NIHIL INTENTATUM

Universidad Católica de Salta

Papeles De Mar Del Plata

Anales del IV Congreso Iberoamericano de Seguridad Informática

Papeles De Mar Del Plata

Anales del IV Congreso Iberoamericano de Seguridad Informática

NIHIL INTENTATUM

Universidad Católica de Salta

PAPELES DE MAR DEL PLATA

ANALES DEL IV CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMÁTICA

COMPILADORES

Antonio Castro Lechtaler

Julio César Liporace

Jorge Ramió Aguirre

Universidad Católica de Salta

Salta

2007

Papeles de Mar del Plata: Actas del IV Congreso Iberoamericano de Seguridad Informática / Recopilado por Antonio Castro Lechtaler; Julio Cesar Liporace; Jorge Ramió Aguirre. - 1ª Ed. Salta: Universidad Católica de Salta - Eucasa, 2007.

606 p. ; 24 x 17 cm. (Anales Congreso)

ISBN 978-950-623-043-2

1. Seguridad Informática. I. Castro Lechtaler, Antonio, recop. II. Liporace, Julio Cesar, recop. III. Ramio Aguirre, Jorge, recop.

CDD 005.8

Campo Castañares, Salta, Provincia de Salta, (A4400EDD)
República Argentina
☎ + 54 - 387 – 426-8939 fax + 54 - 387 – 426-8800

ISBN: 978-950-623-043-2
Depósito legal: Argentina 2007

EDITOR: Sebastián Cañón, M.A.
PRODUCTOR: Cristian Cavaleiro
COMPOSICIÓN INTERIOR Y APOYO GRÁFICO: Señor Oscar Iturralde.

IMPRESO EN IMPRENTA DE DOCUPRINT S.A.
Rivadavia Nº 701, (C1002AAF).
Ciudad Autónoma de Buenos Aires, República Argentina.
☎ + 54 - 11 – 43 38 20 00 fax + 54 - 11 – 43 38 20 40

De esta edición se han impreso 300 ejemplares en el mes de noviembre de 2007.

PRINTED IN ARGENTINA - IMPRESO EN ARGENTINA

PAPELES DE MAR DEL PLATA

ANALES DEL IV CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMÁTICA

COMPILADORES

Antonio Castro Lechtaler
Julio César Liporace
Jorge Ramió Aguirre

Universidad Católica de Salta
Salta
2007

COMITÉ DE HONOR

PRESIDENTE: Dr. Néstor AUZA

Presidente de la Comisión de Investigaciones Científicas de la Provincia de Buenos Aires
y Rector de la Universidad Nacional del Centro de la Provincia de Buenos Aires.

MIEMBROS

Ing. Héctor Carlos BROTTO
Rector de la Universidad Tecnológica Nacional

Ing. Norberto CAMINOA
Rector de la Universidad Nacional de Chilecito

Dr. Alfredo Gustavo PUIG
Rector de la Universidad Católica de Salta

General Ingeniero Guillermo SEVILLA
Presidente de CITEFA (Instituto de Investigaciones Científicas y Técnicas de las Fuerzas Armadas)

Dr. Manuel Aguirre TELLEZ
Decano de la Facultad de Ciencias Exactas
Universidad Nacional del Centro de la Provincia de Buenos Aires

Coronel Ingeniero Gustavo LANDA
Director - Decano de la Escuela Superior Técnica/Facultad de Ingeniería
Universidad del Ejército

Lic. Jorge Luis CAJAL
Miembro del Directorio
Comisión de Investigaciones Científicas de la Provincia de Buenos Aires

Arq. Luis De MARCO
Decano de la Facultad Regional Buenos Aires
Universidad Tecnológica Nacional

Ing. Claudio MONDADA
Decano Facultad de Ingeniería
Universidad Católica de Salta

Dr. Hugo Daniel SCOLNIK
Universidad de Buenos Aires

COMITÉ ORGANIZADOR

Ing. Antonio Ricardo Castro Lechtaler, MSc
Presidente

Dr. Jorge Ramió Aguirre,
Vicepresidente y Presidente del Comité de Programa

Lic. Julio César Liporace, EspCyS
Vicepresidente Ejecutivo

Dr. Nelson Acosta,
Vicepresidente Coordinador Local

DIRECTORES DE ÁREAS

Lic. Jorge Zaccagnini,
Director de Comunicación Social y Prensa

Mag. Lic. Carlos Alberto López,
Director de Relaciones Institucionales

Lic. Carlos Tomassino,
Director de Relaciones con las Universidades

Ing. Hugo Ballesteros,
Director de Relaciones con los Institutos de Investigación

DIRECTORES LOCALES

Lic. Oscar Noguez
Director en Buenos Aires

Ing. Roberto Giordano Lerena,
Director en Mar del Plata

Dr. Carlos García Garino
Director en Mendoza

Lic. Javier Díaz,
Director en La Plata

Mag. Ing. Beatriz Parra de Gallo,
Directora en Salta

Ing. Fernanda Carmona,
Directora en La Rioja

COMITÉ DE PROGRAMA

Presidente
Dr. Jorge Ramió Aguirre,
Universidad Politécnica de Madrid, España

MSc. Nicolás César Alfonso Antezana Abarca
Universidad Católica San Pablo, Perú

Dr. Javier Areitio Bertolín
Universidad de Deusto, España

Dr. Walter Baluja García
Instituto Superior Politécnico José Antonio Echeverría, Cuba

Dr. Joan Borrel Viader
Universidad Autónoma de Barcelona, España

Dra. Pino Caballero Gil
Universidad de La Laguna, España

Dr. Josep Domingo i Ferrer
Universidad Rovira i Virgili, España

Dr. Jeimy José Cano Martínez
Universidad de los Andes, Colombia

Dr. Adriano Mauro Cansian
Universidade Estadual Paulista, Brasil

Dr. Hugo César Coyote Estrada
Instituto Politécnico Nacional, México

Dr. Ricardo Dahab
Universidade Estadual de Campinas, Brasil

Dr. Enrique Daltabuit Godas
Universidad Nacional Autónoma de México, México

Dr. Jorge Dávila Muro
Universidad Politécnica de Madrid, España

Dr. Jorge Estrada Sarlabous
Academia de Ciencias de Cuba, Cuba

Dr. Jose Luís Ferrer-Gomila
Universidad de Las Islas Baleares, España

COMITÉ CIENTÍFICO

Dr. Juan Pedro Hecht
Universidad de Buenos Aires, Argentina

Dr. Carlos Marcelo Sánchez
Universidad de Buenos Aires, Argentina

WORKSHOP EN TÉCNICAS DE HACKING Y FORENSIA INFORMÁTICA

Fecha: martes 27 de noviembre de 2007
Seminario práctico de 4 horas

Parte 1 (2 horas)

"Técnicas de Inyección en Hacking de Aplicaciones Web"

Ponente: Chema Alonso
Ingeniero y Dr. en Informática, a falta de la lectura de tesis en este año 2007. Es Microsoft MVP Windows Security desde Julio de 2004. Consultor de Seguridad Informática durante los últimos años. Ha participado en las últimas 7 giras de seguridad de Microsoft y los Security Days. Participa activamente con los cuerpos de seguridad del estado y realiza en Informática 64 test de intrusión para grandes compañías. Ponente en decenas de conferencias de seguridad al año.

Temario:

- Introducción a las técnicas de inyección.
- SQL injection, XPath injection, LDAP injection, HTML injection
- Análisis de exploits - Explotación mediante técnicas a ciegas
- Herramientas y caso práctico

Parte 2 (2 horas)

"Utilización de Patrones de Comportamiento en el Análisis Forense Informático"

Ponente: D. Julio César Ardita
Licenciado en Sistemas y Master en Gestión de las Telecomunicaciones. Es fundador del CISIar, Centro de Investigación en Seguridad Informática Argentina. Consultor de Seguridad Informática, es ponente invitado en decenas de congresos nacionales e internacionales. Desde Cybsec Security Systems S.A. es director de proyectos de investigación sobre sistemas de detección de intrusiones y penetration test, así como profesor en decenas de cursos de seguridad en Latinoamérica.

Temario:

- Características de los incidentes de seguridad internos
- Análisis forense informático
- Metodología de análisis de patrones de comportamiento del intruso
- Aplicación real y resultados obtenidos

PROGRAMA GENERAL ACADÉMICO

Lunes 26 de Noviembre (Sesiones Plenarias)	
10 hs - 11 hs	**11 hs - 12 hs**
Atacando RSA mediante un nuevo método de factorización de enteros	Seguridad y composición de protocolos criptográficos
Dr. Hugo Scolnik: Universidad de Buenos Aires, Argentina	**Dr. Alejandro Hevia; Universidad de Chile, Chile**

Martes 27 de Noviembre (Sesión Plenaria)
12:15 hs a 13:15 hs
Criptografía post-cuántica **Dr. Paulo Barreto; Universidad de Sao Paulo, Brasil**

Martes 27 de Noviembre (09:00 hs a 11:00 hs y 11:15 hs a 12:15 hs)	
Sala 1 (SESIÓN MM1)	**Sala 2 (SESIÓN MM2)**
Construcción de funciones Bent de n + 2 variables a partir de las funciones duales de funciones Bent de n variables. **Joan-Josep Climent, Francisco J. García, Verónica Requena (España)**	Medidas de Seguridad para ficheros no informatizados. **Javier Sempere Samaniego (España)**
Representation of Boolean maps through Hamiltonian paths. **Morales Luna, Rosaura Palma Orozco (México)**	Auditorias de Seguridad en Protección de Datos. **Ángel Igualada Menor (España)**
Performance Evaluation of Cryptographic Algorithms in JCOP41 Smart Card. **Matheus F. Oliveira, Marco A. A. Henriques (Brasil)**	Desarrollo y Mantenimiento Seguro de Software para Pymes: Moprosoft alineado a ISO/IEC 17799:2005. **Nancy Velásquez (Ecuador)**
Prediciendo secuencias producidas por un generador congruente lineal sobre curvas elípticas. **Jaime Gutiérrez, Álvar Ibeas (España)**	Hacia un Proceso sistemático para el desarrollo de sistemas Grid Seguros con Dispositivos Móviles **David G. Rosado, Javier López, Eduardo Fernández-Medina, Mario Piattini (España)**
Criptoanálisis del generador shrinking: una nueva propuesta basada en un time-memory trade-off. **M. E. Pazo-Robles, Amparo Fúster Sabater (Argentina)**	Construcción de un CMI de la Seguridad: Selección de indicadores mediante un sistema experto probabilística. **Daniel Villafranca, Luis Enrique Sánchez, Eduardo Fernández-Medina, Mario Piattini (España)**
StegSecret: una herramienta pública de estegoanálisis. **Alfonso Muñoz Muñoz, Justo Carracedo Gallardo (España)**	Concepción, Diseño e Implantación de un Laboratorio de Seguridad Informática **María Eugenia Corti, Marcelo Rodríguez, Gustavo Betarte (Uruguay)**

Martes 27 de Noviembre (14:30 hs a 16:30 hs y 16:45 hs a 17:45 hs)	
Sala 1 (SESIÓN MT1)	**Sala 2 (SESIÓN MT2)**
Autómatas celulares caóticos en la generación de funciones hash resistentes a los ataques de colisiones diferenciales. **Juan Pedro Hecht (Argentina)**	Buenas prácticas de elicitación de los requerimientos de seguridad. **Susana C. Romaniz (Argentina)**
A Signature Scheme based on Asymmetric Bilinear Pairing Functions. **Routo Terada, Denise H. Goya (Brasil)**	Evaluación de Riesgo en las Tecnologías de Información y Comunicaciones orientada a Organismos Públicos. **Pablo Andrés Pessolani (Argentina)**
A Class of Secret Sharing Schemes. **J.C. Ku, Horacio Tapia-Recillas (México)**	AUDISEG: Una metodología para la auditoría de la seguridad física del ambiente informático en el sector comercial. **Sandra Cristina Riascos, Juan Carlos Guerrero, Luís Byron Calvache, Jesús Eduardo Campaña (Colombia)**
Esquemas de reparto de secretos en términos de códigos producto. **Policarpo Abascal, Juan Tena (España)**	La Universidad Simón Bolivar a la luz de los controles de seguridad de las ISO - 17799/27001. **Vidalina De Freitas (Venezuela)**
Evitando el Replay attack en Protocolos de Intercambio Equitativo con Requisitos de Privacidad. **M. Magdalena Payeras-Capellà, Macià Mut-Puigserver, Llorenç Huguet-Rotger, Josep Lluís Ferrer-Gomila (España)**	Revisión sistemática y comparación de ontologías en el marco de la seguridad. **Carlos Blanco, Joaquín Lasheras, Rafael Valencia-García, Eduardo Fernández-Medina, Ambrosio Toval, Mario Piattini (España)**
Vulnerabilidad a un Ataque de Repetición en un Protocolo de Seguridad. **Macià Mut-Puigserver, Josep Lluís Ferrer-Gomila, Magdalena Payeras-Capellà, Llorenç Huguet-Rotger (España)**	

Miércoles 28 de Noviembre (09:00 hs a 11:00 hs y 11:15 hs a 13:15 hs)	
Sala 1 (SESIÓN XM1)	**Sala 2 (SESIÓN XM2)**
Análisis de las medidas de distancia entre sesiones para la clasificación de intrusos. **Sebastián García (Argentina)**	Análisis de la Seguridad en Ecosistemas de Ambiente Inteligente. **Juan J. Ortega, Antonio Maña, Antonio Muñoz, Alejandro Gómez(España)**
NCD Based Masquerader Detection Using Enriched Command Lines. **Maximiliano Bertacchini, Carlos E. Benitez (Argentina)**	Nuevas Tendencia en Fraude electrónico. Relación entre malware y criptografía. **Delgado, José María Cámara (España)**
Metodología para la Evaluación de la Seguridad de Aplicaciones Web frente a Ataques Blind SQL Injection. **Chema Alonso, Rodolfo Bordón, Marta Beltrán, Antonio Guzmán (España)**	Sistema de identificación biométrica mediante patrón de iris utilizando operadores morfológicos y representación multiescala. **Alberto de Santos Sierra, Carmen Sánchez Ávila, Raúl Sánchez Reíllo (España)**
w3af – Web Application Attack and Audit Framework. **Andrés Riancho (Argentina)**	Attacking the Giants: Exploiting SAP Internals. **Mariano Nuñez Di Croce (Argentina)**
Transacciones Seguras para Sistemas Móviles por medio de Relaciones de Confianza. **Chadwick Carreto Arellano, Rolando Menchaca Garcia, Rolando Menchaca Méndez (México)**	Implementación de una Interfaz de Administración para Java Cards. **Luis Adrián Lizama Pérez, Roberto León Oramas, Tirso Alejandro (México)**
Técnicas antiforenses: Ocultando información en HFS+. **Carlos Enrique Nieto Lara (Colombia)**	Message-embedding from a control-theoretical point of view. **Gilles Millérioux, José María Amigó, Jamal Daafouz (España)**
Servicio de No Repudio para Marketing y Comercio basados en Servicios de Localización. **Benjamín Ramos, Ana I. González-Tablas, Arturo Ribagorda, Daniel Garzón (España)**	

Miércoles 28 de Noviembre (14:30 hs a 16:30 hs)	
Sala 1 (SESIÓN XT1)	**Sala 2 (SESIÓN XT2)**
Analysis of security protocol MiniSec for Wireless Sensor Networks. **Llanos Tobarra, Diego Cazorla, Fernando Cuartero (España)**	Arquitectura Estándar para Identificación Digital. **Chadwick Carreto Arellano, Rolando Menchaca García, Jesús Martínez Castro (México)**
Análisis Forense de Equipos de Telefonía Celular. **Rubén Vázquez-Medina, Lucio Santes-Galván, Alberto Ramos Toxtle (México)**	Performance issues to consider when applying Digital Signature in XML documents. **Eduardo Esteban Casanovas, Marcelo da Cruz Pinto (Argentina)**
SCMM-TOOL: Desarrollando una herramienta para gestionar la seguridad de los sistemas de información en las PYMES basada en Esquemas predefinidos **Luís Enrique Sánchez, Daniel Villafranca, Antonio Santos-Olmo, Eduardo Fernández-Medina, Mario Piattini (España)**	VALI - Herramienta de correlación de mensajes de bitácoras basada en relojes vectoriales. **Roberto Gómez, Julio César Rojas, Erika Mata (México)**
OTPM: Utilización del teléfono móvil como token de autenticación en servicios de banca electrónica. **Jorge Munilla, Alberto Peinado, Bernardo Quintero, Javier Téllez (España)**	Una propuesta de Autenticación Unificada Basada en la Sincronización de LDAP con Microsoft Active Directory. **Federico Herman Lutz, Sebastián Azubel (Argentina)**

Señores Congresales del IV Congreso Iberoamericano de Seguridad Informática.

Para la Universidad Católica de Salta es un gran honor haber sido invitada a publicar, a través de su fondo editorial, estos Papeles de Mar del Plata – Actas del IV Congreso Iberoamericano de Seguridad Informática, resultado del Congreso Internacional que se realizará del 25 al 28 de noviembre de 2007 en nuestro país con ese nombre.

Los 48 trabajos que aquí se presentan, aprobados por un Comité de Expertos Internacional de muy alto nivel profesional que hoy se ponen a consideración de la comunidad de investigadores de Iberoamérica y del mundo entero, representan una importante contribución al desarrollo de la criptografía y la seguridad informática. Estamos por ello seguros, que serán sin duda de gran valor para aquellos que trabaja en estas temáticas.

Nuestra Universidad, a través de su Facultad de Ingeniería, ha dado una importante prioridad a la enseñanza e investigación en las áreas de la informática y las telecomunicaciones, carreras que se dictan en ella al más alto nivel, con destacados profesionales que participarán de este significativo evento.

Deseamos entonces, darles la bienvenida a las personalidades extranjeras que hoy nos visitan, como así también a los numerosos colegas de nuestro país. A todos ellos, nuestros más afectuosos saludos. Son bienvenidos en nuestra patria.

Salta, noviembre de 2007

Dr. ALFREDO GUSTAVO PUIG
Rector
Universidad Católica de Salta

PROLOGO DE LA COMISIÓN ORGANIZADORA

Estimados Colegas,

A fines del año 2006, cuando Jorge Ramió Aguirre concurría a dictar un curso de postgrado en la Especialización en Criptografía y Seguridad Teleinformática que se dicta todos los años en la Escuela Superior Técnica de la Universidad del Ejercito desde el año 2002, nos convocó y entusiasmó a los que en la República Argentina estamos de alguna manera vinculados a la Criptografía y a la Seguridad a organizar el IV Congreso Iberoamericano que se viene haciendo con singular éxito.

A partir de allí, hemos tratado de ir armando el Congreso del que a partir de hoy ustedes podrán participar en esta ciudad de Mar del Plata. Esperamos que ella, les resulte grata y acogedora.

Como ocurre en estos casos, no han sido pocos los problemas que hemos debido ir superando para llegar a esta fecha. Y son varias las Instituciones a las que les debemos nuestro agradeciendo por su colaboración recibida desde el primer momento que les planteamos la realización de este evento.

En primer lugar, a la Comisión de Investigaciones Cientificas de la Provincia de Buenos Aires como Institución, y en particular a su Presidente y Rector de la Universidad Nacional del Centro de la Provincia de Buenos Aires Dr. Néstor Auza quien fue el primero en brindarnos su sincero apoyo. También a todos aquellos que forman parte de la Comisión de Honor, que de alguna manera han colaborado a que este Congreso esté siendo inaugurado, en particular a las autoridades nacionales y universitarias a las que estamos muy agradecidos.

En ésta como en toda reunión científica, sus objetivos se enfocan para observar hacia donde se dirige el estado del arte de la actividad en particular, y para convocar a los expertos a un intercambio de reflexiones que permitan avizorar -en singular oportunidad- los nuevos desafíos.

No dudamos que el primero se ha cumplido. El numeroso conjunto de ponencias aprobadas con referato internacional así lo prueba. El segundo seguramente será también una realidad porque esta disciplina ya dejó de ser parte de otras disciplinas, para ocupar un lugar propio manejado por verdaderos profesionales en las temáticas.

Esperemos que estos Papeles de Mar del Plata sean una guia para aquellos que trabajan e investigan en estas ciencias con el objeto de correr cada día más las fronteras del conocimiento.

Mar del Plata, noviembre de 2007

Lic. JULIO CÉSAR LIPORACE, EspCySeg.
Vicepresidente Ejecutivo
Comité Organizador
IV Congreso Iberoamericano de Seguridad Informática

Prof. Ing. ANTONIO CASTRO LECHTALER, MSc
Presidente
Comité Organizador
IV Congreso Iberoamericano de Seguridad Informática

PRÓLOGO DEL COORDINADOR DE LA RED TEMÁTICA CRIPTORED

Estimados compañeros:

Por cuarta vez nos juntamos como cada dos años en este espacio académico y de investigación propuesto por la Red Temática CriptoRed, y que hemos denominado Congreso Iberoamericano de Seguridad Informática CIBSI, para hacer un repaso del estado del arte en las materias propias de la seguridad de la información, evento que dentro de Iberoamérica congrega al mayor número de representantes y expertos en seguridad informática de los países que la conforman: Latinoamérica, Portugal y España.

CIBSI 2007 cuenta con la especial acogida de la Universidad del Centro de la Provincia de Buenos Aires, quien organiza este congreso conjuntamente con la Universidad Politécnica de Madrid, a cuyos directivos así como a todos y cada uno de los miembros del Comité Organizador deseo agradecer desde estas páginas su buen hacer y la excelente hospitalidad que nos brindan a todos los asistentes.

De 69 trabajos recibidos, un selecto grupo de 43 expertos de 13 países (Argentina, Brasil, Chile, Colombia, Cuba, Ecuador, España, México, Panamá, Perú, Portugal, Venezuela y Uruguay) ha seleccionado 48 documentos, de los que al final se presentan en este evento 43, y que proceden de investigadores de Argentina, Brasil, Colombia, Ecuador, España, México, Uruguay y Venezuela.

Así mismo, el congreso cuenta con tres conferenciantes invitados a sesiones plenarias, el Dr. Paulo Barreto de Brasil, el Dr. Alejandro Hevia de Chile y el Dr. Hugo Scolnik de Argentina, y se impartirá de forma simultánea un Workshop sobre Técnicas de Hacking y Forensia Informática, a cargo de los expertos D. Julio César Ardita de Argentina y D. José María Alonso de España.

Ya van quedando para el histórico aquellos gratos recuerdos de las ediciones de Morelia en 2002 y en el DF en 2003, ambos en México, así como el de Valparaíso en Chile en 2005, observando que en cada edición aumenta la cantidad de los trabajos presentados, participan más países y más grupos de investigación, lo que permite augurar excelentes expectativas de crecimiento para las futuras ediciones de CIBSI en el año 2009 y siguientes.

Como coordinador de CriptoRed, comunidad virtual de expertos en seguridad de la información con más de 650 miembros de 185 universidades y 240 empresas, que son el verdadero motor de este congreso, sólo puedo reiterar mis agradecimientos a todos, organizadores, autores, revisores, patrocinadores y asistentes, por permitir que este gran esfuerzo que todos hemos realizado se convierta nuevamente en una realidad, esta vez ante el marco excepcional de la hermosa ciudad de Mar del Plata y en un bello país de paisajes y gentes, Argentina.

A todos, un caluroso abrazo con todo mi afecto.

Mar del Plata, noviembre de 2007

Dr. JORGE RAMIÓ AGUIRRE
Coordinador de CriptoRed

Presidente
Comité de Programa
IV Congreso Iberoamericano de Seguridad Informática

INDICE

Hacia un Proceso sistemático para el desarrollo de sistemas Grid Seguros con Dispositivos Móviles

David G. Rosado[1], Javier López[2], Eduardo Fernández-Medina[1], Mario Piattini[1]

(1) Grupo ALARCOS, Departamento de Tecnologías y Sistemas de Información
Centro Mixto de Investigación y Desarrollo de Software UCLM-Indra
Universidad de Castilla-La Mancha. Paseo de la Universidad, 4–13071 Ciudad Real, España
{David.GRosado, Eduardo.Fdez-Medina,Mario.Piattini}@uclm.es
(2) Departamento de Lenguajes y Ciencias de la Computación
Universidad de Málaga, 29071 – Málaga, España
jlm@lcc.uma.es

Resumen. A lo largo de la historia, muchos desarrollos científicos y tecnológicos han surgido como respuesta a alguna necesidad, como la de compartir los recursos, almacenar y analizar grandes cantidades de datos, aunado al hecho de que los usuarios y las instituciones están distribuidos geográficamente. Para dar una solución a estas necesidades han surgido los Grids Computacionales. Además, con el desarrollo de la tecnología inalámbrica y los dispositivos móviles, el Grid se convierte en el candidato perfecto para que los usuarios móviles puedan realizar trabajos complejos, a la vez que añaden nueva capacidad computacional al Grid. La seguridad en estos sistemas, por su naturaleza distribuida y abierta, cobra gran importancia. Existe una infraestructura que es capaz de aportar mecanismos y servicios de seguridad a los sistemas grid (GSI), lo que hace falta es una metodología que indique la forma de hacerlo, es decir, un proceso de ingeniería que defina los pasos a seguir para que, partiendo de unas necesidades a resolver, podamos diseñar y construir un sistema Grid seguro con soporte para dispositivos móviles que sea capaz de resolver y cubrir dichas necesidades. Esa es la propuesta de este trabajo, definir una metodología de desarrollo para sistemas Grid seguros con dispositivos móviles.

Palabras claves: Grid, Seguridad, Arquitectura de Seguridad, dispositivos móviles, proceso de desarrollo seguro.

1 Introducción

La idea del Grid está enfocada fundamentalmente en el acceso remoto a recursos computacionales, solventando el problema de coordinar los recursos compartidos entre las organizaciones virtuales multi-institucionales y dinámicas. Cuando se habla de compartir, no es sólo el intercambio de ficheros, sino también el acceso directo a las computadoras, software, datos y otros recursos que son requeridos por múltiples aplicaciones en los campos de la industria, ciencia e ingeniería [1]. Para poder compartir de forma controlada, es necesario definir lo que se quiere compartir, a quién

se le permite compartir y bajo qué condiciones se comparte. El conjunto de instituciones y usuarios que comparten estos recursos y se someten a unas reglas forman lo que llamamos organización virtual (Virtual Organization, VO). Las infraestructuras que soportan la creación y operación de VOs son a menudo llamadas Grids [2].

Mientras que la estabilidad, rendimiento y heterogeneidad son metas deseables para cualquier sistema distribuido, las características de la computación Grid conducen a problemas de seguridad que no son tratados por las tecnologías Grid existentes para sistemas distribuidos [3][4]. La seguridad es una cuestión de gran importancia en estos sistemas debido a que se comparten recursos entre organizaciones, recursos costosos, que pueden ir desde computadores y otras facilidades hardware, o ficheros de datos potencialmente valiosos, sensibles y confidenciales. Por tanto, debe haber mecanismos y políticas de seguridad en el Grid que se encarguen de comprobar que sólo los usuarios que están autorizados, tengan acceso a los recursos proporcionados por el Grid [5][6][7].

Para alcanzar estos propósitos, se desarrolló el Globus Toolkit [8] por la comunidad Grid y es actualmente la infraestructura grid más utilizada. Dentro de Globus Toolkit, existe una parte dedicada a la seguridad, la Infraestructura de Seguridad Grid (GSI) [9][10], que es el estándar de seguridad *de facto* en la comunidad grid, el cual proporciona propiedades de seguridad básicas como es la autenticación, autorización y confidencialidad.

Existen ciertas investigaciones en el campo de los dispositivos móviles dentro de entornos Grid [11][12][13][14][15], que plantean el problema y la dificultad de incorporar, a los sistemas Grid existentes, dispositivos y terminales móviles que puedan consumir servicios y compartir sus recursos, con la peculiaridad de que son dispositivos flexibles, heterogéneos y limitados, que hacen más difícil la incorporación en una plataforma fija.

Por otra parte, un sistema Grid es un software que ha sido desarrollado mediante cierta tecnología y que cumple con una serie de características y funcionalidades propias del Grid. Como software que es, el problema que surge y el que ha dado lugar a numerosas investigaciones en los últimos años, es el de considerar e integrar la Seguridad dentro de todo el ciclo de vida del software [16][17]. Si le añadimos además la aparición de una nueva tecnología donde la seguridad es primordial y el avance que está teniendo en los últimos años la computación **móvil**, aparece la necesidad de definir, considerar y desarrollar una metodología o proceso de desarrollo que, desde el estado inicial hasta el estado final, se analicen e integren todos los requisitos relacionados con los sistemas Grid, donde además, se analicen los aspectos de seguridad necesarios para estos sistemas, y se analice la forma de incorporar los dispositivos móviles en estos sistemas. Este proceso debe facilitar a los desarrolladores el análisis y caracterización de todas las necesidades funcionales y de seguridad durante todas las etapas del ciclo de desarrollo del software basado en tecnología Grid y que de soporte a los dispositivos móviles.

Lo que se pretende en este artículo es empezar a construir los cimientos de un proceso o metodología ordenada de desarrollo sistemático que sirva de guía para el desarrollo de cualquier sistema Grid con dispositivos móviles, considerando todos los aspectos de seguridad durante todas las fases de desarrollo, obteniendo como resultado un sistema Grid seguro, robusto y escalable. Este proceso debe ser

independiente de la tecnología Grid a utilizar, obteniendo métodos, modelos y arquitecturas que, posteriormente, podrán ser implementadas en las distintas tecnologías existentes. Todos estos modelos, métodos y arquitecturas deben ser escalables, flexibles y dinámicas por la naturaleza dinámica del Grid y por las limitaciones de los dispositivos móviles, donde continuamente cambian las necesidades de recursos, políticas de seguridad, miembros, conexiones, etc., de tal forma que las modificaciones en el ciclo de desarrollo grid sea sencillo y controlado.

En la siguiente sección se definirá todo lo relacionado con la tecnología Grid, arquitectura del Grid, modelo estándar y las distintas aplicaciones Grid existentes. En la sección 3 se hablará de las ventajas e inconvenientes de los dispositivos móviles y su incorporación en el Grid. En la sección 4 se estudiará la tecnología de desarrollo más ampliamente utilizada, el Globus Toolkit y se describirá brevemente la infraestructura de seguridad GSI. La sección 5 es el aporte principal al artículo, y se verá la propuesta inicial del proceso de desarrollo sistemático para construir un sistema Grid seguro que de soporte a los dispositivos móviles. Se definirán las principales etapas del proceso de forma general, con esquemas del proceso y se identificarán el trabajo principal que se realizará en cada etapa, dejando un estudio más detallado para posteriores trabajos. Terminaremos con las conclusiones y daremos algunas líneas de nuestro trabajo futuro.

2 Computación Grid

La tecnología Grid surge del nuevo paradigma de computación distribuida propuesto por Ian Foster y Carl Kesselman a mediados de los 90. El objetivo de la tecnología Grid es permitir gestionar y distribuir la potencia de cálculo disponible, de tal forma que los usuarios se beneficien de la potencia de ordenadores ociosos que se encuentran dispersos geográficamente y conectados mediante una red de alta velocidad. La tecnología grid es una tecnología relativamente nueva, que está en fase de desarrollo y explotación.

2.1 Arquitectura Grid

La idea de Grid [1] es que sean arquitecturas fiables, consistentes y accesibles. Por ello, cinco características indispensables están presentes en ellas: uniformidad, transparencia, fiabilidad, ubicuidad y seguridad. Principalmente, la arquitectura propuesta es una arquitectura de protocolos que definen los mecanismos básicos que permiten a los usuarios y a los recursos negociar, establecer, gestionar y explotar la forma de compartir recursos. Una arquitectura abierta basada en un estándar facilita la extensibilidad, la interoperabilidad, la portabilidad y el compartir código. De esta manera la estandarización de los protocolos permitirá estandarizar los servicios y mejorar las capacidades del grid.

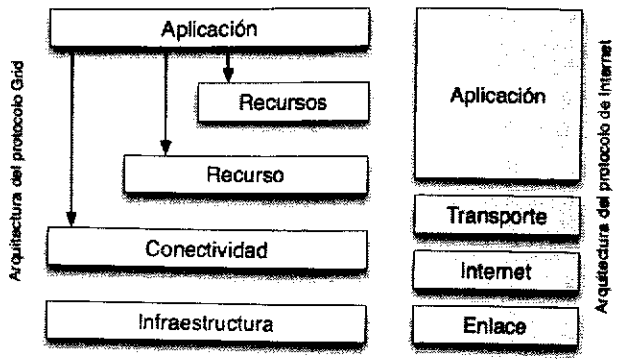

Fig. 1. Arquitectura Grid por capas. Capa Infraestructura, capa de Conectividad, capa de Recurso, capa de Recursos o Colectiva y capa de Aplicación.

La figura 1 muestra una clasificación por capas de la arquitectura Grid. En la capa *Infraestructura*, tenemos los recursos que deseamos compartir: computadores, sistemas de almacenamiento, bases de datos, etc., junto con la infraestructura de red y sus mecanismos de gestión y control. La capa *Conectividad* proporciona los servicios de comunicación y autenticación necesarios para comunicarse con los recursos. En la capa *Recurso* se encuentran los protocolos que permiten obtener la información de un recurso en particular y gestionarlo, controlando el acceso, arranque de procesos, gestión, monitorización y auditoria. La capa *Recursos* o Colectiva contiene los protocolos y servicios que permiten gestionar la interacción de un conjunto de recursos. En la capa *Aplicación* se encuentran definidos los protocolos que permiten el acceso a la estructura Grid. Otros artículos presentan los componentes necesarios de una arquitectura Grid [1] y los servicios adicionales requeridos dentro de una arquitectura Grid de datos [18].

2.2 Open Grid Services Architecture (OGSA)

El GGF (Global Grid Forum) [19] ha adoptado una arquitectura abierta de servicios Grid (OGSA) [20] como el modelo para la computación grid basada en estándares. Representa una evolución hacia una arquitectura del sistema Grid basada en conceptos y tecnologías de los servicios Web. Con el término "*arquitectura*" se denota un conjunto de interfaces básicas bien definidas desde las cuales se pueden construir sistemas interesantes, y "*abierto*" significa que es utilizado para comunicar extensibilidad, y al proceso usado para desarrollar estándares que alcancen la interoperabilidad.

La Arquitectura de Servicios Abiertos Grid (OGSA) presenta un conjunto de especificaciones y estándares que combina los beneficios de la informática Grid y los servicios web. Así, los clientes pueden, por primera vez, compartir y acceder a los recursos informáticos que necesitan en Internet, contando con el soporte de una infraestructura muy resistente, con capacidad de autogestión y siempre disponible; pueden integrar aplicaciones y compartir datos y potencia de procesado, consiguiendo unos niveles de eficiencia muy altos, así como muy bajos costos.

2.3 Aplicaciones de la computación Grid

Considerando las necesidades de cálculo, el espacio para el almacenamiento de los datos y el tiempo de respuesta de los sistemas Grid, Foster y Kesselam [2] definen 5 grandes áreas de trabajo que son:

- **Supercomputación distribuida**. Aquellas aplicaciones cuyas necesidades, que se producen en instantes de tiempo determinados y consumen muchos recursos, son imposible satisfacer en un único nodo. Ejemplos: simulaciones, herramientas de cálculo numérico, procesos de análisis de datos, etc.
- **Sistemas distribuidos en tiempo real**. Aplicaciones que generan un flujo de datos a alta velocidad que debe ser analizado y procesado en tiempo real. Ejemplos: experimentos de física de alta energía, control remoto de equipos médicos de alta precisión y precio, procesos de la denominada e-Medicine, etc.
- **Proceso intensivo de datos**. Aquellas aplicaciones que hacen un uso intensivo del espacio de almacenamiento. Ejemplos: sistemas gestores de bases de datos distribuidas.
- **Servicios puntuales**. En esta área, nos olvidamos del concepto de potencia de cálculo y capacidad de almacenamiento para centrarnos en recursos que una organización puede considerar como no necesarios. De esta manera el grid ofrece a la organización esos recursos sin que la organización deba desarrollarlos por si misma. Ejemplos: equipos costosos de medida o de análisis de muestras.
- **Entornos virtuales de colaboración**. Esta área está relacionada directamente con el concepto de Teleinmersión, de manera que se utilizan los enormes recursos computacionales del grid y su naturaleza distribuida para generar entornos virtuales 3D distribuidos.

3 Dispositivos móviles en el Grid

El interés de incorporar dispositivos móviles a los sistemas Grid es para enriquecer tanto a los usuarios de estos dispositivos como a la propia infraestructura Grid. El beneficio es bilateral, el Grid ofrece sus servicios a los usuarios móviles para completar sus trabajos de forma rápida y sencilla, y los dispositivos móviles ofrecen sus limitados recursos, pero millones de ellos, en cualquier lugar y en cualquier momento, respaldados por el rápido avance en el rendimiento y capacidad que se está llevando a cabo en la tecnología móvil.

En la actualidad, el desarrollo de la tecnología wireless y los dispositivos móviles nos permiten acceder al servicio de red desde cualquier lugar en cualquier momento. Aunque los dispositivos móviles promueven la comunicación móvil y el uso flexible, todavía traen problemas tales como calidad imprevisible de la red, baja confianza, recursos limitados (energía, ancho de banda, etc.) y períodos de desconexiones [21]. Puesto que los dispositivos móviles tienen la capacidad de computación limitada, el Grid se convierte en un importante proveedor de servicio de computación permitiendo que el usuario móvil realice trabajos complicados [22]. Por otra parte, el rendimiento de los dispositivos móviles actuales está aumentado significativamente, por lo que las

computadoras portátiles y PDAs pueden proporcionar capacidad de cómputo agregada al Grid cuando están conectadas a la red., formando un Grid in situ. Esta capacidad puede aventajar el uso de las aplicaciones grid incluso en lugares donde esto sería imaginario.

Uno de los principales problemas que tienen las tecnologías wireless es que el ancho de banda son varios órdenes de magnitud más baja que en las redes conectadas, y la pérdida de señal es más frecuente y el nivel de ruido está influenciado por las condiciones externas. Un segundo aspecto a tener en cuenta es que los dispositivos móviles tienen escasos recursos en términos de CPU, RAM, visualización, almacenaje, y son equipados con pequeñas baterías que limitan la potencia de consumo y afecta tanto a la transmisión wireless y al acceso a servicios que requieren una alta carga computacional. Finalmente, un tercer aspecto a considerar es la movilidad del usuario que causa problemas de perdida de señal durante el movimiento y a la necesidad de adaptar los servicios a la posición real del usuario.

En entornos móviles el contexto es dinámico y no puede ser manejado por suposiciones a priori. Es por ello que estos sistemas Grids tienen que proporcionar el soporte móvil necesario para poder manejar todas las cuestiones relacionadas con los entornos móviles. Habría que identificar una serie de servicios que ayuden al manejo de estos entornos, tal como descubrimiento de servicio, QoS, adaptación del servicio, balance de carga, etc.

En un entorno de computación móvil típico, una o más de las transacciones están basadas en algún dispositivo de computación wireless. Sin embargo, la seguridad en una plataforma móvil es más crítica debido a la naturaleza abierta de las redes wireless. Además, la seguridad es más difícil de implementar en una plataforma móvil debido a las limitaciones de recursos en estos dispositivos. Por tanto, una infraestructura Grid que soporte la participación de nodos móviles jugará un papel significante en el desarrollo de la computación Grid.

4 Tecnología para el desarrollo Grid

El incremento de popularidad e importancia de la computación Grid en campos científicos e industriales, ha motivado una serie de investigaciones e iniciativas de desarrollo en sistemas de computación Grid. El proyecto Globus [9] es uno de los más importantes esfuerzos en la comunidad Grid para desarrollar una infraestructura y herramientas que faciliten el desarrollo de aplicaciones Grids [23].

El programa genera software de código abierto que se utiliza en producción de actividades científicas, de ingeniería y comerciales. La herramienta principal generada por Globus Alliance es el Globus Toolkit [8], que es una colección de componentes software que ofrecen la infraestructura básica necesaria para la creación y ejecución de aplicaciones distribuidas, así como para la construcción de Grids. Este conjunto de componentes o herramientas provee soluciones para la seguridad, obtención de información, gestión de recursos, gestión de datos, comunicación, detección de fallos y portabilidad.

Actualmente, Globus se ha convertido en el estándar de facto para la computación en Grid. Globus consta de cuatro componentes fundamentales (ver fig. 2): Gestión o manejo de recursos (GRAM), Servicios de información (MDS), Gestión o manejo de datos (GridFTP) y una infraestructura de seguridad Grid (GSI).

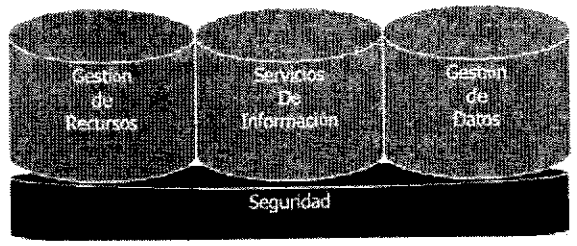

Fig. 2. Componentes del Globus Toolkit: Gestión de Recursos, Servicios de Información, Gestión de Datos y Seguridad.

El servicio administrador y localizador de recursos Grid (GRAM) provee una simple interfaz para el requerimiento y uso de sistemas de recursos remotos para la ejecución de trabajos. Está diseñado para proveer una flexible interfaz a sistemas de planificación de trabajos. El sistema de monitoreo y descubrimiento (MDS) es el componente de servicio de información de Globus Toolkit y provee información sobre recursos disponibles sobre la Grid y su estado. GridFTP es protocolo de alto rendimiento, seguridad, confiabilidad de transferencia de datos optimizado para importantes anchos de banda en redes de extensión amplia. La infraestructura de seguridad Grid (GSI) permite autenticación y comunicación segura sobre una red de trabajo, que se describe a continuación.

4.1 Infraestructura de Seguridad Grid

La infraestructura software de seguridad Grid (GSI) es un conjunto de librerías y herramientas que permiten que un usuario pueda acceder a los recursos de forma segura. GSI ha emergido como un componente middleware esencial que ha sido integrado en muchas herramientas y consta de un conjunto de interfaces y protocolos. Define un formato de credencial común basado en certificados de identidad X.509 [24] y un protocolo común basado en seguridad de capa de transporte (TLS, SSL). Los mensajes seguros pueden ser transportados, entendidos y manipulados por herramientas y software estándares de servicios Web [3][4][25]. Pero estas tecnologías todavía no pueden satisfacer toda la seguridad que necesitan los usuarios en este ambiente dinámico abierto. El sistema Grid requiere funciones de seguridad estándar, incluyendo confidencialidad, integridad, privacidad, autenticación y no repudio [3][4].

5 Hacia un proceso para el desarrollo sistemático de sistemas Grid seguros con dispositivos móviles.

Lo que se pretende es proveer al desarrollador de una metodología o proceso sistemático de desarrollo que abarcará el desarrollo completo de sistemas Grid sea cual sea su complejidad y magnitud, donde se definan modelos, procesos, métodos, mecanismos, técnicas, herramientas, soporte documental, y se defina una arquitectura que ayude a desarrollar un sistema Grid seguro que de soporte a dispositivos móviles, que partiendo de las necesidades o requisitos del sistema inicial nos lleve al diseño e implementación de un sistema Grid seguro de forma ordenada y sistemática.

Este proceso sistemático de ingeniería se enfrentará principalmente a dos grandes retos: por un lado establecer una metodología para el desarrollo seguro de los sistemas Grid, no sólo teniendo en cuenta las necesidades funcionales, sino también las necesidad no funcionales, especialmente la seguridad tanto del sistema a construir como las necesidades que surgen al implantarlo con la tecnología Grid. Por otro lado, otro reto a solventar es el uso de los dispositivos móviles en los sistemas Grid, con toda la dificultad que conlleva el construir una infraestructura Grid que de soporte a los dispositivos móviles, debido a las limitaciones y características de estos dispositivos.

Por ello, el disponer de una metodología de desarrollo centrada en sistemas Grid, aportando un desarrollo seguro y con soporte para dispositivos móviles es un gran avance para el campo de los sistemas Grid y de los dispositivos móviles, a la vez que supone una potente herramienta para los desarrolladores de estos sistemas.

5.1 Propuesta del Proceso de Desarrollo de Sistemas Grid seguros

Como se puede ver en la figura 3, se parte de las necesidades que el sistema a construir debe cumplir, teniendo en cuenta las características específicas de los dispositivos móviles. Estas necesidades son las entradas al proceso de desarrollo, donde, a través de una serie de etapas, se diseñará y construirá un sistema Grid seguro donde todas las necesidades iniciales estarán cubiertas siguiendo los modelos definidos por la metodología.

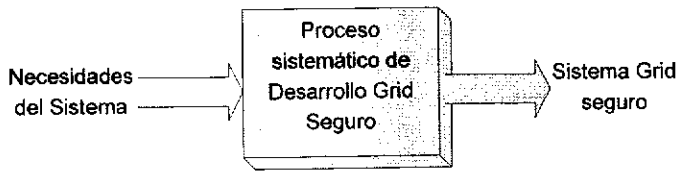

Fig. 3. Entrada y salida de Proceso sistemático de Desarrollo del Sistema Grid seguro.

El proceso sistemático de desarrollo es un proceso iterativo e incremental. Un enfoque iterativo propone una comprensión incremental del problema a través de refinamientos sucesivos y un crecimiento incremental de una solución efectiva a través de varias versiones. De esta forma, en cada iteración del proceso se pueden añadir y ampliar nuevas y necesarias características, de forma que se obtenga un

diseño final completo y cubriendo las necesidades iniciales. En esta primera propuesta, y siguiendo algunas metodologías de desarrollo software como el Proceso Unificado [26], se dará una visión general de la metodología de desarrollo, dejando un estudio más detallado para posteriores investigaciones.

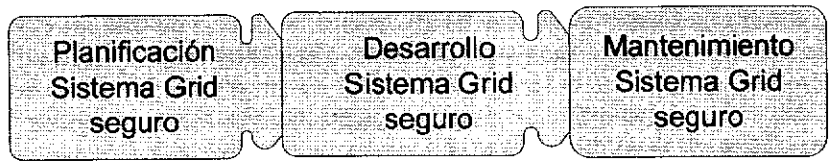

Fig. 4. Metodología de desarrollo de un sistema Grid seguro.

La metodología a desarrollar o proceso sistemático constará de distintos procesos y cada uno de ellos se descompondrá a su vez en subprocesos, y éstos en actividades y tareas. Nuestra metodología constará inicialmente de 3 etapas (ver figura 4): planificación, desarrollo y mantenimiento del sistema Grid seguro.

La metodología de desarrollo lleva algunos artefactos asociados, bien sean requeridos como entradas, bien sean generados como salidas. Algunos artefactos se utilizan como entradas directas en las actividades siguientes, se mantienen como recursos de referencia, o se generan en algún formato específico para su posterior entrega.

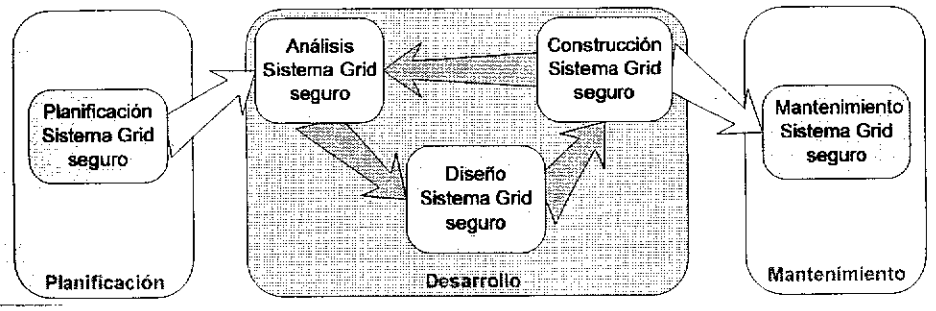

Fig. 5. Procesos de la metodología de Desarrollo Grid seguro. El proceso de desarrollo, que se compone de tres subprocesos, es iterativo, de forma que se pueda volver a iniciar una nueva iteración para completar la construcción del sistema.

A continuación se describirán cada una de estas etapas (ver figura 5), las fases que forman parte de cada etapa, las actividades y tareas definidas en cada fase de forma general, dejando una descripción más detallada (entrada, salida, actores, artefactos, modelos, lenguajes de especificación y modelado, vistas, procedimientos, resultados, etc., etc.) conforme vayamos avanzando en nuestro estudio e investigación de la metodología.

5.2 Proceso de Planificación del Sistema Grid seguro

El primer paso es estudiar si el problema a resolver entra dentro de las características y necesidades que la computación Grid resuelve. Es el estudio de un conjunto concreto de necesidades para proponer una solución que tenga en cuenta restricciones económicas, técnicas, legales y operativas. De aquí partirá la decisión de si el sistema se desarrollará basándonos en la tecnología Grid, por lo que entraría en la siguiente etapa del proceso sistemático, o si por el contrario se procede a buscar otras alternativas más fiables y que mejor cumpla con la solución deseada, siguiendo otras metodologías clásicas de desarrollo software.

En este proceso se hace un estudio de viabilidad, se definirán las necesidades básicas del sistema, los criterios de éxito, la evaluación del riesgo, estimaciones de recursos que se necesitarán, los participantes que intervendrán tanto en el sistema como en el proceso sistemático, los modelos a definir, artefactos requeridos, se evaluarán las distintas alternativas de solución, y para cada una de ellas se analizarán los costes y riesgos, y se seleccionará la solución más adecuada a llevar a cabo para su planificación. El tema de la seguridad y de los dispositivos móviles debe estar muy presente en todo momento a la hora de tomar decisiones estratégicas.

Después del primer paso, si todos los estudios resultan favorables para construir el sistema mediante la tecnología Grid, y el cliente está conforme con los resultados, se continúa con la siguiente etapa.

5.3 Proceso de Desarrollo del Sistema Grid seguro

Este proceso engloba el análisis, diseño y construcción del sistema Grid seguro basándose en las necesidades iniciales y en los artefactos obtenidos en la etapa anterior que describen toda la información relevante y el plan de desarrollo del sistema a construir. En este proceso se definirán los artefactos necesarios y resultantes para cada subproceso, los participantes que intervendrán y cualquier otra información que se necesite conforme vayamos profundizando en la metodología. A continuación se describen los tres subprocesos que forman parte de la etapa de desarrollo.

5.3.1 Subproceso de Análisis del Sistema Grid seguro

El objetivo de este subproceso es la obtención de una especificación detallada del sistema Grid que satisfaga las necesidades de los usuarios y sirva de base para el posterior diseño del sistema. Esta especificación contendría un catálogo de requisitos y modelos que cubran las necesidades, y toda la información relevante referente a los dispositivos móviles, y que será la entrada de la siguiente etapa del diseño de la arquitectura.

Este subproceso se centrará en el estudio de los requisitos identificados en las etapas anteriores, tanto los requisitos funcionales como los no funcionales, haciendo un esfuerzo especial para los requisitos de seguridad y la definición de políticas de seguridad del sistema. También se definirán y analizarán, de forma especial, los requisitos funcionales y no funcionales que son exclusivos de los sistemas Grid, destacando los más importantes a tener en cuenta, definiendo los protocolos y mecanismos propios de los sistemas Grid que serán utilizados en pasos posteriores.

En este subproceso también se modelarán dichos requisitos utilizando modelos clásicos y/o desarrollando y describiendo nuevos modelos que capturen todos los requisitos analizados en esta etapa.

En este segundo paso se obtiene un análisis detallado del sistema a desarrollar. Esta etapa es el inicio del proceso de iteración, pudiendo volver a él para un análisis más concreto de algunas partes del sistema que necesitan analizarse en más detalle o modificar alguna información concreta analizada en los pasos previos.

5.3.2 Subproceso de Diseño del Sistema Grid seguro

En este paso se inicia el proceso de diseño del sistema Grid seguro. El objetivo de este subproceso es la definición de la arquitectura del sistema y del entorno tecnológico que le va a dar soporte, junto con la especificación detallada de todos los componentes del sistema Grid, siempre considerando el uso de los dispositivos móviles. Se determinará el conjunto de elementos de seguridad que son necesarios tomados de una arquitectura de referencia, que se definirá en trabajos futuros, y que pretende ser la arquitectura de Seguridad Grid genérica sobre la que se diseñen las arquitecturas de Seguridad de los sistemas Grid bajo desarrollo.

Por tanto, se debe diseñar una arquitectura común para la construcción de sistemas Grid, siguiendo los requisitos y especificaciones analizadas y obtenidas en las etapas anteriores, y además, hay que enriquecer la metodología para que no sólo sea un proceso sistemático para el diseño y construcción de sistemas Grid, sino que sea un proceso sistemático para la construcción de sistemas Grid bajo un entorno seguro. Se debe diseñar una arquitectura de Seguridad genérica, que complete y se relacione con la arquitectura común y que, las dos arquitecturas constituyan "la arquitectura" del sistema a desarrollar, que servirá como una base sólida sobre la que construir el sistema Grid seguro.

Después de esta etapa, se obtiene una arquitectura Grid que es independiente de la tecnología a utilizar y que cubre todas las necesidades definidas al principio del proceso. Es la arquitectura resultante del sistema Grid seguro a desarrollar.

5.3.3. Subproceso de Construcción del Sistema Grid seguro

Durante este subproceso, se desarrolla de forma iterativa e incremental un sistema Grid completo que está preparado para ser lanzado a la comunidad de usuarios. Esto implica describir los requisitos restantes y los criterios de aceptación, refinando el diseño y completando la implementación y las pruebas del sistema.

Se genera el código de los componentes del sistema Grid, representados en la arquitectura definida en la etapa de diseño, se desarrollan todos los procedimientos y se elaboran todos los manuales de usuario final y de explotación con el objetivo de asegurar el correcto funcionamiento del sistema para su posterior implantación.

Se define un plan de pruebas para validar y verificar si el sistema resultante es correcto y cumple con los requisitos definidos inicialmente. En el caso que haya errores no detectados o no cumple con alguno de los requisitos de seguridad se vuelve atrás, a la etapa de análisis, en una nueva iteración, y se modifica los aspectos relevantes para solucionar el error, que progresivamente va fluyendo por las siguientes etapas de la iteración hasta conseguir que el resultado de la prueba sea válido para pasar a la siguiente etapa.

Al final de la fase de construcción se decide si el software, los lugares donde se instalará y los usuarios están todos preparados para que el sistema empiece a funcionar.

5.4 Proceso de Mantenimiento del Sistema Grid seguro

Es la última etapa del desarrollo y en ella se define un plan de mantenimiento del sistema para su posterior modificación según las nuevas necesidades del cliente. Una vez que el sistema ha sido puesto en manos de los usuarios finales, a menudo aparecen cuestiones que requieren un desarrollo adicional para ajustar el sistema, corregir algunos problemas no detectados o finalizar algunas características que habían sido pospuestas.

Dependiendo de la petición de mantenimiento recibida, se debe estudiar la viabilidad del cambio propuesto, identificar a qué parte del sistema afecta y quién debe intervenir en su corrección, pudiendo ser aceptada o denegada dependiendo del alcance de dicho cambio.

El resultado final es el software que representa el sistema Grid seguro, que el cliente puede utilizar para llevar a cabo el propósito por el que fue desarrollado y que cumple con todos los requisitos definidos inicialmente.

6 Conclusiones

El Grid conecta grupos de ordenadores, unidades de almacenamiento y redes, permitiendo a los centros de investigación y empresas, asignar dinámicamente los recursos de acuerdo a las necesidades del negocio. Los recursos están distribuidos en la red de forma transparente, pero manteniendo un alto nivel de seguridad y una correcta política de gestión que tenga en cuenta parámetros tanto técnicos como económicos. Es un nuevo paradigma de computación, un modelo compartido que permite no solo la comunicación y almacenamiento sino el procesamiento de información por todo el mundo.

En este nuevo modelo compartido, la seguridad juega un papel esencial para el éxito de este nuevo paradigma, asegurando los accesos a los recursos, a la información, a los usuarios y a las organizaciones que ponen sus recursos a la disposición del mundo.

En la comunidad Grid, existe un estándar *de facto* que proporciona las propiedades de seguridad básicas, y otras muchas propiedades que van desarrollándose conforme se avanza en las investigaciones. Estamos hablando de la Infraestructura de Seguridad Grid (GSI), que es un componente de Globus Toolkit y se encarga de todos los aspectos de seguridad de la plataforma.

Resulta difícil incorporar, de forma segura, dispositivos móviles a los Grid existentes, de forma que el impacto sea mínimo y transparente al usuario. Actualmente existen muchas tecnologías y herramientas que hacen que las aplicaciones Grid sean seguras, pero a la hora de incorporar dispositivos móviles (PDA, teléfonos móviles, etc.) las posibilidades de implantar la seguridad se reducen,

debidas principalmente a las limitaciones de estos dispositivos móviles y a sus tecnologías (wireless, WAP, etc.).

Existen numerosos estudios referentes a incorporar seguridad en todo el ciclo de vida del software para obtener un producto final que cumpla con los requisitos de seguridad requeridos. En el caso del ciclo de vida de un sistema Grid, ocurre la misma situación, hace falta incorporar la seguridad desde las primeras etapas del desarrollo, definiendo algún proceso o metodología que, además de desarrollar un sistema Grid, vaya incorporando todos lo aspectos de seguridad Grid al ciclo de vida y obteniendo, por tanto, un producto final seguro. Es por ello que surge la necesidad de elaborar y definir un proceso de desarrollo de un sistema basado en tecnología Grid, teniendo en cuenta las peculiaridades y necesidades de este tipo de sistemas. Este proceso debe ser flexible, escalable y dinámico, de forma que se adapte a las necesidades, siempre cambiantes, de los sistemas Grid.

Como trabajo futuro se buscará una solución para incorporar dispositivos móviles a los sistemas Grid de forma transparente para el usuario y se analizará en profundidad el método propuesto, definiendo más específicamente cada etapa, actividades y tareas que se requieren, y se identificarán los detalles que se deben llevar a cabo en cada etapa, llevándonos a la definición del proceso definitivo que queremos desarrollar. Haremos un esfuerzo especial en la parte de diseño de la arquitectura Grid con el fin de construir una arquitectura genérica del sistema y además otra arquitectura de seguridad que sea fácilmente integrable y que soporte la incorporación de los dispositivos móviles y sirva de referencia para todos los sistemas Grid a construir mediante esta metodología.

Agradecimientos. Esta artículo ha sido desarrollado en el contexto de los proyectos DIMENSIONS (PBC-05-012-2) y MISTICO (PBC-06-0082) financiados parcialmente por FEDER y por la "Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha" (España), RETISTRUST (TIN2006-26885-E) y ESFINGE (TIN2006-15175-CO5-05) de la "Dirección General de Investigación del Ministerio de Educación y Ciencia" (España).

Referencias

1. Foster, I., C. Kesselman, and S. Tuecke, *The Anatomy of the Grid: Enabling Scalable Virtual Organizations.* 7th International Euro-Par Conference Manchester on Parallel Processing, 2001. **15(3)**: p. 1 - 4.
2. Foster, I. and C. Kesselman, *The Grid: Blueprint for a Future Computing Infrastructure.* 1999, San Francisco, CA: Morgan Kaufmann Publishers; 1ST edition.
3. Welch, V., F. Siebenlist, I. Foster, J. Bresnahan, K. Czajkowski, J. Gawor, C. Kesselman, S. Meder, L. Pearlman, and S. Tuecke. *Security for Grid services*. in 12th IEEE International Symposium on High Performance Distributed Computing (HPDC-12 '03). 2003: IEEE Computer Society. p. 48- 57
4. Foster,. I., C. Kesselman, G. Tsudik, and S. Tuecke. *A Security Architecture for Computational Grids*. in 5th ACM Conference on Computer and Communications Security Conference. 1998. San Francisco, CA, USA: ACM Press. p. 83-92

5. Chadwick, D.W. and A. Otenko, *The PERMIS X.509 Role Based Privilege Management Infrastructure*. Future Generation Computer Systems, 2003. **19**(2): p. 277–289.
6. Crampton, J. and H.W. Lim, *Role Signatures for Access Control in Grid Computing*. 2007. p. 19. http://www.ma.rhul.ac.uk/static/techrep/2007/RHUL-MA-2007-2.pdf
7. Pearlman, L., V. Welch, I. Foster, and C. Kesselman. *A Community Authorization Service for Group Collaboration*. in IEEE 3rd International Workshop on Policies for Distributed Systems and Networks. 2002.
8. Globus Toolkit. www.globus.org/toolkit/
9. Globus Project, *Grid Security Infrastructure (GSI)*. www.globus.org/security
10. The Globus Security Team, *Globus Toolkit Version 4 Grid Security Infrastructure: A Standards Perspective*. 2005
11. Guan, T., E. Zaluska, and D.D. Roure. *A Grid Service Infrastructure for Mobile Devices*. in First International Conference on Semantics, Knowledge, an Grid (SKG 2005). 2005. Beijing, China.
12. Jameel, H., U. Kalim, A. Sajjad, S. Lee, and T. Jeon. *Mobile-To-Grid Middleware: Bridging the gap between mobile and Grid environments*. in European Grid Conference EGC 2005. 2005. Amsterdam, The Netherlands: Springer. p. 932-941
13. Kalim, U., H. Jameel, A. Sajjad, and S. Lee. *Mobile-to-Grid Middleware: An Approach for Breaching the Divide Between Mobile and Grid*. in 4th International Conference on Networking. 2005. Reunion Island, France: Springer. p. 1-8
14. kwok-Yan, L., Z. Xi-Bin, C. Siu-Leung, M. Gu, and S. Jia-Guang, *Enhancing Grid Security Infrastructure to Support Mobile Computing Nodes*. Lecture Notes in Computer Science, 2004. **2908/2003**: p. 42-54.
15. Sajjad, A., H. Jameel, U. Kalim, S.M. Han, Y.-K. Lee, and S. Lee. *AutoMAGI - an Autonomic middleware for enabling Mobile Access to Grid Infrastructure*. in Joint International Conference on Autonomic and Autonomous Systems and International Conference on Networking and Services - (icas-icns'05). 2005. p. 73
16. Baskerville, R., *Information systems security design methods: implications for information systems development*. ACM Computing Surveys, 1993. **25**(4): p. 375 - 414.
17. Anderson, R., *Security Engineering - A Guide to Building Dependable Distributed Systems*. 2001: John Wiley & Sons, Inc. 640 Pgs.
18. Foster, I. and C. Kesselman, *A Data Grid Reference Architecture*. 2001, GriPhyN
19. The Global Grid Forum. www.gridforum.org
20. Foster, I., C. Kesselman, J.M. Nick, and S. Tuecke, *The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration*, in *Open Grid Service Infrastructure WG, Global Grid Forum*. 2002
21. Forman, G.H. and J. Zahorjan, *The Challenges of Mobile Computing*. IEEE Computer, 1994. **27**(4).
22. Trung, T.M., Y.-H. Moon, C.-H. Youn, J.-J. Cho, and S.-J. Jeong. *A Gateway Replication Scheme for Improving the Reliability of Mobile-to-Grid Services*. in IEEE International Conference on e-Business Engineering (ICEBE'05). 2005.
23. Foster, I. and C. Kesselman, *Globus: A Metacomputing Infrastructure Toolkit*. The International Journal of Supercomputer Applications and High Performance Computing, 1997. **11**(2): p. 115--128.
24. IETF, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile (RFC 3280)*. http://www.ietf.org/rfc/rfc3280.txt
25. Foster, I. and C. Kesselman, *Globus: A Toolkit-Based Grid Architecture*, in *The Grid: Blueprint for a New Computing Infrastructure*. 1999, Morgan Kaufmann. p. 259-278.
26. Kruchten, P., *The Rational Unified Process: An Introduction*. 2nd ed. 2000: Addison-Wesley. 320 Pgs.