novática
UPGRADE
Revista de la Asociación de Técnicos de Informática
NOVIEMBRE - DICIEMBRE 2002
160

Novática, revista fundada en 1975, es el órgano oficial de expresión y formación continua de ATI (Asociación de Técnicos de Informática). *Novática* edita también *Upgrade*, revista digital de CEPIS (*Council of European Professional Informatics Societies*), en lengua inglesa.

<http://www.ati.es/novatica/>
<http://www.upgrade-cepis.org/>

ATI es miembro de CEPIS (*Council of European Professional Informatics Societies*) y tiene un acuerdo de colaboración con ACM (*Association for Computing Machinery*). Tiene asimismo acuerdos de vinculación o colaboración con AdaSpain, AI² y ASTIC

Coordinación Editorial y Redacción Central (ATI Madrid)
Padilla 66, 3º, dcha., 28006 Madrid
Tlf.914029391; fax.913093685 <*novatica@ati.es*>
Composición, Edición y Redacción ATI Valencia
Palomino 14, 2ª, 46003 Valencia
Tlf./fax 963918531 <*secreval@ati.es*>
Administración y Redacción ATI Cataluña
Via Laietana 41, 1º, 1ª, 08003 Barcelona
Tlf.934125235; fax 934127713 <*secregen@ati.es*>
Redacción ATI Andalucía
Isaac Newton, s/n, Ed. Sadiel, Isla Cartuja 41092 Sevilla
Tlf./fax 954460779 <*secreand@ati.es*>
Redacción ATI Aragón
Lagasca 9, 3-B, 50006 Zaragoza
Tlf./fax 976235181 <*secreara@ati.es*>
Redacción ATI Asturias-Cantabria <*gp-astucant@ati.es*>
Redacción ATI Castilla-La Mancha <*gp-clmancha@ati.es*>
Redacción ATI Galicia
Recinto Ferial s/n, 36540 Silleda (Pontevedra)
Tlf.986581413; fax 986580162 <*secregal@ati.es*>
Suscripción y Ventas: <*http://www.ati.es/novatica/interes.html*>,
o en ATI Cataluña y ATI Madrid
Publicidad: Padilla 66, 3º, dcha., 28006 Madrid
Tlf.914029391; fax.913093685 <*novatica.publicidad@ati.es*>

Imprenta: 9·Impressió S.A., Juan de Austria 66, 08005 Barcelona.
Depósito Legal: B 15.154-1975
ISBN: 0211-2124; CODEN NOVAEC

Portada: Antonio Crespo Foix / © ATI 2002

SUMARIO

En resumen: **e-Comercio para cerrar el año** 3
Rafael Fernández Calvo

Monografía: *«Seguridad en e-Comercio»*
(En colaboración con ***Upgrade***)
Editores invitados: *Javier Areitio Bertolín, Javier López Muñoz, José A. Mañas Argemí, Stephanie Teufel*
Presentación. Comercio Electrónico: seguridad y confianza 4
Javier Areitio Bertolín, Javier López Muñoz, José A. Mañas Argemí, Stephanie Teufel
PISCIS: Comercio Electrónico basado en una infraestructura de certificación avanzada y tarjetas inteligentes 6
Félix J. García Clemente, Antonio F. Gómez Skarmeta, Gabriel López Millán, Rafael Marín López, Antonio Ruiz Martínez
Esquema de seguridad de un sistema interoperable de cobro electrónico de peajes: el proyecto CARDME 12
Francisco R. Soriano García, Juan G. Jordán Aldasoro
Un método de control de acceso para agentes móviles en aplicaciones Mar-de-Datos 18
Guillermo Navarro Arribas, Sergi Robles Martínez, Joan Borrell Viader
Privacidad, personalización y gestión de seguridad 23
Andreas Erat
Los motores de búsqueda y su influencia en la seguridad del Comercio Electrónico 28
José María Sierra Cámara, Julio César Hernández Castro, Arturo Ribagorda Garnacho
CREDO: sistema seguro de Certificación REmota de DOcumentos 31
Francisco J. Rico Novella, Jordi Forga Alberich, Emilio Sanvicente Gargallo, Jorge Mata Díaz, Juan José Alins Delgado, Luis de la Cruz Llopis
Esquemas de *fingerprinting* para la protección de derechos de distribución 36
Marcel Fernández Muñoz, Miquel Soriano Ibañez, Josep Domingo-Ferrer, Francesc Sebé Feixas

/ DOCS /
El adelanto tecnológico al servicio del desarrollo humano 41
Programa de las Naciones Unidas para el Desarrollo (PNUD)

Secciones Técnicas

Bases de Datos
TEXRET: un sistema interactivo de Recuperación de Texturas (*TEXture RETrieval*) 48
Javier Ruiz-del-Solar, Pablo Navarrete, Patricio Parada

Mundo Estudiantil
El asociacionismo estudiantil hoy 56
Adolfo Vázquez Rodríguez

Sistemas de Tiempo Real
Método de evaluación arquitectónica para Sistemas de Tiempo Real 58
José L. Arciniegas, Juan C. Dueñas

TIC para la Sanidad
Un nuevo reto en la integración hospitalaria: el Sistema Integral Hospitalario (AMH) 63
M. Dolores Muñoz

Referencias autorizadas 66

Sociedad de la Información

Programar es crear
Almejas gigantes e interfaces de usuario 70
25º Concurso Internacional de Programación ACM (2001): problema E
Gestión de una partición fija de memoria:solución 72
José Alberto Verdejo López

Asuntos Interiores

Coordinación editorial / Programación de Novática 76
Normas de publicación para autores / Socios Institucionales 77

Monografía del próximo número:
«*Interacción Persona-Computador*»

Seguridad en e-Comercio

Presentación Comercio Electrónico: seguridad y confianza

Javier Areitio Bertolín[1], Javier López Muñoz[2], José A. Mañas Argemí[3], Stephanie Teufel[4]
[1] Universidad de Deusto; [2] Universidad de Málaga; [3] Universidad Politécnica de Madrid; [4] Universidad de Friburgo (Suiza)

<jareitio@eside.deusto.es>
<jlm@lcc.uma.es>
<jmanas@dit.upm.es>
<stephanie.teufel@unifr.ch>

Las empresas se enfrentan a una serie de retos cada vez más difíciles a la hora de hacer realidad sus planes, de tal forma que la actividad comercial tiende a caracterizarse por unas capacidades de suministro cada vez mayores, una competencia creciente a nivel mundial y unas expectativas y demandas en constante aumento por parte de los clientes.

En ese escenario, las comunicaciones electrónicas resultan muy importantes, y la *Seguridad* es un factor crítico; una cuestión de importancia capital para el desarrollo de cualquier iniciativa en el área de las actividades comerciales electrónicas. Las comunicaciones han de poseer una alta disponibilidad (el tiempo muerto en un entorno de Negocio Electrónico no sólo significa un costo en ingresos iniciales sino que también puede alejar a los clientes de la compañía), han de ser fiables (con elevada funcionalidad y rendimiento y un esquema ágil de gestión y administración), han de garantizar la confidencialidad, etc.

Conseguir un nivel adecuado de cumplimiento de estos requisitos se ha convirtiendo en uno de los retos fundamentales de las empresas en la llamada Nueva Economía. Aunque el comercio electrónico B2B (*Business-to-Business*) no es nuevo y desde hace muchos años viene funcionando bajo otros modelos como el EDI (*Electronic Data Interchange*), la novedad del sistema basado en Internet implica la aceptación por parte del cliente de aplicaciones específicas y en las que las relaciones establecidas son más amplias debido a que en la mayoría de los casos se realizan bilateralmente.

Precisamente, la clave del comercio electrónico es el establecimiento de una relación de confianza entre el comprador y el vendedor, la misma que debe existir en las transacciones comerciales tradicionales. Los mercados digitales evolucionan hacia comunidades de valor añadido centradas en agregar a sus participantes servicios de valor mucho mas allá de los que proporciona un mercado digital, dando un contenido amplio que

Nota del Editor de Novática: por razones de espacio no se incluyen en esta monografía los siguientes artículos: «*The Public Key Infrastructure in Switzerland*», de **Stefano Casa** y **Thomas Schlienger**; «*A Best Practice Guide for Secure Electronic Commerce*», de **Sokratis K. Katsikas** y **Stefanos A. Gritzalis**; «*Arquitectura de seguridad para la comunicación entre agentes*», de **Luis Mengual** y **Julio García Otero**; y «*CPC-OCSP: Una adaptación de OCSP para m-Commerce*», de J**osé L. Muñoz** y **Jordi Fornè**.

Dichos artículos serán publicados, en inglés, en el número 6/2002 de ***Upgrade***, <http://www.upgrade-cepis.org>, y en próximos números de ***Novática***, en castellano

Editores invitados

Javier Areitio Bertolín es Catedrático de la Universidad de Deusto, Facultad de Ingeniería, Dpto. de Telecomunicaciones. Forma parte de CORDIS (*Community Research and Development Information Service*) European Commission, Directorate General XIII-D.2. Es Tutor de la AECI (Agencia Española de Cooperación Internacional). Es ponente, moderador y evaluador habitual de Congresos, Seminarios y Symposium y autor de más de 200 artículos científicos en revistas especializadas y autor de libros técnicos sobre Seguridad en Redes de Computadores, Criptografía y Criptoanálisis. Actualmente dirige proyectos sobre Seguridad/Criptología en Tecnologías de la Información y las Comunicaciones con empresas españolas y participa en proyectos europeos con otras Universidades. Pertenece a diversas asociaciones españolas y extranjeras, entre ellas a ATI, siendo coordinador de la Sección Técnica "Seguridad" de su revista *Novática*.

Javier López Muñoz es Doctor Ingeniero en Informática, adscrito al Área de Ingeniería Telemática del Departamento de Lenguajes y Ciencias de la Computación de la Universidad de Málaga. Desarrolla su actividad docente como Profesor Titular en la E.T.S. de Ingeniería Informática y su labor investigadora dentro del grupo GISUM (Grupo de Ingeniería del Software) de esta universidad, donde coordina el subgrupo de Seguridad. Su actividad investigadora está centrada en el en el área de Seguridad en Redes de Comunicación y en Comercio Electrónico, habiendo realizando parte de esa labor de investigación en varios centros universitarios de E.E.U.U. especializados en la materia. En GISUM, es responsable técnico de varios proyectos de investigación relacionados con los aspectos prácticos de Seguridad de las TIC, entre los que destaca el proyecto internacional «Global PKI» del Telecommunications Advancement Organization de Japon. Asimismo, es Director Técnico del Proyecto IST «CASENET» del V Programa Marco de la Unión Europea.

José A. Mañas Argemí es Ingeniero de Telecomunicación y Doctor en Informática, Catedrático de Ingeniería de Sistemas Telemáticos en la E.T.S.I. Telecomunicación de la Universidad Politécnica de Madrid. Especializado en redes de comunicaciones (Internet en particular) y seguridad (criptografía y protocolos seguros para comunicaciones y medios de pago). Ha participado en la creación del servicio de banca por Internet de BCH y Bankinter, en la definición de la arquitectura de sistemas para los Juegos Olímpicos de Salt Lake City, y análisis de seguridad del canal Internet de Loterías del Estado. Miembro del SC27 (seguridad) de ISO y editor de la norma internacional 18014 (fechado electrónico). Es socio de ATI y colaborador de *Novática*.

Stephanie Teufel estudió Informática en la Universidad Técnica de Berlín y en el Instituto Federal Suizo de Tecnología de Zurich (ETH), donde se licenció en dicha disciplina en 1987. Entre 1989 y 1990 fue profesora en la Universidad de Wollongong, Australia. Más tarde fue investigadora senior en el Departamento de Informática de la Universidad of Zurich, donde se doctoró en 1991. Desde 1999 a 2000 fue profesora de Informática Empresarial en el Departmento de Informática de la Universidad Carl von Ossietzky de Oldenburg, Alemania. Desde abril de 2000 es profesora de Gestión de las Telecomunicaciones en la Universidad de Friburgo, Suiza. Es también Directora del IIMT (*International Institute of Management in Telecommunications*) de la misma Universidad. Sus intereses profesionales son: negocio electrónico a través de móviles, gestión de la seguridad de la información, gestión de la información y las comunicaciones y gestión de la tecnología.

ayude a los integrantes a gestionar todos sus procesos de negocio, pudiendo ofrecer toda la gama de servicios que se pueda imaginar. Aquí es donde, sin duda, la Seguridad se presenta como de especial trascendencia.

Esta monografía trata de dar respuesta, parcial sin duda, al problema fundamental que presenta el comercio electrónico para su completa consolidación: la falta de información en torno a la seguridad de las transacciones generadas en dicho comercio por Internet. En un tema tan extenso y que admite múltiples planteamientos creemos que se ha obtenido un conjunto de artículos que permite dar una visión equilibrada sobre la situación actual del mismo:

- **Félix J. García, Antonio F. Gómez, Gabriel López, Rafael Marín, Antonio Ruiz** muestran los resultados del Proyecto PISCIS, donde se se ha desarrollado un sistema de comercio electrónico avanzado basado en Web y tarjetas inteligentes, y que opera sobre una infraestructura completa de certificación definida en el mismo proyecto.
- **Francisco Soriano y Juan Jordán** presentan un esquema de seguridad para el cobro electrónico de peajes desarrollado en el Proyecto CARDME del V Programa Marco de la Unión Europea.
- **Guillermo Navarro, Sergi Robles y Joan Borrell** presentan un método de control de acceso a recursos basado en RBAC utilizando certificados SPKI, parte de una plataforma segura, Proyecto MARISM-A, de agentes móviles para aplicaciones Mar-de-Datos (procesamiento masivo de datos distribuidos).
- **Andreas Erat** explica que los datos del cliente son de gran importancia para el éxito de cualquier empresa y que el e-Comercio ofrece nuevas posibilidades de obtener nuevos tipos de datos y de utilizarlos de otras formas; todo ello origina riesgos que las empresas deben evitar para impedir que los clientes pierdan la confianza en ellas.
- **José María Sierra, Julio César Hernández y Arturo Ribagorda** exponen cómo los motores de búsqueda pueden utilizarse como herramientas que faciliten el ataque a los servidores web de una empresa, y explican algunas de las medidas que pueden implementarse para dificultar las actividades de posibles atacantes.
- **Francisco Rico, Jordi Forga, Emilio Sanvicente, Jorge Mata, Juan José Alins y Luis de la Cruz** presentan el sistema CREDO para la certificación remota de documentos, que genera de forma individual, no centralizada, documentos no duplicables con un valor monetario asociado que puedan ser certificados remotamente.
- **Marcel Fernández, Miquel Soriano, Josep Domingo-Ferrer y Francesc Sebé** muestran una clasificación y describen los tipos de códigos que proporcionan métodos de rastreo para ataques de confabulación a los esquemas de *fingerprinting*, que intantan proteger la propiedad intelectual y los derechos de distribución de contenidos digitales.

A todos ellos expresamos nuestro agradecimiento por su valiosa colaboración, así como a los editores de *Novática* y *Upgrade* por su iniciativa, y al Grupo de Interés en Seguridad Informática de ATI <http://www.ati.es/gt/seguridad/> por su apoyo.

Referencias útiles sobre Seguridad en Comercio Electrónico

Además de las referencias que aparecen en los artículos de esta monografía, los lectores interesados pueden consultar los siguientes libros, publicaciones periódicas y actas de congresos.

Libros:

· **Ford, W. & Baum, M.**, *Secure Electronic Commerce*, Prentice-Hall, 2001.
· **Goldman, J.E.**, *Network and E-Commerce Security*, John Wiley & Sons, 2002.
· **Gosh, A.**, *E-Commerce Security*, John Wiley & Sons, 1998.
· **Graff, J.C.**, *Cryptography and E-Commerce*, John Wiley & Sons, 2001.
· **Hassler, V.**, *Security Fundamentals for E-Commerce*, Artech House, 2001.
· **Jagannatha, L**. *Internet Commerce Metrics and Models in a New Era of Accountability and Secure Electronic Commerce Package*, Prentice-Hall, 2002.
· **Lacoste, G., Pfitzmann, B., Steiner, M., Waidner, M.**, *Semper – Secure Electronic Marketplace for Europe*, Springer, 2000.
· **Treese, G. W. & Stewart, L.C.**, *Designing Systems for Internet Commerce*, Addison-Wesley, 1998.

Publicaciones periódicas:

· ACM Trans. on Information and System Security
· Electronic Markets
· International Journal of Electronic Commerce
· International Journal of Information Security
· Seguridad en Informática y Comunicaciones (SIC)

Conferencias:

· ACM Conference on Electronic Commerce <http://www.acm.org/sigecom/>
· Congreso anual de Seguridad en las Tecnologías de la Información y las Comunicaciones Español <http://www.securmatica.com/>
· IEEE Workshop on Trust and Privacy in Digital Business <http://www.dexa.org>
· Simposio Español de Comercio Electrónico <http://isg.upc.es/sce03>