DEPARTAMENTO DE
INFORMÁTICA

Universidad Técnica Federico Santa María

Contacto

CIBSI'05
Departamento de Informática - UTFSM
Casilla 110-V
Valparaíso - Chile

Fono: +56(32) 654 429
Fono: +56(32) 654 424
Fax: +56(32) 797 513
e-mail: cibsi@inf.utfsm.cl
cibsi05@inf.utfsm.cl
URL:http://cibsi05.inf.utfsm.cl

≫ AUSPICIA

Microsoft · software AG · IBM · McAfee · Cisco Systems · Impsat · mti · GALA · Grani · NEOSECURE · ORACLE · Guidance Software

≫ PATROCINA

Biblioteca del Congreso Nacional de Chile · Corporación de Capacitación y Empleo SOFOFA · Sociedad Chilena de Ciencia de la computación

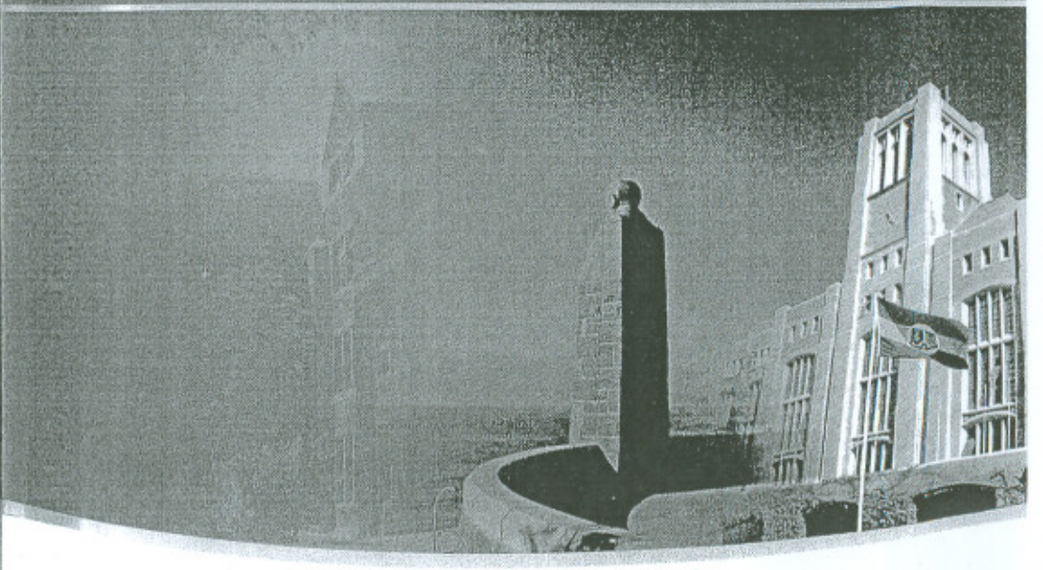
UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA
DEPARTAMENTO DE INFORMATICA

3ER CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMATICA

DEPARTAMENTO DE INFORMÁTICA

CIBSI05



21-25 NOVIEMBRE 2005

ACTAS

CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMATICA

21 - 25 de Noviembre de 2005

Valparaíso, Chile

ISBN 956-7051-10-0
Actas del
3° Congreso Iberoamericano de Seguridad Informática

CIBSI'05

Prólogo

Tenemos el agrado de poner a disposición de los participantes los trabajos aceptados y presentados en el **Tercer Congreso Iberoamericano de Seguridad Informática (CIBSI'05)** realizado entre el 21 y el 25 de Noviembre del 2005 en la ciudad de Valparaíso, Chile, evento que ha sido organizado por el Departamento de Informática de la Universidad Técnica Federico Santa María (Chile) en conjunto con la Universidad Politécnica de Madrid (España).

De un total de 60 artículos enviados al congreso, se seleccionaron un total de 35 trabajos. De este total, 31 de ellos tenían autores de un solo país, y que se distribuyen de la siguiente manera: Argentina (6), Brasil (2), Colombia (3), Chile (1), España (14), México (4) y Uruguay (1). Además se presentaron otros 4 trabajos con autores de diferentes países, donde en cada uno de ellos al menos existe un coautor español y los demás coautores son de Chile, EE.UU., Francia, Polonia y Uruguay.

Los artículos seleccionados cubren las áreas:

- Criptografía, esteganografía y protocolos de seguridad.
- Seguridad en sistemas, redes, comunicaciones y prevención y detección de intrusos.
- Seguridad en sistemas de información, en la Web y en el comercio electrónico.
- Modelos de gestión y auditoría en seguridad

Como parte del programa se han incluido tres charlas magistrales sobre voto electrónico, seguridad en entornos ubicuos y tendencias en criptografía.

También como parte del programa, se organizó en conjunto con la Biblioteca del Congreso Nacional de Chile, en el primer día, un evento sobre seguridad informática en el Estado y se incluyeron 5 charlas técnicas de empresas auspiciadoras tales como Cisco Systems, IBM, McCaffee, Neosecure y Software AG.

Deseamos agradecer primero al Comité de Programa por el esfuerzo realizado en la revisión de todos los artículos y en el proceso de selección de éstos. En segundo lugar agradecer a los patrocinadores y auspiciadores que apoyaron de diferentes formas a producir el evento CIBSI'05. Finalmente agradecer a todos los organizadores. Esperamos que la estadía en Valparaíso y la participación en CIBSI'05 haya sido provechosa y de su agrado.

Raúl Monge
Presidente de Comité Organizador

Jorge Ramió
Vicepresidente de Comité Organizador

Valparaíso, Chile

Noviembre, 2005

Organización

Comité Organizador

Dr. Raúl Monge Anwandter (Universidad Técnica Federico Santa María, Chile)
Dr. Jorge Ramió Aguirre (Universidad Politécnica de Madrid, España)
Sr. Javier Cañas Robles (Universidad Técnica Federico Santa María, Chile)

Conferencistas Invitados

Dr. René Peralta (National Institute of Standards and Technology, USA)
Dr. Javier López (Universidad de Málaga, España)

Comité de Programa

Dr. Juan Pedro Hecht (Universidad de Buenos Aires, Argentina)
Dr. Hugo Scolnik (Universidad de Buenos Aires, Argentina)
Dr. Ricardo Dahab (Universidade Estadual de Campinas, Brasil)
Dr. Marco Aurelio Henriques (Universidade Estadual de Campinas, Brasil)
Dr. Adriano Mauro Cansian (Universidade Estadual Paulista, Brasil)
Dr. Routo Terada (Universidade de São Paulo, Brasil)
Dr. Marcos Kiwi (Universidad de Chile, Chile)
Dr. Horst von Brand (Universidad Técnica Federico Santa María, Chile)
Dr. Juan Guillermo Lalinde Pulido (Universidad EAFIT, Colombia)
Dr. Jeimy José Cano Martínez (Universidad de los Andes, Colombia)
Dr. Julio Cesar López (Universidad del Valle, Colombia)
Dr. Jorge Estrada Sarlabous (Academia de Ciencias de Cuba, Cuba)
Dr. Javier Areito Bertolín (Universidad de Deusto, España)
Dr. Joan Borrel Viader (Universidad Autónoma de Barcelona, España)
Dra. Pino Caballero Gil (Universidad de La Laguna, España)
Dr. Jorge Dávila Muro (Universidad Politécnica de Madrid, España)
Dr. Luis Hernández Encinas (Consejo Superior de Investigaciones Científicas CSIC, España)
Dr. Josep Lluís Ferrer-Gomila (Universidad de Las Islas Baleares, España)
Dr. Francisco Javier López Muñoz (Universidad de Málaga, España)
Dra. Amparo Fúster Sabater (Consejo Superior de Investigaciones Científicas CSIC, España)
Dr. Arturo Ribagorda Garnacho (Universidad Carlos III de Madrid, España)
Dr. Miguel Soriano Ibañéz (Universidad Politécnica de Cataluña, España)
Dr. Hugo César Coyote Estrada (Instituto Politécnico Nacional, México)
Dr. Enrique Daltabuit Godas (Universidad Nacional Autónoma de México, México)
Dr. Carlos Mex Perera (ITESM campus Monterrey, México)

Dr. Sergio Rajsbaum Godorezky (Universidad Nacional Autónoma de México, México)
Dr. Horacio Tapia Recillas (Universidad Autónoma Metropolitana, México)
Dr. Edmundo Monteiro (Universidad de Coimbra, Portugal)
Dr. Emilio Hernández (Universidad Simón Bolívar, Venezuela)
Dr. Alfredo Viola Deambrosis (Universidad de la República - Uruguay)

Logística

Srta. Claudia Arancibia (Universidad Técnica Federico Santa María, Chile)
Srta. Carol Castro (Universidad Técnica Federico Santa María, Chile)

Edición y Publicación de Actas

Sr. Pablo Itaim (Universidad Técnica Federico Santa María, Chile)

Auspician

ADEXUS
Cisco Systems
Guidance Software
IBM
impSat
McAfee Proven Security
Microsoft
SECURE
Software AG The XML Company
ORACLE
Grami
GALA Hotel & Centro de Eventos
mti

Patrocinan

Sociedad Chilena de Ciencia de la Computación
Biblioteca del Congreso Nacional de Chile
Corporación de Capacitación y Empleo SOFOFA

Índice general

Conferencias Magistrales

Tecnologías de voto electrónico

Martes, 22 de Noviembre 2005, 12:45-14:00

Dr. René Peralta
National Institute of Standards and Technology, USA

Se describirán, en líneas generales, las principales técnicas propuestas que existen hoy en día (algunas ya en uso) para voto electrónico. En EE.UU. existen actualmente dos fuertes controversias con respecto a esta tecnología. El primer punto en discusión es la conveniencia o no de generar, para efectos de auditoria, una copia en papel de cada voto. El segundo punto es la factibilidad del voto por Internet. Se presentarán los principales argumentos en pro y en contra de estas alternativas. Luego se muestra la posición del conferencista al respecto.

Entornos pervasivos y ubicuos: La nueva (in)-seguridad

Miércoles, 23 de Noviembre 2005, 12:45-14:00

Dr. Javier López
Universidad de Málaga, España

Como evolución a las aplicaciones desarrolladas para entornos móviles, las aplicaciones para entornos pervasivos y ubicuos se han establecido firmemente como la próxima frontera en la investigación de Seguridad. Parece obvio que las soluciones de seguridad desarrolladas para la tecnología de hace unos pocos años no resultan adecuadas, dadas las restrictivas características físicas de los nuevos dispositivos y los característicos entornos donde se usan. Aún así, el diseño de las nuevas soluciones preservan muchas de las características de antes, lo que supone un error en multitud de ocasiones. En esta presentación se analizarán los problemas que están abiertos y el abanico de posibles estrategias a seguir para dotar de soluciones seguras a estos nuevos entornos tecnológicos.

Elicitación de Requisitos de Seguridad para Servicios Web en PWSSec

Carlos Gutiérrez, Eduardo Fernández-Medina y Mario Piattini

Grupo de Investigación Alarcos. Universidad de Castilla-La Mancha.
Paseo de la Universidad 4, 13071, Ciudad Real. (SPAIN). Tel: 34 926 29 53 00
{Carlos.Gutierrez, Eduardo.FdezMedina,
Mario.Piattini}@uclm.es

Abstract. *El paradigma de los Servicios Web (WS de aquí en adelante) ha conseguido una relevancia tal tanto en el campo académico como en el campo de la industria que la visión de Internet ha evolucionado pasando de ser considerada como un mero repositorio de datos para convertirse en la infraestructura subyacente sobre la que se están llevando a cabo procesos de negocio críticos y complejos así como alianzas estratégicas entre organizaciones con sistemas de información heterogéneos. La seguridad es un aspecto clave para que los WS sean aceptados de forma generalizada por las organizaciones. De hecho, durante los últimos años, los consorcios de Internet más relevantes, como el IETF, OASIS, o W3C, han desarrollado un número enorme de guías, recomendaciones y estándares de seguridad para WS. Pese a este espectacular crecimiento, no existe todavía un proceso de desarrollo que facilite la integración sistemática de la seguridad en todas y cada una de las etapas del ciclo de desarrollo de sistemas software basados en WS. El último objetivo de un proceso tal sería guiar a los desarrolladores de sistemas basados en el paradigma en cuestión durante la especificación de los requisitos de seguridad, el diseño de la arquitectura de seguridad software y el despliegue de los estándares de seguridad para WS más adecuados para cada proyecto. En este artículo, presentaremos de forma breve un proceso, denominado PWSSec (Proceso para el Desarrollo de Sistemas Seguros basados en Servicios Web) y, con más detenimiento, los artefactos que son utilizados durante la actividad de elicitación incluida en la etapa WSSecReq (Requisitos de Seguridad para Servicios Web) que pertenece a PWSSec y cuyo propósito es producir una especificación de requisitos de seguridad específicos para WS.*

1 Introducción

Los WS se basan en estándares de Internet, red sobre la cual, tal y como demuestran las estadísticas presentadas por el CERT, el número de incidentes relacionados con la seguridad ha crecido de manera exponencial durante los últimos años (se ha pasado de 2573 incidentes reportados en 1996 hasta los 137529 en el año 2003) [1]. Uno de los factores principales que motivan este fenómeno es la incorporación de forma generalizada de las nuevas tecnologías, como aquellas basadas en Internet, en un gran número de aspectos de la sociedad moderna ya que las aplicaciones software son cada vez más ubicuas, heterogéneas y críticas en sus objetivos y vulnerabilidades [2].

Un aspecto determinante para la adopción definitiva por parte de la industria de las tecnologías basadas en WS es la seguridad. Los WS se ejecutan sobre Internet lo cual implica un riesgo inherente. Además, el trabajo llevado a cabo por los principales consorcios de la industria dirige su esfuerzo a alcanzar la completa estandarización de los mecanismos de seguridad que pueden ser aplicados en este tipo de sistemas. Esto ha provocado que exista un número muy alto de estándares de seguridad que dificultan la tarea a los desarrolladores, muchas veces no expertos en seguridad, a la hora de saber qué mecanismos de seguridad deben aplicar y con cuál de todos los estándares deben ser implementados. Es necesario pues, un paso previo, que infiera a los desarrolladores la capacidad de identificar fácilmente qué requisitos de seguridad son necesarios considerar en su sistemas de forma que puedan saber qué mecanismos de seguridad necesitan y, por tanto, qué estándar o estándares deben conocer con mayor profundidad.

Con el objeto de resolver este problema, hemos definido el proceso PWSSec (Proceso para el Desarrollo de Sistemas Seguros basados en Servicios Web). Este proceso se compone de tres etapas. La primera etapa, denominada WSSecReq (Requisitos de Seguridad para Servicios Web) tiene como objetivo producir la, mencionada con anterioridad, especificación de requisitos de seguridad específicos para WS. En particular, su primera actividad, denominada elicitación, aplica un conjunto de artefactos reutilizables que sirven de guía a los desarrolladores en la tarea de identificar y especificar los requisitos de seguridad para sus sistemas basados en WS. El principal propósito de este artículo es describir este conjunto de artefactos mostrando cómo se pueden utilizar de una manera coordinada para especificar, de una manera sistemática, los requisitos de seguridad de cierto sistema software basado en WS.

La contribución principal realizada en este artículo con respecto a otras publicaciones como [3] es la descripción detallada del conjunto de artefactos de seguridad utilizados durante la actividad de elicitación de la etapa WSSecReq del proceso PWSSec.

El resto de este artículo se organiza de la siguiente manera: en la sección 2 se presenta una visión general del proceso PWSSec; en la sección 3, se ofrece una descripción completa de los artefactos mencionados; y en la sección 4, se presentan las conclusiones así como las líneas de investigación abiertas.

2 PWSSec – Proceso para el Desarrollo de Sistemas Seguros basados en Servicios Web

El proceso PWSSec [3] permite definir los requisitos de seguridad para sistemas basados en WS y describe una arquitectura de seguridad de referencia que facilita el diseño e implementación de arquitecturas concretas de seguridad basadas en WS que implementen cierto conjunto de estándares.

En general, las principales características de este proceso son: i) Proceso iterativo e incremental de forma que facilita el desarrollo y la gestión de los riesgos [4] y la integración gradual de la seguridad en los sistemas basados en WS [5]; ii) trazabilidad y reusabilidad del proceso de desarrollo e interoperabilidad y reusabilidad de los

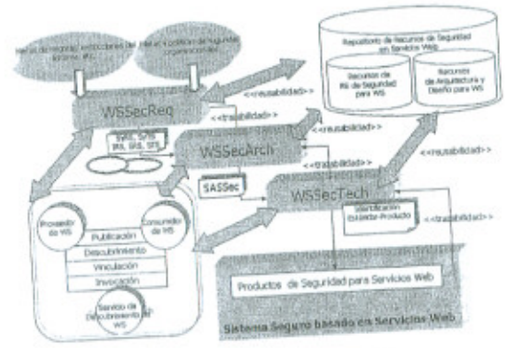


Fig. 1. Esquema general del proceso PWSSec

productos; iii) proceso centrado en los elementos y los procedimientos básicos definidos para una arquitectura basada en WS [6]: los actores básicos son los agentes proveedores de servicios, los agentes consumidores de los servicios y los agentes de descubrimiento mientras que los procedimientos básicos son publicación, descubrimiento, vinculación e invocación.

Como ya se ha señalado previamente, PWSSec define tres etapas de desarrollo que permiten obtener una especificación de los requisitos de seguridad (WSSecReq), posteriormente una arquitectura de seguridad (WSSecArch – Arquitectura de Seguridad para Servicios Web) y, finalmente, un diseño a bajo nivel basado en estándares de seguridad para WS (Tecnologías de Seguridad para Servicios Web). En la siguiente sección veremos con más detalle la primera de estas etapas.

3 Elicitación en WSSecReq

En esta sección, explicaremos el conjunto de artefactos de seguridad utilizados en la etapa WSSecReq.

En ocasiones, presentaremos algunos ejemplos concretos en los que se muestran la aplicación práctica de estos artefactos. Los ejemplos de los artefactos concretos mostrados en este artículo se basan en el caso de uso clásico 'Procesar Pedido'. Este caso de uso consiste de una interacción petición/respuesta que inicia el agente de WS de la empresa minorista (que llamaremos WS-Minorista), cuando detecta que alguno de sus productos está fuera del stock mínimo, enviando una petición de reposición de

stock al agente de WS consumidor de la organización proveedora (que llamaremos WS-Proveedor).

3.1 Vistazo de WSSecReq

Se han considerado dos principios básicos en la definición de WSSecReq: reusabilidad y trazabilidad. La reusabilidad de los productos se consigue mediante la definición de dos repositorios:

- Un repositorio denominado *Recursos de E&A de Requisitos de Seguridad en WS* que incluye el conjunto de artefactos reutilizables, descritos en la Figura 1, que facilitan el descubrimiento de los requisitos de seguridad específicos para WS. Estos artefactos serán explicados en detalle más adelante.
- Repositorio de Requisitos de Seguridad para WS que contiene un conjunto de plantillas de requisitos de seguridad para WS que pueden ser aplicadas a diversos sistemas basados en WS pertenecientes a diferentes dominios.

Ambos repositorios son actualizados constantemente. Por otro lado, la trazabilidad de los diferentes productos generados se resuelve por medio de una aplicación progresiva y razonada de un conjunto de artefactos de seguridad. Estos artefactos, y su aplicación, se detallarán en la siguiente sección.

La entrada de la etapa WSSecReq consiste de:

- Una especificación del alcance funcional que se desea abarcar durante la iteración (ej: si se dispone de una definición de los casos de uso [7] se pueden seleccionar aquellos que se desean resolver y utilizarlos como entrada para la iteración). La granularidad y nivel de abstracción de la especificación funcional sobre la que se analizará la seguridad es variable y está sujeta al momento del ciclo de desarrollo para el que se planea la iteración. Por ejemplo, en la iteraciones iniciales la granularidad y nivel de abstracción se podría establecer a nivel de caso de uso de negocio o proceso de negocio y, en etapas donde ya se divisa de manera inicial la arquitectura software, el nivel de granularidad y nivel de abstracción podría estar dada por especificaciones de casos de uso de sistema o diagramas de interacción de las entidades definidas en el modelo conceptual del análisis. De acuerdo con [8], y aplicado a los sistemas basados en WS, el proceso de identificación de los servicios es una actividad que se lleva a cabo previamente a la especificación de los casos de uso de sistema. En este tipo de proceso de desarrollo, los requisitos funcionales, una vez han sido identificados son transformados en flujos de actividades, que resultan ser lo suficientemente detalladas de forma que cada actividad sea llevada a cabo por un actor. Tras esta división inicial, los requisitos son reordenados en base a los actores que los ejecutan, es decir, los actores que obtienen información de la actividad o los actores que le envían información. Hay que tener en cuenta que, en los procesos de desarrollo de este tipo de sistemas, el modelo tradicional de actores se extiende para incorporar un nuevo tipo de actor denominado servicio.
- Las metas de negocio y seguridad definidas para el sistema así como el fragmento de la política de seguridad organizacional que se estime que pueda impactar en el diseño del mismo.

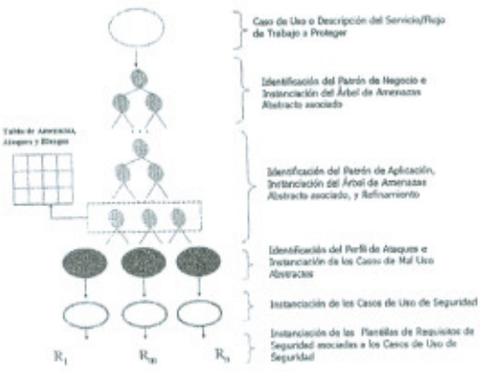


Fig. 2. Aplicación progresiva de los artefactos de seguridad utilizados durante la actividad de elicitación de la etapa WSSecReq.

Esta etapa define cinco actividades [3]: elicitación, análisis, especificación y verificación y validación. En este artículo nos centraremos en la actividad de elicitación y, en particular, en los artefactos involucrados. La actividad de elicitación se basará en la realización de un análisis completo de la seguridad de cada WS (incluidas las interacciones en las que participe) identificado y considerado en la iteración actual.

La actividad de elicitación combina conceptos derivados de métodos de análisis y gestión de riesgos (en particular del proceso elaborado por el SEI conocido como Operationally Critical Attack, Asset, and Vulnerability Evaluation ^{SM} (OCTAVE) [9]) con técnicas que facilitan la reusabilidad de los requisitos de seguridad [10, 11].

3.2 Trazabilidad en WSSecReq

Árbol Abstracto de Amenazas y Ataques de Patrón de Negocio de WS Extended Enterprise
ID: A3Neg-EE
Objetivo: 1. Causar Daño durante la Ejecución de **[Proceso de Negocio | Caso de Uso de Negocio]** *X*.
OR/AND 1. Atacar Entidades de Negocio.
2. Atacar de Red.
3. Atacar Reglas de Negocio.
4. Atacar Interacciones.

Fig. 3. Árbol de amenazas abstracto asociado con el patrón de negocio Empresa Extendida.

Instancia de Árbol Abstracto de Ataques y Amenazas de Patrón de Negocio de WS

ID: A3Neg-EE-1
Objetivo: 1. Causar Daño durante Ejecución del ***Proceso de Negocio Realizar Pedido***.
OR/AND 1. Atacar Entidades de Negocio.
OR/AND 1. Atacar Organización Proveedora.
AND/OR 1. Atacar Infraestructura Tecnológica.
AND/OR 1. Atacar Centro de Procesamiento de Datos.
2. Atacar Infraestructura Financiera.
...
3. Atacar Infraestructura Humana.
AND/OR 1. Atacar Personal Operativo con Misión Crítica.
AND/OR 1. Sobornar
2. Amenazar
...
2. Atacar Organización Minorista.
AND/OR 1. Atacar Infraestructura Tecnológica.
2. Atacar Infraestructura Financiera.
3. Atacar Infraestructura Humana.
2. Atacar Red.
OR/AND. 1. Atacar Red Organización Proveedora.
AND/OR 1. Atacar Proveedor de Servicios de Internet
2. Atacar Red Organización Minorista.
AND/OR 1. Atacar Proveedor de Servicios de Internet
3. Atacar Red Internet
AND/OR 1. Atacar DNS
...
3. Atacar Reglas de Negocio
OR /AND 1. Atacar Reglas de Negocio R1.
...
OR /AND 1. Atacar Reglas de Negocio Rn.
4. Atacar Interacciones.
OR/AND 1. Atacar Interacciones de Caso de Solicitar Stock.

Fig. 4. Árbol de Amenazas y Ataques asociado con el patrón de negocio para servicios web conocido como Empresa Extendida.

trazabilidad plena entre los WS funcionales, cuya seguridad está siendo analizada, y los requisitos de seguridad elicitados. Los artefactos principales, y los pasos en los que toman parte, se muestran en la Figura 2. En las siguientes secciones, comentaremos cada uno de estos artefactos y su papel en la actividad de elicitación.

3.2.1 Patrones de negocio y aplicación para WS

En [12], IBM presenta un catálogo de patrones, específicos para WS, clasificados como patrones de negocio, integración, aplicación, composición y tiempo de ejecución. Este catálogo de patrones basados en WS ofrece un espacio de soluciones de diseño completo para sistemas basados en este paradigma. En nuestro trabajo,

Árbol Abstracto de Ataque de Patrón de Aplicación de WS
ID: A3Ap-CED.
Objetivo: 1. Atacar Patrón de Aplicación Conexión Expuesta Directamente
AND/OR 1. Atacar Sistema
AND/OR 1. Atacar Agente Origen
2. Atacar Agente Destino
2. Atacar Zona
AND/OR 1. Atacar Zona Segura
2. Atacar Zona Desmilitarizada
3. Atacar Zona Entre Empresas
3. Atacar Reglas de Conexión.
AND/OR 1. Atacar Reglas de Conexión Tipo A
...
N. Atacar Reglas de Conexión Tipo N
4. Atacar Interacciones del Sistema
AND/OR 1. Atacar Interacción A.
AND/OR 1. Atacar Canal de Mensaje
AND/OR 1. Alteración de Mensaje.
2. Confidencialidad del Mensaje.
3. Mensajes falsificados.
4. Suplantación del principal.
5. Declaraciones forjadas.
6. Repetición de Partes del Mensaje
7. Repetición Completa del Mensaje.
8. Denegación de Servicio.
2. Atacar Acciones Desencadenadas.
AND/OR 1. Atacar Infraestructura Subyacente.
2. Atacar Interacción B.
AND/OR 1. Atacar Canal de Mensaje
AND/OR 1. Alteración de Mensaje.
2. Confidencialidad del Mensaje.
...
...
N. Atacar Interacción N
...

Fig. 5. Árbol de amenazas abstracto asociado al patrón de aplicación para servicios Web Conexión Expuesta Directamente

utilizamos estos patrones como una referencia para identificar el conjunto de potenciales amenazas que deben ser tenidas en cuenta durante la etapa de elicitación. Básicamente, estos patrones definen un conjunto de elementos así como las interacciones existentes entre ellos. Así, se pueden estudiar las posibles amenazas sobre estos elementos e interacciones desde el principio del diseño del sistema.

En primer lugar se identificará qué patrón de negocio para WS es acorde con la problemática propuesta y, de entre sus posibles patrones de aplicación, cuál se corresponde con la interacción bajo análisis. La idea es que, a partir de identificar el patrón de aplicación para WS en el fragmento funcional cuya seguridad está bajo análisis, seamos capaces de obtener de manera sistemática un conjunto de amenazas potenciales para nuestro sistema.

Tabla 1. Perfiles de ataque asociados con el patrón de aplicación específico para WS conocido como Conexión Expuesta Directamente.

Patrón de Negocio	Patrón de Aplicación	Elemento	Variación	Perfil de Ataque	ID
Empresa Extendida	Conexión Expuesta Directamente	Interacción	Variación basada en Mensaje	*Interacción WS basada en Mensaje sin Acuse de Recibo sobre Internet*	PAA-1-1
			Variación basada en Invocación	*Interacción WS basada en Mensaje con Acuse de Recibo sobre Internet*	PAA-1-2

Para cada patrón de negocio, y sus correspondientes patrones de aplicación, hemos definido un árbol de amenazas abstracto. El concepto de amenaza y ataque aplicado en nuestro estudio se basa en el Glosario de Internet (RFC 2828) [13].

3.2.2. Árbol de Amenazas/Ataque abstracto y concreto

Hemos adaptado los árboles de ataque, tal y como se definen en [14, 15] al contexto de la seguridad en sistemas basados en WS. Para cada patrón de negocio y aplicación para WS, hemos establecido una relación con un árbol de amenazas y ataque abstracto (AT). De esta forma, una vez se hayan identificado el patrón de negocio, y su correspondiente patrón de aplicación, y se hayan contextualizado para el problema bajo desarrollo, a continuación deberemos hacer lo mismo con sus árboles de amenazas asociados para obtener un árbol AT a nivel de negocio y una árbol AT a nivel de aplicación. Estos árboles identifican las amenazas a tener en cuenta sobre el fragmento de funcionalidad cuya seguridad está siendo analizada en la iteración actual. En la Figura 3, se muestra un ejemplo del árbol AT que hemos definido y asociado con el patrón de negocio conocido como Empresa Extendida (Extended Enterprise). En la Figura 4, se muestra un ejemplo (resumido por motivos de espacio) de la instanciación de dicho árbol AT. Este mismo proceso se sigue con el patrón de aplicación de forma que se obtiene el árbol AT concreto. En la Figura 5 se muestra el árbol AT abstracto asociado con el patrón de aplicación conocido como EmpresaExtendida::ConexiónExpuestaDirectamente.

La rama 1.1 del A3Ap-CED, denominada *Atacar Sistema* refinará la rama 1.1 *Atacar Entidad de Negocio* del A3Neg-EE, la 1.2 refinará la rama 1.2 del A3Neg-EE, y así sucesivamente. De esta forma, la rama 1.4 *Atacar Interacciones del [Caso de Uso de Negocio | Caso de Uso de Sistema]* del A3Neg-EE será refinada por la rama 1.4 *Atacar Interacciones del Sistema* del A3Ap-CED. El conjunto de amenazas que aparecen bajo las ramas 1.4.x.1 se han extraído de [16]. Tal y como se expresa en dicha fuente las amenazas contempladas pueden superponerse entre sí en cuanto a que el mismo ataque podría representar amenazas de varias categorías.

Tabla 2. Caso de mal uso abstracto 'Ataque a la Semántica del Mensaje SOAP'.

Nombre: Ataque a la Semántica del Mensaje SOAP [BASADO EN MENSAJE]	
ID: CMUA-1-1-1	
PROBABILIDAD: [ALTA | MEDIA | BAJA]	
Resumen: el tipo atacante [tipo de atacante] accede al mensaje [nombre mensaje] intercambiado por el agente [consumidor/proveedor][descubrimiento] [nombre agente] y el agente [consumidor/proveedor/descubrimiento] [nombre agente] y [modifica/elimina/inserta [parte]] el mensaje a nivel de la capa de [transporte / SOAP] obtenida en la [enhorno/corporativo] con el propósito de [objetivo].	
Precondiciones: 1) El atacante tiene acceso físico al mensaje. 2) El atacante tiene un conocimiento claro de la estructura y significado del mensaje.	
Interacciones del Agente Consumidor	Interacciones del Atacante	Interacciones del Agente Proveedor
El agente consumidor envía el mensaje [nombre mensaje]		
	El atacante [tipo de atacante] lo intercepta.	
	El atacante [tipo de atacante] identifica la parte a modificar y [elimina, reemplaza o agrega] información.	
	El atacante reenvía el mensaje al agente proveedor.	
		El agente proveedor recibe el mensaje y lo procesa de forma errónea en base a la semántica alterada.
Poscondiciones: 1) El sistema quedará en un estado erróneo con respecto a las intenciones originales del agente consumidor [nombre agente consumidor]. 2) En el registro del sistema sobre el que se ejecuta el agente proveedor [nombre de agente proveedor] aparecerá que la petición recibida fue aquella con la semántica alterada.		

Debemos destacar que gracias a esta adaptación de los árboles de ataque de Schneier con los patrones de negocio para WS estamos permitiendo que no sólo se consideren los aspectos de la seguridad de las interacciones entre los agentes WS en sí, sino que también consideramos posibles ataques a las organizaciones proveedoras y consumidoras de los servicios o a la infraestructura de Red empleada así como a otros elementos a nivel organizativo (y no sólo de sistema). Por ejemplo, en la Figura 4 se muestra cómo se podrían desarrollar hipotéticamente las ramas vinculadas con las amenazas dirigidas hacia las entidades que soportan el flujo de trabajo. Por tanto, desde nuestro trabajo incluimos el análisis del entorno organizacional en el que el sistema estará operativo tratando de ser consistentes con los marcos de trabajo de ingeniería de requisitos de seguridad modernos que analizan el aspecto social y organizacional del sistema como primer paso hacia la especificación de los requisitos (de seguridad) del sistema [17-21].

3.2.3 Identificación de los Ataques

El siguiente paso consistirá en refinar las hojas del árbol AT resultante de combinar los árboles de negocio y aplicación mediante la especificación de los ataques que consuman cada una de las amenazas. Las amenazas por sí mismas no son de gran relevancia si no existen ataques que las lleven a cabo. El siguiente paso será, por tanto, identificar el conjunto de potenciales ataques que podrían ocurrir para cada una de las amenazas contempladas. Para conseguir este objetivo, se ha hecho uso del concepto de perfil de ataque tal y como se describe en [15]. La única diferencia con respecto a este trabajo es que nosotros hemos optado, con respecto a la forma de especificar la secuencia de pasos que lleva a cabo el ataque, por los casos de mal uso [22, 23] (en [15] se describe una manera poco formal de definir los ataques).

Básicamente, un perfil de ataque contiene un conjunto de casos de mal uso abstractos que aplican a un modelo de referencia, que en este caso lo define el patrón de aplicación con el que se ha relacionado cada perfil de ataque definido. Cada patrón de aplicación para WS se ha relacionado con uno o más perfiles de ataque los cuales establecen el conjunto de potenciales ataques a los que se pueden ver sujetos. Por ejemplo, la Tabla 2 muestra, para el patrón de aplicación EmpresaExtendidad::ConexiónExpuestaDirectamente, el conjunto de perfiles de ataques que se han definido.

Cada perfil de ataque agrupa un conjunto de casos de mal uso abstractos que se centran en un elemento particular definido en el patrón de aplicación. En la Tabla 1, ambos perfiles de ataque están centrados en la interacción, es decir, los ataques que definen se centran en explotar cualquier vulnerabilidad que se puede deducir del análisis de los mensajes intercambiados en la interacción así como de su naturaleza (ej: patrón de mensajes empleado, síncrono vs. asíncrono, etc.).

En nuestro ejemplo, la interacción ProcesarPedido, sigue un patrón de intercambio de mensajes petición/respuesta. Estas son las variantes (tal y como se aplica este término en [15]) especificadas para este perfil:

- Organizaciones Proveedora y Consumidora de WS. En este caso de estudio, éstas son la organización Proveedora y la organización Minorista respectivamente.
- Agente Proveedor y Consumidor de WS. En nuestro caso de estudio, estos son los agentes WS-Proveedor y WS-Minorista, respectivamente.
- El nombre de la operación que debe llevar a cabo, en nuestro caso conocida como ProcesarPedido, la cual se corresponde con el patrón de intercambio de mensajes petición/respuesta tal y como se define en el estándar WSDL (Web Services Description Language) [24].
- Un conjunto de casos de mal uso que refinan las ramas 1.4.x.1.y de árbol AT de aplicación mostrado en la Figura 5.

Los casos de mal uso especifican los escenarios de ataque que materializan las amenazas con las que se encuentran asociados. Nuestro trabajo considera casos de mal uso abstractos y casos de mal uso concretos. Como hemos mencionado anteriormente, el primer tipo están agrupados en perfiles de ataques, mientras que los segundos son instancias de los primeros e indican la secuencia de pasos que lleva a cabo un atacante para cierto ataque. Hasta ahora, en nuestro trabajo hemos definido los siguientes casos de mal uso abstractos: i) caso de mal uso de **Ataque a la**

El [agente consumidor | agente proveedor | agente descubrimiento] [nombre agente] deberá proteger el mensaje [nombre del mensaje] a nivel de la capa de [transporte <protocolo>| mensaje SOAP | anexo SOAP] que transmite de posibles [modificaciones | eliminaciones | inserciones] sobre [partes del mensaje] que alteren su semántica debido a ataques [no sofisticados | semisofisticados | sofisticados] durante la ejecución de [interacción | caso de uso] con cierta [métrica]

Fig. 6. Plantilla de requisito de seguridad específico para WS.

Semántica del contenido SOAP (AMUC-1-1-1), el cual refina la amenaza representada por la rama 1.4.x.1.1 (Alteración del Mensaje) del patrón de aplicación Conexión Expuesta Directamente mostrada en la Figura 5; ii) caso de mal uso de **Ataque sobre la Confidencialidad de la Autenticidad del Mensaje SOAP** (AMUC-1-1-2), el cual refina la amenaza de las ramas 1.4.x.1.3, 1.4.x.1.4 y 1.4.x.1.5 del patrón de aplicación mencionado.

Finalmente, los posibles atacantes, actores primarios de los casos de mal uso señalados, son (tal cual está definido en el perfil de ataque): i) agente WS-Proveedor malicioso: el agente WS-Provider podría no comportarse como se espera realizando actividades ilícitas tal como la revelación de la identidad de los compradores para su propio beneficio (vender esta información, creando perfiles de compradores para personalizar ofertas, etc.); ii) agente WS Intermediario: en la arquitectura SOAP, sobre la que se basa los sistemas basados en servicios Web, aparece la figura de los nodos SOAP intermediarios capaces de procesar los mensajes durante su recorrido. Es posible, y permisible, que un agente emisor desconozca la existencia de este tipo de intermediarios en el camino de los mensajes que envía; iii) atacante externo: atacante situado en Internet capaz de llevar alguno de los ataques señalados. El riesgo de que exista este tipo de atacante es muy alto dado lo imprevisible e incontrolable de Internet. En la Tabla 2, se muestra un ejemplo de caso de mal uso abstracto. Como se puede apreciar, se encuentra altamente parametrizado siendo reutilizable y aplicable a cualquier sistema.

3.2.4 Especificación del Comportamiento de la Seguridad del Sistema

Cada caso de mal uso mantiene una relación con uno o más casos de uso de seguridad [25, 26]. Los casos de uso de seguridad definen una secuencia de pasos que permiten al sistema prevenir, detectar o reaccionar a cada uno de los ataques que tienen lugar en forma de una instancia de los casos de mal uso con los que están asociados.

3.2.5 Especificación de los Requisitos de Seguridad

Cada caso de uso de seguridad abstracto tiene asociado una o más plantillas de requisitos de seguridad para WS, las cuales serán instanciadas con el objetivo de obtener los requisitos de seguridad finales. En la Figura 6, se muestra un ejemplo de plantilla que define un requisito de seguridad genérico que resuelve la integridad de los mensajes incluidos en una o más interacciones. Esta plantilla está asociada con el caso de uso de seguridad mostrado en la Tabla 2.

Los pasos que se deben seguir cuando se instancian las plantillas de seguridad específicas para WS se pueden encontrar en [3].

4 Conclusiones y Trabajo Futuro

La seguridad es un aspecto crucial si los sistemas basados en WS se deben convertir en la solución por defecto para la integración entre sistemas heterogéneos [27].

En este artículo hemos presentado una visión general del proceso PWSSec. Luego, hemos centrado nuestra discusión en los artefactos reutilizables utilizados durante la actividad de elicitación de la etapa de requisitos de seguridad WSSecReq. La aplicación presentada de los artefactos permite a los desarrolladores realizar un análisis sistemático de seguridad para producir una especificación completa de los requisitos de seguridad específicos para WS. Además, todos estos artefactos utilizados durante la elicitación exponen una serie de asociaciones entre ellos que proporcionan una trazabilidad. Esta trazabilidad permite conocer qué requisitos de seguridad han sido derivados de qué fragmento de funcionalidad y viceversa. Esta trazabilidad conecta el fragmento de funcionalidad software cuya seguridad está bajo análisis con el conjunto de requisito de seguridad elicitados a través de un conjunto de artefactos de seguridad (árboles de amenazas y ataques, casos de mal uso, casos de uso de seguridad, etc.).

Algunas de líneas de investigación sobre las que estamos trabajando son:

- Definir y refinar los árboles de amenazas y ataques a nivel de negocio con el objetivo de obtener una visión de seguridad completa del problema. Este análisis está produciendo nuevos árboles de amenazas y ataque a nivel de negocio, perfiles de ataque de negocio, casos de mal uso de negocio, casos de uso de seguridad de negocio y plantillas de requisitos de seguridad de negocio.
- Analizar las potenciales relaciones que pueden existir entre las ramas definidas dentro y entre los árboles de amenazas y ataques definidos en los diferentes niveles de abstracción (ej: negocio, aplicación, composición, etc.).
- Definir una meta-modelo formal de los artefactos que haga posible crear un repositorio de artefactos reutilizables y desarrollar una herramienta que ofrezca un soporte basado en una herramienta durante la actividad de elicitación.
- Incorporar árboles de amenaza y ataque como resultado de tener en cuenta los patrones 'en tiempo de ejecución' para WS definidos por IBM en su catálogo.

5 Agradecimientos

Este trabajo es parte de los siguientes proyectos de investigación: Red RETISTIC (TIC2002-12487-E), de la Dirección General de Investigación del Ministerio de Ciencia y Tecnología, y DIMENSIONS (PBC-05-012-1), financiado por el FEDER y la Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha.

6 Referencias

1. CERT. Véase: http://www.cert.org.
2. Devanbu, P.T. and S. Stubblebine. *Software Engineering for Security: a Roadmap*, en *The Future of Software Engineering, Special Volume publicado conjuntamente con ICSE*. 2000. Limerick, Ireland.
3. Gutiérrez, C., E. Fernández-Medina, and M. Piattini. *PWSSec: Process for Web Services Security, IEEE International Conference on Web Services 2005*. 2005. Orlando, Florida, USA.
4. Boehm, B.W., *A Spiral Model of Software Development and Enhancement*. IEEE Computer, 1988: p. 61-72.
5. Breu, R., et al. *Key Issues of a Formally Based Process Model for Security Engineering, 16th International Conference on Software and Systems Engineering and their Applications (ICSSEA'03)*. 2003.
6. W3C, *Web Services Architecture*. 2004.
7. Cockburn, A., *Writing Effective Use Cases*. 1st ed. 2000: Addison-Wesley Pub Co. 270.
8. Deubler, M., et al. *Tool Supported Development of Service Based Systems*. in *11th Asia-Pacific Software Engineering Conference (APSEC 2004)*. 2004. Busan, Korea: IEEE Computer Society.
9. Firesmith, D.G., *Engineering Security Requirements*. Journal of Object Technology, 2003. **2**(1): p. 53-68.
10. Toval, A., et al., *Requirements Reuse for Improving Information Systems Security: A Practitioner's Approach*. Requirements Engineering Journal, 2001. **6**(4): p. 205-219.
11. Firesmith, D.G., *Specifying Reusable Security Requirements*. Journal of Object Technology, 2004. **3**(1): p. 61-75.
12. Endrei, M., et al., *Patterns: Service-Oriented Architecture and Web Services*. 2004. p. 345.
13. Shirey, R., *Internet Security Glossary (RFC 2828)*. 2000.
14. Schneier, B., *Attack Trees: Modeling Security Threats*. Dr. Dobb's Journal, 1999.
15. Moore, A.P., R.J. Ellison, and R.C. Linger, *Attack Modelling for Information Security and Survivability*, in *Survivable Systems*. 2001, Software Engineering Institute.
16. WS-I, *Security Challenges, Threats and Countermeasures Versión 1.0*. 2005, WS-I.
17. Yu, E.S.K., L. Liu, and J. Mylopoulos. *Analyzing Security Requirements As Relationships among Strategic Actors*. in *SREIS'02*. 2002. North Carolina.
18. Liu, L. and E. Yu. *From Requirements to Architectural Design - Using Goals and Scenarios*. in *ICSE-2001 Workshop From Software Requirements to Architectures (STRAW 2001)*. 2001. Toronto, Canada.
19. Liu, L., E. Yu, and J. Mylopoulus. *Security and Privacy Requirements Analysis within Social Setting*. in *11th IEEE International Requirements Engineering Conference*. 2003. Monterey Bay, CA, USA.

20. Bresciani, P., et al., *Tropos: Agent-Oriented Software Development Methodology*. Journal of Autonomous Agents and Multi-Agent System, 2004. **8**(3): p. 203-236.
21. Mouratidis, H., et al. *A Natural Extension of Tropos Methodology for Modelling Security*. in *Workshop on Agent-oriented methodologies, at OOPSLA 2002*. 2003. Seattle, WA, USA.
22. Alexander, I., *Misuse Cases: Use Cases with Hostile Intent*. IEEE Computer Software, 2003. **20**(1): p. 58-66.
23. Sindre, G. and A.L. Opdahl. *Eliciting Security Requirements with Misuse Cases*. in *TOOLS-37'00*. 2000. Sydney, Australia.
24. Christensen, E., et al., *W3C Web Services Description Language (WSDL) 1.1 - W3C Note 15 March 2001*. 2001.
25. Firesmith, D.G., *Security Use Cases*. Journal of Object Technology, 2003. **2**(3): p. 53-64.
26. Sindre, G., D.G. Firesmith, and A.L. Opdhal. *A Reuse-Based Approach to Determining Security Requirements*. in *9th International Workshop on Requirements Engineering: Foundation of Software Quality (REFSQ'03)*. 2003. Klangenfurt, Velden, Austria.
27. Zhang, J., *Trustworthy Web Services: Actions for Now*. IEEE IT Pro, 2005. **7**(1): p. 32-36.

Sesión 10

Modelos de Gestión de la Seguridad de la Información