otras ventajas como el desacoplamiento o la creación de un sistema mucho más mantenible y escalable. Concretamente vamos a hacer uso de Mule ESB [3,7] que nos proporciona los componentes necesarios para integrar las diferentes tecnologías.

Otro de los puntos de interés de este trabajo es el uso de una herramienta para la monitorización del tráfico de red, concretamente Snort [4], que es un sistema de detección de intrusos o *Intrusion Detection System* (IDS) basado en reglas que pueden ser desarrolladas a medida. En este artículo exponemos cómo hemos llevado a cabo la integración de este IDS (funciona como productor de eventos) con nuestra aplicación y los resultados que se han obtenido detectando intrusiones en tiempo real.

El resto del artículo se estructura de la siguiente manera. En la sección 2 se describe e implementa el caso de estudio en el que utilizamos nuestro sistema para la detección de amenazas. Posteriormente en la sección 3 se enumera una serie de trabajos relacionados y, por último, en la sección 4 se exponen las conclusiones y el trabajo futuro.

2. Caso de Estudio

En los últimos tiempos el número de ataques contra los sistemas de información y las pérdidas originadas por ello se han visto incrementadas de manera significativa [1]. Por tanto, hemos desarrollado un caso de estudio para paliar cuanto antes esta situación detectando estos ataques en tiempo real.

Se ha adaptado al campo de la seguridad informática la arquitectura SOA 2.0 propuesta en [6] con el fin de detectar los ataques más comunes utilizando Snort como productor de eventos. Como consumidor de la información se ha decidido implementar una solución que envía las alarmas de cada ataque detectado mediante un correo electrónico al responsable de la seguridad del sistema.

En cuanto a los ataques posibles a detectar, hemos escogido algunos de los ataques más comunes que intentan explotar algunos puertos específicos. Se han tenido en cuenta los ataques de denegación de servicios (DOS), ataques que utilizan técnicas de ocultación de identidad (e.g., *spoofing*) como el ataque *smurf* o *land*, ataques sobre puertos específicos tales como ataque *supernuke*, ataque al puerto FTP, ataque *flood* al email o el escaneo de puertos TCP.

2.1. Patrones de Eventos Complejos Aplicados a la Seguridad

A continuación vamos a describir en la Tabla 1 los patrones de eventos complejos que permiten detectar los ataques especificados anteriormente. En esta sub-sección se especifican tan solo el nombre de cada patrón, y los parámetros que tenemos en cuenta en cada caso para detectarlos.

Cuando el requisito para detectar un ataque es que en todas las alertas un parámetro sea siempre el mismo se indicará en la tabla con el valor "igual", mientras que si dicho parámetro debe variar en cada alerta lo indicamos especificando "varía" para dicho parámetro.

Ataque	IP origen	IP destino	Puerto origen	Puerto destino	Eventos/min
DOS	Igual	Igual		Igual	10
Smurf	IP destino	Igual		Distinto de origen	2
Land	IP destino	Igual	Puerto destino	Igual	2
Supernuke		Igual		137, 138 o 139	10
Escaneo puertos	Igual	Igual	Igual	Varía	10
Flood a email		Igual		25, 110, 143, 993	10
FTP		Igual		21	10

Tabla 1. Detalle de los parámetros tenidos en cuenta para cada patrón de evento.

2.2. Arquitectura Propuesta

El funcionamiento básico de nuestra arquitectura (véase Figura 1) es el siguiente: el productor de eventos, Snort, generará una alerta cada vez que detecte una situación anómala. A continuación, el sistema capturará en tiempo real cada una de esas alertas cuya información será transformada en eventos que serán enviados al motor de Esper. Finalmente, este motor correlacionará y comparará los eventos recibidos con los patrones de eventos y, cuando se cumplan las condiciones establecidas en dichos patrones, se informará al *listener* correspondiente que se encargará de notificar estas situaciones al consumidor de eventos pertinente.

2.3. Resultados

En este trabajo se han llevado a cabo los experimentos necesarios para demostrar que el sistema diseñado utilizando Snort y el motor CEP de Esper es adecuado para la detección de ataques de seguridad en tiempo real. Para ello, hemos comprobado qué tasa de eventos es capaz de responder correctamente.

Por lo tanto, para medir la eficiencia del sistema, nuestro objetivo se centra en comprobar cuántas alertas de cualquier ataque es capaz de procesar nuestro sistema. En este caso, estos eventos pueden referirse a cualquiera de los ataques especificados.

La finalidad de nuestro software es detectar un ataque utilizando un número bajo de eventos, ya que lo que se pretende es la detección temprana en el tiempo

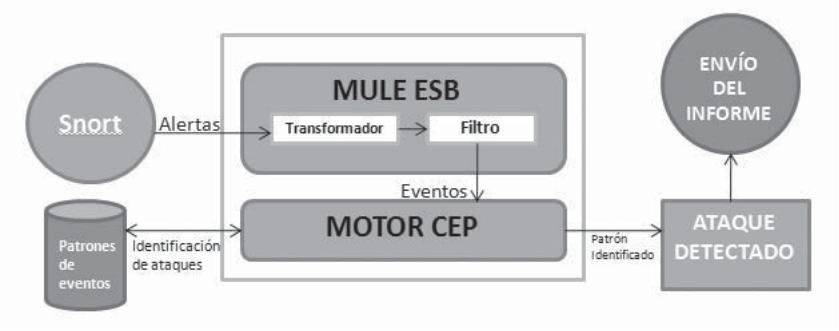

Figura 1. Arquitectura SOA 2.0 que integra Snort, Mule y Esper para la detección temprana de amenazas de seguridad .

de un posible ataque, antes de causar un daño mayor. En un escenario real, a pesar de detectar el ataque con una cifra baja de eventos, los atacantes pueden persistir en el ataque mientras que no se tomen las medidas adecuadas. En la Tabla 2 se muestra el tiempo necesario para procesar los eventos hasta que se detecta la amenaza, así podemos conocer cuál es la capacidad real de nuestro sistema para recibir y procesar grandes cantidades de eventos.

Para obtener un buen rendimiento, este software debe ser ejecutado en una máquina con al menos 2048 MB de memoria RAM y un procesador de 2 GHz. Además, puede ser utilizado tanto en plataformas Windows como Linux.

Para llevar a cabo los experimentos se han generado diferentes baterías de eventos a partir de alertas reales de Snort y se han comprobado cuántos de estos eventos es capaz de procesar y detectar nuestro sistema. Dichas baterías se componen, en cada caso, de una cantidad cada vez mayor de eventos reales de Snort que se pretende que reciba el sistema para comprobar la capacidad de reacción que tiene nuestro sistema en cada uno de estos escenarios.

Nº de eventos recibidos	10	100	500	1000	2000	5000
Tiempo (s)	0,468	0,771	1,895	3,194	11,538	84,184

Tabla 2. Tiempo desde que recibe el primer evento hasta que informa al consumidor.

3. Trabajos Relacionados

Cada vez son más los trabajos que se llevan a cabo sobre CEP. En los últimos tiempos debemos destacar el trabajo de Zappia et al. [15], que proponen una arquitectura muy ligera, fácil de usar, escalable, extensible y portable basada en un diseño de arquitecturas en capas. Estas características son similares a las de nuestra aplicación, gracias sobre todo al uso de un ESB. Este artículo presenta un caso sobre el seguimiento de mercancías peligrosas en el transporte

marítimo y los resultados obtenidos para este campo crítico apoyan nuestro trabajo demostrando que este enfoque es correcto para estas aplicaciones.

En el campo de la seguridad informática podemos destacar el trabajo de Kou y Wen [11] que proponen un sistema de defensa para un *smartphone* utilizando Snort. Este artículo demuestra la portabilidad de este tipo de sistemas, que pueden diseñarse para otro tipo de plataformas como Android. A diferencia de nuestro trabajo, los autores de este artículo no incluyen resultados concluyentes respecto a la capacidad de respuesta del sistema ante grandes cantidades de amenazas, algo que nosotros hemos solucionado con el uso de un motor CEP.

Otro estudio a tener en cuenta es el de Ismail et al. [10] que proponen la implementación de un IDS basado en Snort con el fin de detectar el *malware* en una red de área local. Este estudio se ha implementado en la universidad de Kuala Lumpur y tiene como objetivo la detección de accesos a una base de datos MySQL, WINPCAP y *scripts* de Perl. Aunque a diferencia de nuestra propuesta, no trata de detectar ataques en los que se envíen una gran cantidad de información contra un puerto determinado ni muestra resultados sobre experimentos donde se reciban cantidades importantes de ataques al mismo tiempo.

Existen otros trabajos que proponen el uso de Sn*ort* junto a otras herramientas; por ejemplo, Jiqiang y Yining [16] han diseñado un sistema en el que cooperan tanto Snort como *IPSec* para la detección de diferentes amenazas en sistemas de tipo Windows, a diferencia de nuestro software que sí puede utilizarse en diferentes plataformas.

4. Conclusiones y Trabajo Futuro

En este artículo se ha propuesto el uso de una arquitectura software SOA 2.0 junto con el motor CEP de Esper, utilizando el ESB Mule para la integración de las diferentes tecnologías. Además, hemos utilizado Snort como proveedor de la información y un servidor de correo electrónico como consumidor de la información. Gracias a este enfoque podemos detectar en un reducido espacio temporal distintos ataques de seguridad, que hemos definido previamente mediante patrones de eventos en EPL.

Los resultados demuestran que el uso de CEP es adecuado para trabajar en el campo de la seguridad informática, ya que nos permite trabajar en tiempo real con una gran cantidad de eventos sin ver afectado su rendimiento.

Una de las principales mejoras a introducir en nuestro sistema es la incorporación de nuevos patrones de eventos, que permitirán detectar más ataques de seguridad de los que tenemos en cuenta actualmente.

Aprovechando la escalabilidad del sistema que hemos diseñado, sustituiremos el IDS Snort por otras soluciones disponibles en el mercado. Así podremos observar el comportamiento del sistema ante un cambio de proveedor de información, además de llevar a cabo una comparativa entre los resultados obtenidos actualmente con Snort y los que se puedan obtener utilizando otros productores de eventos. A su vez, también se estudia la posibilidad de combinar varios ESB

y motores CEP para obtener un sistema de procesamiento de eventos a gran escala y más eficiente.

Agradecimientos. Este trabajo fue financiado por el proyecto MoDSOA (TIN 2011-27242) del Programa Nacional de Investigación, Desarrollo e Innovación del Ministerio de Ciencia e Innovación y por el proyecto PR2011-004 del Plan de Promoción de la Investigación de la Universidad de Cádiz.

Referencias

1. Abc (septiembre 2011), http://www.abc.es/20110915/sociedad/abci-perdidas-cibercrimen-201109151628.html
2. Esper (diciembre 2011), http://esper.codehaus.org/
3. Mule ESB (enero 2012), http://www.mulesoft.org/
4. Snort (enero 2012), http://www.snort.org/
5. Ayllón, V., Reina, J.M.: CEP/ESP: Procesamiento y Correlacion de gran Cantidad de Eventos en Arquitecturas SOA. In: 4th Jornadas Científico-Técnicas en Servicios Web y SOA. pp. 97–110. Sevilla (2008)
6. Boubeta Puig, J., Ortiz, G., Medina Bulo, I.: Procesamiento de Eventos Complejos en Entornos SOA: Caso de Estudio para la Deteccion Temprana de Epidemias. In: Actas de las VII Jornadas de Ciencia e Ingenieria de Servicios. pp. 63–76. Servizo de publicacions da Universidade da Coruña, A Coruña, Spain (septiembre 2011)
7. Dossot, D., DÉmic, J.: Mule in Action. Manning Publications (2010)
8. Etzion, O., Niblett, P.: Event Processing in Action. Manning Publications (agosto 2010)
9. Inc., E.: Esper 4.0.0 - reference documentation (2009), http://esper.codehaus.org/esper/documentation/documentation.html
10. Ismail, M.N., Ismail, M.T.: Framework of Intrusion Detection System via Snort Application on Campus Network Environment. In: International Conference on Future Computer and Communication, 2009. ICFCC 2009. pp. 455–459. IEEE (abril 2009)
11. Kou, X., Wen, Q.: Intrusion Detection Model Based on Android. In: 2011 4th IEEE International Conference on Broadband Network and Multimedia Technology (ICBNMT). pp. 624–628. IEEE (octubre 2011)
12. Michelson, B.M.: Event-driven architecture overview: Event-Driven SOA Is Just Part of the EDA Story (febrero 2006), http://dx.doi.org/10.1571/bda2-2-06cc
13. Rademakers, T., Dirksen, J.: Open Source ESBs in Action. Manning Publications (2009)
14. Sward, R.E., Boleng, J.: Service-Oriented Architecture (SOA) concepts and Implementations. In: Proceedings of the 2011 ACM annual international conference on Special interest group on the ada programming language. pp. 3–4. New York, NY, USA (2011)
15. Zappia, I., Paganelli, F., Parlanti, D.: A lightweight and Extensible Complex Event Processing System for Sense and Respond Applications. Expert Systems with Applications
16. Zhai, J., Xie, Y.: Researh on Network Intrusion Prevention System Based on Snort. In: 2011 6th International Forum on Strategic Technology (IFOST). vol. 2, pp. 1133–1136. IEEE (agosto 2011)