INTRODUCCIÓN

Desde el año 2006 la Cátedra UPM Applus+ de Seguridad y Desarrollo de la Sociedad de la Información CAPSDESI viene organizando en España el Día Internacional de la Seguridad de la Información bajo las siglas DISI.

Se trata de una iniciativa de la ACM, Association for Computing Machinery, que en 1988 propone celebrar todos los 30 de noviembre el Computer Security Day CSD, con el objetivo de concienciar a la sociedad sobre la importancia de la seguridad en el uso y gestión de las Nuevas Tecnologías de la Información.

La cuarta edición del DISI se celebrará el lunes 30 de noviembre de 2009 en el Salón de Actos del Campus Sur de la Universidad Politécnica de Madrid, de 09:00 a 15:00 horas. Constará de una conferencia inaugural sobre vulnerabilidades de las funciones hash y dos coloquios sobre temas de tanta actualidad como el malware y hacking.

En esta IV edición DISI cuenta con tres invitados internacionales: el Dr. Hugo Krawczyk de Estados Unidos, D. José Bidot de Cuba y D. Luis Guillermo Castañeda de México. Participan, además, cinco invitados nacionales: D. Ero Carrera, D. Emilio Castellote, D. Chema Alonso, D. Alejandro Ramos y D. Fermín Serna.

DIRIGIDO A

Responsables de seguridad y profesionales de empresas del sector de las TICs, organismos e instituciones, estudiantes universitarios y, en general, personas interesadas en la seguridad y en la calidad de las Tecnologías de la Información.

ASISTENCIA GRATUITA

AFORO DE LA SALA: 550 PERSONAS

INFORMACIÓN ADICIONAL

Para mayor información, dirigirse a:

Dña. ***Beatriz Miguel Gutiérrez***
Secretaría de Dirección de la EUITT
Cátedra UPM Applus+
Teléfono: 91 336 7842
Correo: bmiguel@euitt.upm.es

Formación equivalente a 5 créditos CPE
Continuing Professional Education

Para tener derecho a este certificado es imprescindible asistir al evento y haberse inscrito con una dirección de e-mail.

Escuela Universitaria de Ingeniería
Técnica de Telecomunicación
Salón de Actos Campus Sur UPM
Carretera de Valencia Km 7
28031 - Madrid

Cátedra UPM Applus+ de Seguridad y Desarrollo de la Sociedad de la Información

CUARTA EDICIÓN DEL DÍA INTERNACIONAL DE LA SEGURIDAD DE LA INFORMACIÓN
DISI 2009

Lunes 30 de noviembre de 2009

Escuela Universitaria de Ingeniería Técnica de Telecomunicación de la UPM

MADRID

INSCRIPCIÓN GRATUITA

www.capsdesi.upm.es

PROGRAMA

Hora	Actividad
08:15	**ACREDITACIÓN Y REGISTRO**
09:00 09:30	**INAUGURACIÓN** - D. José Manuel Perales Vicerrector de TI de la UPM - D. Ramón Capellades Subdirector General Técnico de Applus+ - Dr. Hugo Krawczyk IBM Research - USA - D. César Sanz Director de la EUITT - D. Jorge Ramió Director de la Cátedra UPM Applus+
09:30 10:30	**CONFERENCIA INAUGURAL** **Randomized Hashing: Secure Digital Signatures without Collision Resistance** Ponente: Dr. Hugo Krawczyk
10:30 12:00	**COLOQUIO** **Tendencias en Malware** Modera: - D. Justo Carracedo Catedrático de la EUITT Participan: - D. José Bidot - D. Ero Carrera - D. Emilio Castellote
12:00 12:45	**Descanso e invitación a cóctel en salones del Campus Sur UPM**
12:45 14:45	**COLOQUIO** **Mitos y Realidades en Hacking** Modera: - D. Daniel Calzada Profesor Titular de la EUI Participan: - D. Luis Gmo. Castañeda - D. Chema Alonso - D. Alejandro Ramos - D. Fermín Serna
14:45 15:00	**CLAUSURA** - D. César Benavente Subdirector Investigación de la EUITT - Dña. Gemma Déler Directora Adjunta Unidad TI de Applus+ - D. Jorge Ramió Director de la Cátedra UPM Applus+ - D. Justo Carracedo Catedrático de la EUITT

CONFERENCIA INAUGURAL

Randomized Hashing: Secure Digital Signatures without Collision Resistance

Los ataques criptoanalíticos en años recientes contra funciones de hash han demostrado la fragilidad de nuestros sistemas criptográficos y han puesto en duda nuestra habilidad para diseñar sistemas que resistan ataques a largo plazo. En particular, estos ataques han expuesto la inseguridad de firmas digitales a tal punto que un grupo de investigadores en Holanda lograron recientemente utilizar los ataques contra la función hash MD5 para falsificar un certificado de clave publica que les permitiría falsificar y desviar a gusto tráfico y transacciones en el Internet. En esta charla presentaremos métodos para obtener firmas digitales seguras aun cuando las funciones de hash utilizadas sean vulnerables a ataques de colisión. Estos métodos están validados con pruebas matemáticas de seguridad y están siendo estandarizados por el gobierno de los EEUU.

Dr. Hugo Krawczyk (Estados Unidos)
Investigador en el campo de la criptografía en IBM. Además de una amplia lista de publicaciones académicas, el Dr. Krawczyk es conocido por sus contribuciones a la seguridad informática, incluyendo la invención de la función de autenticación HMAC y de varios diseños criptográficos en estándares internacionales como por ejemplo IPsec y TLS.

PONENTES INVITADOS

D. José Bidot (Cuba)
Director de Segurmática

D. Luis Guillermo Castañeda (México)
Director de Servicios Profesionales de Rusoft

D. Ero Carrera (España)
Chief Research Officer de Virus Total

D. Emilio Castellote (España)
Director de Marketing de Panda Security

D. Chema Alonso (España)
Consultor de Seguridad de Informática64

D. Alejandro Ramos (España)
Manager de TigerTeam en SIA

D. Fermín Serna (España)
Security Software Engineer MSRC de Microsoft

En hoja anexa se entregará un breve CV de estos expertos invitados a los dos coloquios del DISI.

CON LA COLABORACIÓN DE

HISPASEC SISTEMAS

red seguridad

ISMS Forum Spain

VIRUS PROT .COM

ati