

# S16 CCSI 2007

## II SIMPOSIO SOBRE SEGURIDAD INFORMÁTICA

### ■ Actividades Plenarias

HORA	ACTIVIDAD	SALA	UBICACIÓN
<b>■ MARTES 11 DE SEPTIEMBRE DE 2007</b>			
19:30	Acto de inauguración del CEDI	Mozart	Auditorio
20:00	Conferencia inaugural: "The Microprocessor Ten Years from Now: Why it is Relevant to all Informatics"; Prof. Yale Patt	Mozart	Auditorio
21:15	"Grupo Folklórico El Pilar" y Recepción	Mozart	Auditorio
<b>■ MIÉRCOLES 12 DE SEPTIEMBRE DE 2007</b>			
12:45	Mesa Redonda I: La situación y el futuro de la Investigación (en Informática) en España	Mozart	Auditorio
21:00	Recepción en el Excmo. Ayuntamiento de Zaragoza	Ayuntamiento	
<b>■ JUEVES 13 DE SEPTIEMBRE DE 2007</b>			
12:45	Mesa Redonda II: Carrera profesional en informática ¿Influye ser mujer?	Mozart	Auditorio
21:30	Entrega Premios de Informática (Cena de Clausura)	Finca Sansui	
<b>■ VIERNES 14 DE SEPTIEMBRE DE 2007</b>			
12:45	Mesa Redonda III: Futuras ediciones del CEDI y actividades inter-congreso	Mozart	Auditorio
13:30	Clausura	Mozart	Auditorio
16:30	Visita guiada a la ciudad		

### ■ Actividades Específicas del Simposio

#### SESIONES

HORA	SESIÓN	TÍTULO DE LA SESIÓN	PRESIDENTE/A	SALA	UBICACIÓN
<b>■ MARTES 11 DE SEPTIEMBRE DE 2007</b>					
9.00-10.30	11-1	Seguridad en redes	Ángel Martín	3	Facultad de Ciencias - Edificio Matemáticas
11.00-12.30	11-2	Seguridad en redes	José Luis Salazar	3	Facultad de Ciencias - Edificio Matemáticas
12.30-14.30	11-3	Criptografía	Jorge Ramío	3	Facultad de Ciencias - Edificio Matemáticas
16.30-17.45	11-4	Ponencia invitada	Arturo Ribagorda	3	Facultad de Ciencias - Edificio Matemáticas
18.15-19.15	11-5	Protección ante intrusiones	Ana I. González-Tablas	3	Facultad de Ciencias - Edificio Matemáticas

■ MIÉRCOLES 12 DE SEPTIEMBRE DE 2007					
9.00-10.30	12-1	Protocolos y aplicaciones	Eduardo Fez-Medina	3	Facultad de Ciencias - Edificio Matemáticas
11.00-12.30	12-2	Protocolos y aplicaciones	Joan Borrell	3	Facultad de Ciencias - Edificio Matemáticas
16.30-18.00	12-3	Mesa redonda	Benjamín Ramos	3	Facultad de Ciencias - Edificio Matemáticas
18.15-19.15	12-4 A	Autenticación y biometría	Candelaria Hernández	3	Facultad de Ciencias - Edificio Matemáticas
19.15-20.00	12-4 B	Gestión de la seguridad	Candelaria Hernández	3	Facultad de Ciencias - Edificio Matemáticas

## ■ Contenido de las Sesiones

### ■ Sesión 11-1: Seguridad en redes

■ 11-09-2007 / 9:00-10:30 / AULA 3 / FACULTAD DE CIENCIAS - EDIFICIO MATEMÁTICAS

*Resolución de escenarios en control de acceso a grupo en entornos distribuidos*

Joan Arnedo Moreno, Jordi Herrera Joancomartí

*Coste de los protocolos de seguridad en redes MANET*

Helena Rifa Pous, Joan Vila Canals, Jordi Herrera Joancomartí

*Protocolo para la Autenticación de Contenidos en Redes P2P*

Esther Palomar González, Arturo Ribagorda Garnacho, Manuel V. Muñoz Esteban, David Oñoro Navarro

*Descon2: un agregador de información de seguridad y sistema de cuarentena*

Rafael Calzada Pradas, Francisco Valera Pintor

### ■ Sesión 11-2: Seguridad en redes

■ 11-09-2007 / 11:00-12:30 / AULA 3 / FACULTAD DE CIENCIAS - EDIFICIO MATEMÁTICAS

*Desarrollo de una herramienta para obtener el código remoto en ataques de inyección de código a aplicaciones web*

Hugo Francisco González Robledo

*CERTILOC: Análisis y diseño de un servicio de certificación espacio-temporal respetuoso con la privacidad*

Ana Isabel González-Tablas, José María Fuentes, José Carlos Calvo, Agustín Orfila, Johanna Gallo, John Patter

*Comunicaciones Privadas en Redes Ad-hoc Vehiculares*

Alexandre Viejo, Francesc Sebé, Josep Domingo-Ferrer, Jesus Manjón

*Puntos de Vista para Patrones de Arquitectura de Seguridad*

David García Rosado, Carlos Gutierrez, Eduardo Fernández-Medina, Mario Piattini

### ■ Sesión 11-3: Criptografía

■ 11-09-2007 / 12:30-14:30 / AULA 3 / FACULTAD DE CIENCIAS - EDIFICIO MATEMÁTICAS

*Un esquema para el reparto de secretos utilizando los autómatas celulares elementales irreversibles con reglas 90 y 150*

Ángel Martín del Rey, Gerardo Rodríguez Sánchez

*Análisis comparativo entre métodos de ataque a los criptosistemas RSA, ElGamal y Curvas Elípticas*

Vicente Jara Vera, Carmen Sánchez Ávila

*Anonymizing Data via Polynomial Regression*

Jordi Nin Guerrero, Jordi Pont-Tuset, Pau Medrano-Gracia, Josep L. Larriba-Pey, Víctor Muntés-Mulero

*Generador pseudoaleatorio matricial optimizado sobre  $Z_2$*

Rafael Álvarez Sánchez, José Vicente Aguirre, Leandro Tortosa, Antonio Zamora

*Análisis del cifrado ElGamal de un módulo con curvas elípticas propuesto para el GnuPG*

Sergi Blanch i Torné, Ramiro Moreno Chiral

*Esquema criptográfico de póquer mental sobre teléfonos móviles*

Susana Bujalance García, Jordi Castellà-Roca, Alexandre Viejo

---

■ **Sesión 11-4: Ponencia invitada**

■ 11-09-2007 / 16:30-17:45 / AULA 3 / FACULTAD DE CIENCIAS - EDIFICIO MATEMÁTICAS

- Empresa TB-Solutions
- Empresa Zitralia

**Moderador:** Arturo Ribagorda Garnacho

---

■ **Sesión 11-5: Protección ante intrusiones**

■ 11-09-2007 / 18:15-19:15 / AULA 3 / FACULTAD DE CIENCIAS - EDIFICIO MATEMÁTICAS

*Mejora del clustering de ataques realizado en la red Leurre.com a través de la eliminación de las anomalías de red*

Miguel Fernández Arrieta, Roberto Uribeetxeberria, Urko Zurutuza, Ekain Azketa

*Análisis de datos procedentes de un Sistema de Detección de Gusanos mediante técnicas de clustering*

Urko Zurutuza Ortega, Roberto Uribeetxeberria, Miguel Fernández, Diego Zamboni

*Computación evolutiva para selección pesada de características en sistemas de detección de intrusiones basados en anomalías*

Francisco de Toro Negro, Pedro García Teodoro, Jesús Esteban Díaz Verdejo, Gabriel Maciá Fernández

---

■ **Sesión 12-1: Protocolos y aplicaciones**

■ 12-09-2007 / 9:00-10:30 / AULA 3 / FACULTAD DE CIENCIAS - EDIFICIO MATEMÁTICAS

*TPM en Sistemas de Protección de Streaming Media*

Gimena Pujol, Antonio Muñoz, Antonio Maña

*Hacia una solución global para servicios médicos en situaciones de emergencia*

Joan Borrell, Maria Carmen de Toro, Sergi Robles, Ramon Martí, Guillermo Navarro

*Optimizaciones al Voto Electrónico para la e-Cognocracia*

Joan Josep Piles Contreras, Ángel Luis de Juan, José Luis Salazar

*Solución Global para la Autenticación de Nodos en MANETs*

Pino Caballero Gil, Cándido Caballero Gil, Jezabel Molina Gil

### ■ Sesión 12-2: Protocolos y aplicaciones

■ 12-09-2007 / 11:00-12:30 / AULA 3 / FACULTAD DE CIENCIAS - EDIFICIO MATEMÁTICAS

*Protocolo de intercambio justo para comercio electrónico basado en políticas de firma*  
Jorge López Hernández-Ardieta, Ana Isabel González-Tablas Ferreres, Benjamín Ramos Álvarez

*Herramientas para la Seguridad Cooperativa en Redes Ad-Hoc*  
Pino Caballero Gil, Jezabel Molina Gil, Cándido Caballero Gil

*Mejoras en el Modelo Auto-Organizado de Gestión de Claves en MANETS*  
Candelaria Hernández Goya, Pino Caballero Gil

*Modelo de Madurez para la Gestión de la Seguridad en las PYMES basado en Esquemas predeterminados*  
Luis Enrique Sánchez Crespo, Antonio Santos-Olmo Parra, Daniel Villafranca Alberca, Eduardo Fernández-Medina Patón, Mario Piattini Velthius

### ■ Sesión 12-3: Mesa redonda

■ 12-09-2007 / 16:30-18:00 / AULA 3 / FACULTAD DE CIENCIAS - EDIFICIO MATEMÁTICAS

*El Nuevo Reglamento de Protección de Datos de Carácter Personal*

**Ponentes invitados:**

- José Luis Piñar Mañas
- Antonio Troncoso Reigada
- Arturo Ribagorda Garnacho
- José de la Peña Muñoz

**Moderador:** Benjamín Ramos Álvarez

### ■ Sesión 12-4 A: Autenticación y biometría

■ 12-09-2007 / 18:15-19:15 / AULA 3 / FACULTAD DE CIENCIAS - EDIFICIO MATEMÁTICAS

*Sistema de seguridad biométrico basado en extracción geométrica de características faciales*  
José Manuel Chaves González, Miguel Ángel Vega Rodríguez, Juan Antonio Gómez Pulido, Juan Manuel Sánchez Pérez

*Mejora de un sistema de seguridad biométrico gracias a un nuevo método de segmentación del iris rápido y robusto*  
Noé Otero Mateo, Miguel Ángel Vega Rodríguez, Juan Antonio Gómez Pulido, Juan Manuel Sánchez Pérez

*Protocolo de autenticación robusta para dispositivos móviles*  
Miguel Ángel Sarasa López

### ■ Sesión 12-4 B: Gestión de la seguridad

■ 12-09-2007 / 19:15-20:00 / AULA 3 / FACULTAD DE CIENCIAS - EDIFICIO MATEMÁTICAS

*Hacia un método para la construcción de Cuadros de Mando de la Seguridad en TI para PYMES*  
Daniel Villafranca Alberca, Luis Enrique Sánchez Crespo, Eduardo Fernández-Medina, Mario Piattini

*Ontologías de seguridad: revisión sistemática y comparativa*  
Carlos Blanco Bueno, Joaquín Lasheras, Rafael Valencia-García, Eduardo Fernández-Medina, Ambrosio Toval, Mario Piattini



*Ingeniería de seguridad y Ciclo de vida de desarrollo de software*

Manuel Rodríguez García, Benjamín Ramos Álvarez

*Nuevo servicio de intermediación de pasarelas de pago*

Mildrey Carbonell Castro, José María Sierra Cámara, Joaquín Torres, Antonio Izquierdo, Javier López

