DEPARTAMENTO DE TRATAMIENTO DE LA INFORMACIÓN Y CRIPTOGRAFÍA DE ITEFI-CSIC

IDENTIFICACIÓN DEL EQUIPO INVESTIGADOR

NOMBRE DEL EQUIPO O GRUPO DE INVESTIGACIÓN	**Departamento de Tratamiento de la Información y Criptografía - DTIC**
UNIDAD/DEPARTAMENTO DE PERTENENCIA	**Departamento de Tratamiento de la Información y Criptografía - DTIC**
CENTRO/INSTITUTO/UNIVERSIDAD/ORGANISMO DE PERTENENCIA	**Instituto de Tecnologías Físicas y de la Información**

DATOS DE CONTACTO

DATOS DE CONTACTO DEL EQUIPO

PERSONA DE CONTACTO	**Luis Hernández Encinas**	TELÉFONO	915618806 ext 458
ROL EN EL EQUIPO	Científico Titular	MAIL	luis@iec.csic.es
WEB DEL EQUIPO	www.itefi.csic.es/es/departamentos/dtic		

DIRECCIÓN POSTAL DEL EQUIPO

EDIFICIO	-	CENTRO	**Instituto de Tecnologías Físicas y de la Información**
TIPO DE VÍA	Calle	NOMBRE DE LA VÍA	Serrano
NÚMERO	144	CIUDAD	Madrid
PROVINCIA	Madrid	CÓDIGO POSTAL	28006

DATOS DE CONTACTO DEL ORGANISMO AL QUE PERTENECE

PERSONA DE CONTACTO	**Agustín Martín Muñoz**		
MAIL	agustin@iec.csic.es		
TELÉFONO	915618806	WEB	www.itefi.csic.es/

DIRECCIÓN POSTAL DEL ORGANISMO

EDIFICIO	-	CENTRO	**Instituto de Tecnologías Físicas y de la Información**
TIPO DE VÍA	Calle	NOMBRE DE LA VÍA	Serrano
NÚMERO	144	CIUDAD	Madrid
PROVINCIA	Madrid	CÓDIGO POSTAL	28006

INVESTIGADOR/ES PRINCIPAL/ES

NOMBRE	TITULACIONES
Agustín Martín Muñoz	Doctor en Ciencias Físicas

TRAYECTORIA PROFESIONAL

- Seguridad en Sistemas de Información
- Sistemas dinámicos
- Ataques *side-channel*
- Criptografía
- Simulación Numérica
- Comunicaciones Móviles

WEB Y REDES SOCIALES

MIEMBROS DEL EQUIPO

- Gonzalo Álvarez Marañón
- Alfonso Blanco Blanco
- Alberto Antonio Carrasco Casado
- Marta Conde Pena
- Natalia Denisenko Yakucheva
- José Raúl Durán Díaz
- Javier Espinosa García
- Verónica Fernández Mármol
- Carlos Juan Fernández-Gallardo Alia
- Alberto Fuentes Rodríguez
- Amparo Fúster Sabater
- Víctor Antonio Gayoso Martínez
- Jorge Gómez García
- Luis M. González Bausá
- Fernando Hernández Álvarez
- Luis Hernández Encinas
- Fausto Montoya Vitini
- Jaime Muñoz Masqué
- Jesús Antonio Negrillo Espigares
- Amalia Beatriz Orúe López
- Gerardo Pastor Dégano
- Mª Eugenia Rosado María
- José Ignacio Sánchez García
- Carmen Torrano Giménez

LÍNEAS Y ÁREAS DE INVESTIGACIÓN

PRINCIPALES LÍNEAS DE INVESTIGACIÓN	ÁREAS DE INVESTIGACIÓN
• Seguridad, autenticidad e integridad de la información transmitida • Distribución cuántica de claves	• Procesado de datos
• Criptografía • Diseño y criptoanálisis de sistemas para el cifrado de texto, imagen y voz	• Otras áreas de interés
• Análisis de seguridad	• Sistemas fiables y actualizables
• Aplicaciones web y bases de datos	• Infraestructuras críticas
• Propagación de malware	• Ataques y defensa ante amenazas
• Certificados digitales • DNIe	• Gestión de la identidad

PUBLICACIONES RELACIONADAS DESTACADAS

PUBLICACIONES 2016

Claves para la gestión de la seguridad integral
Luis Hernández Encinas, Javier Espinosa García, 2016

La Criptografía
Luis Hernández Encinas, 2016

Una visión de la Seguridad Integral para una Formación Global en Seguridad
Luis Hernández Encinas, Javier Espinosa García, 2016

PAgIoT – Privacy-preserving Aggregation protocol for Internet of Things
L. González-Manzano, José M. de Fuentes, Sergio Pastrana, Pedro Peris-Lopez, Luis Hernández-Encinas, 2016

PUBLICACIONES RELACIONADAS DESTACADAS

PUBLICACIONES 2015

Software Implementation of Cryptographic Sequence Generators over Extended Fields
O. Delgado, A. Fúster-Sabater, 2015

Performance of the Cryptanalysis over the Shrinking Generator
S. D. Cardell, A. Fúster-Sabater, 2015

A Model for Scale-Free Networks: Application to Twitter
S. Aparicio, J. Villazón, G. Álvarez, 2015

Revision of J3Gen and Validity of the Attacks
A. Peinado, J. Munilla, A. Fúster-Sabater, 2015

Cryptanalysing the shrinking generator
S. D. Cardell, A. Fúster-Sabater, 2015

PUBLICACIONES 2014

A toolbox for DPA attacks to smart cards
A. Fuentes Rodríguez, L. Hernández Encinas, A. Martín Muñoz, B. Alarcos Alcázar, 2014

Generation of Cryptographic Sequences by means of Difference Equations
A. Fúster-Sabater, 2014

Disclosure of sensitive information in the virtual learning environment Moodle
V. Gayoso Martínez, L. Hernández Encinas, A. Hernández Encinas, A. Queiruga Dios, 2014

PUBLICACIONES 2011

Analysis of the Generalized Self-Shrinking Generator
A. Fúster-Sabater, P. Caballero, 2011

PROYECTOS RELEVANTES

Ciberseguridad: datos, información y riesgos (CIBERDINE)
Objetivos: Este proyecto pretende fortalecer la capacidad para prevenir, detectar y responder a los ciberataques desarrollando técnicas que mejoran y proveen de técnicas dinámicas para manejar las amenazas. Para ello, proponemos un programa de investigación transversal que se enfrenta a tres desafíos importantes en la investigación de la ciberseguridad:
Primero, las interdependencias entre las redes y sistemas de información, mediante modelos y tecnologías que faciliten la compartición a través de la determinación de lo que compartir, cuándo y con quién, así como el razonamiento acerca de las repercusiones de intercambio de datos confidenciales.
En segundo lugar, una mejora de la capacidad de defensa requiere un análisis más profundo y más inteligente de todos los eventos que tienen lugar en la red. Para ello es necesario adaptar y desarrollar las tecnologías Big Data para analizar cantidades masivas de información relacionadas con la seguridad.
Por último, un sistema eficaz de gestión de amenazas tiene que poner en su contexto la información disponible, obtener de forma automática los niveles máximos de riesgo para todos los sistemas dinámicos y apoyar las decisiones sobre la selección y el despliegue de las contramedidas óptimas.

Protocolos criptográficos para la ciberseguridad: identificación, autenticación y protección de la información (ProCriCiS)
Objetivos: En nuestra actual Sociedad de la Información, se están produciendo enormes cambios en la vida diaria de las empresas, instituciones y ciudadanos, y uno de los actores principales es Internet. La red, a la que nos conectamos para realizar un sinfín de actividades, tanto profesionales como personales (correo electrónico, e-comercio, operaciones bancarias, mensajería instantánea, etc.), se ha convertido en un elemento fundamental de nuestra sociedad.
Dos de los pilares de las TIC de hoy son la Ciberseguridad y la Computación en la nube, ambos elementos primordiales en el desarrollo del nuestro tejido empresarial

Redes Cuánticas Híbridas (HyQuNet)
Objetivos: Se propone la realización de redes cuánticas basadas en repetidores débilmente confiables mediante la codificación en red, que fuerza a un atacante a romper simultáneamente todos los posibles enlaces si quiere obtener una clave, mejorando así la seguridad y robustez de la red. Se pretende realizar esto duplicando los enlaces utilizando fibra óptica y enlaces al aire

Identificación y autenticación segura en comunicaciones electrónicas (IDEASEC-e)
Objetivos: El objetivo fundamental de este proyecto es mejorar sustancialmente la seguridad para la identificación de las partes y la autenticación de la información, que están presentes en cualquier comunicación. Para ello, pretendemos modificar los protocolos y algoritmos de intercambio de información empleados actualmente en tales comunicaciones, haciendo más seguros los primeros y con mayor privacidad los últimos, así como diseñar otros nuevos y mejorar su implementación en dispositivos portátiles (típicamente tarjetas inteligentes, pero no limitado a ellas). Todo ello debido a que cada vez son más los ataques contra la identificación y autenticación en las comunicaciones, cuyo principal fin es emprender acciones fraudulentas y delictivas para conseguir suplantaciones de identidad y acceso a información privilegiada

CUántica y CaOs (CUCO): Algoritmos Criptográficos de Frontera
Objetivos: Existen ramas de la criptografía que acaban de nacer, pero resultan muy prometedoras, como la criptografía cuántica y la criptografía basada en los sistemas dinámicos no lineales (caos). Se pretende desarrollar un sistema comercial que combine estas dos tecnologías para proporcionar un nuevo sistema de comunicación cifrada de alta seguridad y velocidad, que pueda captar el interés de sectores especialmente sensibles a la seguridad de las comunicaciones como bancos y fuerzas armadas