Reunión Española sobre Criptología y Seguridad de la Información, RECSI 2012

http://recsi2012.mondragon.edu

Presentación

La Sociedad de la Información es hoy en día una realidad en la que participan los principales agentes sociales: empresas, administraciones, agentes científicos, y la sociedad en su conjunto. Los agentes científicos proveen un conocimiento, que con el apoyo de la administración y su transformación en tecnología por parte de la empresa, debe dar respuesta a las necesidades que demanda la sociedad a corto, medio y largo plazo. La seguridad informática ha constituido una necesidad básica para garantizar el éxito de las Tecnologías de la Información y Comunicaciones, velando por el correcto uso de las mismas por parte de la sociedad.

La **Reunión Española sobre Criptología y Seguridad de la Información** (RECSI) es el congreso científico referente español en el tema de la Seguridad en las Tecnologías de la Información. En él se dan cita de forma bianual los principales investigadores españoles en el tema, así como invitados extranjeros de reconocido prestigio. En el año 2012 se celebrará la duodécima edición de este congreso en el mes de septiembre y en la ciudad de Donostia-San Sebastián. Las pasadas ediciones se realizaron en Palma de Mallorca (1991), Madrid (1992), Barcelona (1994), Valladolid (1996), Torremolinos (1998), Santa Cruz de Tenerife (2000), Oviedo (2002), Leganés (2004), Barcelona (2006), Salamanca (2008) y Tarragona (2010).

La XII RECSI se desarrollará entre el **4 y el 7 de Septiembre de 2012**. Se llevarán a cabo varias conferencias plenarias a cargo de investigadores internacionales de reconocido prestigio. También se desarrollarán contribuciones divididas en **dos sesiones paralelas**: Criptología y Seguridad de la Información. Además se contará con la realización de una mesa redonda y la participación de miembros de las principales empresas nacionales del ámbito de la seguridad.

Sede

La RECSI 2012 se desarrollará en el **Palacio de Miramar** bajo el paraguas de los **Cursos de Verano de la EHU**. El palacio está situado en pleno Paseo Miraconcha, 48 20007 San Sebastián. El Palacio es un enclave privilegiado situado sobre el mar, la Bahía de la Concha, y con unas estupendas vistas de Donostia. Su situación facilitará el acceso a los participantes del congreso desde los distintos recintos hoteleros que dispone la Ciudad.

Organización

La organización del evento la realiza el grupo de investigación en Redes, Sistemas y Seguridad de la Información de la Escuela Politécnica Superior de Mondragon Unibertsitatea. La estructura organizacional estará compuesta por un Comité de Organización, y un Comité Científico.

El Comité Organizador, formado por un equipo de trabajo de la Escuela Politécnica Superior de **Mondragon Unibertsitatea**, será el encargado de todos los aspectos organizacionales, tales como definición del programa, fechas y horarios, ponencias plenarias, definir y coordinar las tareas y asignaciones del Comité Científico, publicidad, coordinar los aspectos logísticos, las actividades de ocio y cultura, patrocinio, etc.

El Comité Científico está formado por más de 50 investigadores referentes en el área, y será el encargado de evaluar y seleccionar los trabajos de mayor calidad.

Participación

Durante las últimas tres ediciones de la RECSI, el número de inscripciones se mantiene bastante estable, por lo que se puede asegurar una participación en torno a los **120-150 asistentes**.

El congreso se desarrolla mediante dos sesiones paralelas, necesitando dos salas con aforo mínimo para 75-80 personas. Una de ellas, deberá ser capaz de albergar a todos los asistentes, tanto para la sesión inaugural, como para las ponencias invitadas.

Las ponencias se repartirán de forma equitativa. Teniendo como referencia la anterior RECSI, se presentaron 70 trabajos, 38 en el área de la Seguridad de la Información, y 32 en el área de Criptología.

Los **temas de interés** principales serán:

- Criptología y criptoanálisis
- Autenticación y firma digital
- Aplicaciones de la criptografía
- Privacidad y anonimato
- Marcas de agua y esteganografía
- Control de accesos
- Detección de intrusiones y máquinas trampa
- Análisis de malware
- Detección de spam
- Seguridad en redes sociales
- Seguridad en sistemas embebidos
- Informática forense

Estructura del Programa

Martes 4 de Septiembre (tarde)
16:00-18:00 Registro, Recogida de documentación, y tickets de pintxos

Miércoles 5 de Septiembre

8:00-9:00	Registro	
8:45-9:15	Presentación institucional, apertura, inauguración	
9:15-10:10	KEYNOTE 1: Matt Bishop (University of California, Davis)	
10:15-11:15	Sesión Crypto 1	Sesión S.I. 1
611:15-11:45	Café 1	
11:45-13:25	Sesión Crypto 2	Sesión S.I. 2
13:30-15:00	Comida (Stands, present. Patrocinadores)	
15:00-16:00	Sesión Crypto 3	Sesión S.I. 3
16:00-17:00	Sesión Crypto 4	Sesión S.I. 4
18:00-20:00	Actividades Sociales Donostia (a elegir entre): Actividad 1: Curso de Surf Actividad 2: Curso de Elaboración de Pintxos en el Basque Culinary Center Actividad 3: Curso de Cata en el Basque Culinary Center Actividad 4: Paseo en Catamarán por la bahía de Donostia	
21:30	Cena1: Menú de Sidrería en la Cofradía Gastronómica	

Jueves 6 de Septiembre

8:30-9:00	Registro	
9:00-10:40	Sesión Crypto 5	Sesión S.I. 5
10:40-11:00	Café 2	
11:00-11:55	KEYNOTE 2: Fausto Montoya (C.S.I.C.)	
12:00-13:40	Sesión Crypto 6	Sesión S.I. 6
13:40-15:00	Comida (Stands, present. Patro.)	
15:00-16:00	Sesión Crypto 7	Sesión S.I. 7
16:00-17:00	Sesión Crypto 8	Sesión S.I. 8
21:00	Reunión en Punto de Encuentro	
21:30	Cena de gala (Mirador de Ulía)	

Viernes 7 de Septiembre

10:00-11:00	Sesión Crypto 9	Sesión S.I. 9
11:00-11:30	Café 3	
11:30-13:10	Sesión Crypto 10	Sesión S.I. 10
13:10-13:30	Cierre del Congreso	
13:30-15:00	Cocktail de despedida	

Bio de Matt Bishop

Matt Bishop recibió su doctorado en Informática por la Universidad de Purdue, donde se especializó en seguridad informática, en 1984. Actualmente es catedrático en el Departamento de Ciencias de la Computación en la Universidad de California en Davis. Su principal área de investigación es el análisis de las vulnerabilidades en

los sistemas informáticos, incluyendo el modelado, la construcción de herramientas para la detección de vulnerabilidades, y la mejora o la eliminación de las mismas. En la actualidad, tiene proyectos de investigación relacionados con la desinfección de datos, modelado de procesos electorales, y la atribución en los grandes bancos de pruebas, tales como GENI. Ha sido activo en el área de seguridad en sistemas UNIX desde 1979, y ha presentado tutoriales en SANS, USENIX, y otras conferencias. Su libro de texto, *Computer Security: Art and Science*, se publicó en diciembre de 2002 por Addison-Wesley Professional. También es profesor de ingeniería de software, arquitectura de la máquina, sistemas operativos, programación, y (por supuesto) la seguridad informática. Autor de más de 200 publicaciones, director de tesis doctorales, y editor de las revistas científicas más relevantes, como IEEE Security and Privacy entre otras.

Bio de Fausto Montoya

Fausto Montoya Vitini es doctor ingeniero en Telecomunicación por la Universidad Politécnica de Madrid. Ha sido profesor agregado honorífico del grupo de Cátedra XXII en la ETSI de Telecomunicación de la UPM; director técnico del proyecto de Construcción del Centro Nacional de Ingeniería Genética y Biotecnología del Consejo Superior de Investigaciones Científicas; coordinador del Área de Física y Tecnologías Físicas; director en funciones de la Unidad de I+D TAGS; presidente de la Comisión de Coordinación y Asesoramiento Informático de la Presidencia del CSIC; y miembro del Consejo Científico del Centre de Supercomputació de Catalunya. Las líneas de investigación en las que trabaja actualmente son Criptografía, marcas de agua, Teoría de números, generadores pseudoaleatorios, seguridad de la información, sistemas dinámicos no lineales, procesado de señales y ultrasonidos de potencia. Ha publicado cuatro libros y —en revistas internacionales, recogidas en el JCR del ISI, además de en revistas españolas— casi un centenar de artículos originales de investigación. Tiene registradas catorce patentes nacionales, ocho internacionales y ha dirigido veintidós proyectos en España y en el extranjero.

Difusión

Se cuenta con colaboradores como *Criptored*, *Una al día* de Hispasec, revista *SIC* y gracias a la colaboración de *Euskadi + Innova* (iniciativa del Gobierno Vasco), las noticias sobre el evento podrán alcanzar las 50.000 personas.

Contacto

Urko Zurutuza Ortega
Departamento de Electrónica e Informática
Mondragon Unibertsitateko Goi Eskola Politeknikoa, J.M.A. S.Coop.
MONDRAGON UNIBERTSITATEA
Goiru Kalea, 2, 20500 Arrasate-Mondragon (Spain)
Tel: +34 943 253324 / Fax: +34 943791536
http:// mukom.mondragon.edu/infosec