
XV
Reunión Española sobre Criptología y Seguridad de la Información
Granada, 3-5 octubre 2018
UNIVERSIDAD DE GRANADA
RENIC
CCN
CENTRO CRIPTOLÓGICO NACIONAL
indra
Network Engineering & Security Group
https://nesg.ugr.es

PROGRAMA RECSI 2018

Granada 3-5 octubre 2018

	Martes 2 octubre	Miércoles 3 octubre	Jueves 4 octubre	Viernes 5 octubre
08:00-08:30		*Registro*		
08:30-08:45		*Bienvenida*	*Registro*	
08:45-09:45		**Plenaria Criptología** *D. Luis Jiménez Muñoz* *-Centro Criptológico Nacional-*	**Plenaria Seguridad Industrial** *D. José Valiente Pérez* *-Centro Ciberseguridad Industrial-*	
09:45-10:00		*Registro*	*Registro*	*Registro*
10:00-11:30		**Sesión *1*** *Criptología*	**Sesión *5*** *IoT y Smart Grid*	**Sesión *8*** *Criptografía Aplicada*
11:30-12:00		*Coffee break*	*Coffee break*	*Coffee break*
12:00-13:30		**Sesión *2*** *Forense y Esteganografía*	**Sesión *6*** *Seguridad y Análisis de Datos*	**Sesión *9*** *Seguridad y e-Administración*
13:30-15:00		Comida	Comida	*Despedida y cierre* Comida
15:00-16:30		**Sesión *3*** *Charlas cortas:* *Criptografía y Ciberseguridad*	**Sesión *7*** *Detección y Ciberdefensa*	Paseo por el Albayzín
16:30-17:00		*Coffee break*	*Coffee break*	
17:00-18:30		**Sesión *4*** *Privacidad y Anonimato*	***Mesa Redonda:*** *I+D+i Nacional en Ciberseguridad*	
21:00→				
21:30→	Copa bienvenida	Visita Alhambra	Cena Gala	

MIÉRCOLES 3 DE OCTUBRE

Charla Plenaria (*08:45-09:45*): Criptología y Ciberseguridad

D. Luis Jiménez Muñoz

Subdirector General Centro Criptológico Nacional

Sesión 1 (*10:00-11:30*): Criptología

- Calculando la complejidad lineal de secuencias criptográficas mediante PN-secuencias. *Amparo Fúster-Sabater and Sara D. Cardell*
- Steiner Triple Systems and Zero Knowledge Protocols. *Feliú Sagols, Guillermo Morales-Luna and Edgar González Fernández*
- Generador de ruido Zener para incrementar la entropía de un TRNG. *Alfonso Blanco Blanco, Víctor Gayoso Martínez, Luis Hernández Encinas, Agustín Martín Muñoz, Fausto Montoya Vitini and Amalia B. Orúe López*
- Linear cellular automata, bivariate polynomials and power of two purely periodic binary sequences. *Domingo Gomez-Perez, Ana Isabel Gomez and Jaime Gutierrez*
- Sobre secuencias pseudoaleatorias a partir de autómatas celulares y funciones bent. *Joan-Josep Climent and Verónica Requena*

Sesión 2 (*12:00-13:30*): Forense y Esteganografía

- Fingerprinting in weighted noisy adder channels. *Marcel Fernandez, Elena Egorova and Grigory Kabatyanskiy*
- Diagnóstico de CSM en estegoanálisis. *Daniel Lerch-Hostalot and David Megías*
- Técnica de Detección de Manipulaciones de Imágenes Digitales Basada en la Matriz del Filtro de Color. *Edgar González Fernández, Esteban Alejandro Armas Vega, Ana Lucila Sandoval Orozco and Luis Javier García Villalba*
- Agrupamiento de Vídeos de Dispositivos Móviles. *Raquel Ramos López, Ana Lucila Sandoval Orozco and Luis Javier García Villalba*
- Evaluación de un sistema forense para BitTorrent. *Alberto Caravaca and Gabriel Maciá-Fernandez*

Sesión 3 (*15:00-16:30*): Charlas Cortas: Criptografía y Ciberseguridad

- Improving a smart metering system using elliptic curves and removing the trusted dealer. *Ricard Garra, Santi Martinez, Josep M. Miret and Francesc Sebe*
- Identificación de polinomios primitivos sobre cuerpos extendidos mediante análisis de secuencias entrelazadas. *Guillermo Cotrina, Andrés Ortiz García and Alberto Peinado*
- Criptografía Basada en Identidad aplicada a una MANET formada por robots. *Jonay Suárez-Armas, Alexandra Rivero-García, Pino Caballero-Gil and Cándido Caballero-Gil*
- Prácticas de desarrollo de extensiones en el mercado de Mozilla tras Firefox Quantum. *Félix Brezo and Yaiza Rubio*
- Seguridad aplicada a una herramienta para el Trastorno por Déficit de Atención e Hiperactividad. *Nayra Rodríguez-Pérez, Alexandra Rivero-García, Pino Caballero-Gil and Josué Toledo-Castro*

- Arquitectura de gestión dinámica de riesgos basada en ontologías y reglas de comportamiento. *Irene Romero, Raúl Riesco, Francisco Barea and Víctor A. Villagrá*
- Herramienta para la identificación de requisitos de seguridad en un Modelo de Desarrollo Seguro. *José Carlos Sancho Núñez, Andrés Caro Lindo, Lucio David Fondón Terrón and José Andrés Félix de Sande*
- Ciberdefensa empresarial: Un marco conceptual y práctico en un entorno digitalmente inestable. *Jeimy Cano*

Sesión 4 (*17:00-18:30*): Privacidad y Anonimato

- Anonimización de datos no estructurados a través del reconocimiento de entidades nominadas. *Fadi Hassan, Josep Domingo-Ferrer and Jordi Soria-Comas*
- Privacy in Microblogging Online Social Networks: Issues and Metrics. *Samia Oukemeni, Helena Rifà-Pous and Joan Manuel Marquès Puig*
- Análisis del protocolo para la anonimización de trayectorias desde el lado del cliente. *Cristina Romero-Tris and David Megias*
- Técnica Anti-Forense para la Anonimización de Vídeos de Dispositivos Móviles. *Carlos Quinto Huaman, Ana Lucila Sandoval Orozco and Luis Javier García Villalba*
- Data Utility Evaluation Framework for Graph Anonymization. *Jordi Casas-Roma*
- Anonimización de trayectorias por medio de intercambios. *Julián Salas, David Megias and Vicenc Torra*

JUEVES 4 DE OCTUBRE

Charla Plenaria (*08:45-09:45*): Caso Práctico de las Consecuencias de Ciberincidentes en una Planta Industrial

D. José Valiente Pérez

Director del Centro de Seguridad Industrial

Sesión 5 (*10:00-11:30*): *IoT* y *Smart Grid*

- Validation of a SIR Epidemic Model for the Propagation of Jamming Attacks in Wireless Sensor Networks. *Miguel López, Alberto Peinado and Andrés Ortiz García*
- Ecosistemas IoT que preserven la privacidad. *Juan Hernández-Serrano, Jose L. Muñoz, Arne Bröring, Lars Mikkelsen, Wolfgang Schwarzott, Oscar Esparza, Olga Leon, Miguel Soriano and Jan Zibuschka*
- Pruebas Basadas en el Entorno para la Detección de Ataques de Relay en Accesos a Zonas Restringidas. *Carles Anglés-Tafalla, Jordi Castellà-Roca, Alexandre Viejo, Magdalena Payeras-Capellà and Macià Mut-Puigserver*
- A Survey on Incident Reporting and Management Systems. *Amna Qureshi, David Megías and Helena Rifà-Pous*
- Sistema de comunicaciones seguras para el personal de servicios de emergencias. *Alexandra Rivero-García, Candelaria Hernández Goya, Iván Santos-González and Pino Caballero-Gil*

Sesión 6 (*12:00-13:30*): Seguridad y Análisis de Datos

- Criptografía adversaria usando deep learning. Limitaciones y oportunidades. *Alfonso Muñoz*
- Mejorando la Detección de Spam Social Utilizando la Subjetividad. *Enaitz Ezpeleta, Mikel Iturbe, Iñaki Garitano, Iñaki Velez de Mendizabal and Urko Zurutuza*
- Constrained approximate bit-parallel search with application in cryptanalysis. *Slobodan Petrovic*
- Hacia una Arquitectura de Referencia Segura para Big Data. *Julio Moreno, Manuel A. Serrano, Eduardo Fernandez-Medina and Eduardo B. Fernandez*
- Sistema Basado en Lógica Difusa para la Detección del Robo de Identidad en Redes Sociales. *José Á. Concepción-Sánchez, Pino Caballero-Gil and Iván Santos-González*

Sesión 7 *(15:00-16:30)*: Detección y Ciberdefensa

- Marisma-CPS: Una Aproximación al Análisis y Gestión de Riesgos para Sistemas Ciberfísicos. *David G. Rosado, Julio Moreno, Antonio Santos-Olmo, Luis E. Sánchez, Manuel A. Serrano and Eduardo Fernandez-Medina*
- Aplicación de técnicas de compresión de información a la identificación de anomalías en fuentes de datos heterogéneas: análisis y limitaciones. *Gonzalo de La Torre, Luis Lago and David Arroyo*
- Mapeo de Dependencias para el Impacto de Ciberataques en Misiones: Una Visión Global. *Raúl Barragán Gil, Jorge López Hernández-Ardieta and Pedro García Teodoro*
- Definición de procedimientos para fabricar honeypots IoT basados en criterios de búsqueda. *Antonio Acien, Ana Nieto, Gerardo Fernandez and Javier Lopez*
- MEDEA: Monitorizando el espacio nulo para la detección de anomalías en sistemas industriales. *Ekhi Zugasti, Mikel Iturbe, Iñaki Garitano and Urko Zurutuza*

Mesa redonda (*17:00-18:30*): I+D+i Nacional en Ciberseguridad

- Ponentes:
  - Dr. Arturo Ribagorda Garnacho – *Presidente RENIC/UC3M*
  - Dr. Jorge Ramió Aguirre – *Editor Criptored-ETSISI/UPM*
  - Dr. Jesús Banqueri Ozáez – *Director OTRI-UGR*
  - D. Valentín Pedrosa Rivas – *Asesor Ejecutivo Agencia IDEA*
  - D. Vito Episcopo Solís – *Secretario General onGranada*
- Modera: Dr. Pedro García Teodoro – *Catedrático UGR*

VIERNES 5 DE OCTUBRE

Sesión 8 (*10:00-11:30*): Criptografía Aplicada

- Un esquema de intercambio de clave a tres bandas postcuántico. *Josep M. Miret, Daniel Sadornil, Juan G. Tena and Javier Valera*
- Sistema de Comunicaciones Seguras para Posicionamiento en Interiores. *Iván Santos-González, Alexandra Rivero-García and Pino Caballero-Gil*
- Mejora de la seguridad en la autentificación basada en contraseñas mediante un cifrador en bloque. *Rafael Alvarez, Alicia Andrade Bazurto and Antonio Zamora Gómez*
- Analysis of the SegWit adoption in Bitcoin. *Cristina Pérez-Solà, Sergi Delgado Segura, Jordi Herrera-Joancomarti and Guillermo Navarro-Arribas*
- Reconstrucción de la Clave PILAR utilizada por el Gobierno Civil de Málaga en 1940. *Alberto Peinado*

Sesión 9 (*12:00-13:30*): Seguridad y e-Administración

- Adecuación al Esquema Nacional de Seguridad: Una Aproximación Metodológica. *Pedro García Teodoro and José Antonio Gómez Hernández*
- Esquemas criptográficos post-cuánticos aplicados a la e-democracia: LWE-Helios Voting. *David Yeregui Marcos Del Blanco, Luis Panizo and José Ángel Hermida*
- Notificaciones Certificadas sobre Blockchain. *Macià Mut Puigserver, Magdalena Payeras-Capellà and Miquel Àngel Cabot-Nadal*
- Uso y retos de blockchain en plataformas de votación electrónica. *Victor Garcia-Font and Helena Rifà-Pous*
- Fidelización mediante Cryptotokens. *Magdalena Payeras-Capellà, Macià Mut Puigserver and Llorenç Huguet-Rotger*