Seguridad Informática y Criptografía

Características generales | Características del Equipo de Investigación | Características de la Investigación

IDENTIFICACIÓN DEL EQUIPO INVESTIGADOR

NOMBRE DEL EQUIPO O GRUPO DE INVESTIGACIÓN	Seguridad Informática y Criptografía
UNIDAD/DEPARTAMENTO DE PERTENENCIA	-
CENTRO/INSTITUTO/UNIVERSIDAD/ORGANISMO DE PERTENENCIA	Instituto IMDEA Software

DATOS DE CONTACTO

DATOS DE CONTACTO DEL EQUIPO

PERSONA DE CONTACTO	Juan Caballero	TELÉFONO	911012202
ROL EN EL EQUIPO	Associate Research Professor	MAIL	juan.caballero@imdea.org
WEB DEL EQUIPO	https://software.imdea.org/		

DIRECCIÓN POSTAL DEL EQUIPO

EDIFICIO		CENTRO	Instituto IMDEA Software
TIPO DE VÍA		NOMBRE DE LA VÍA	Campus de Montegancedo
NÚMERO	S/N	CIUDAD	Pozuelo de Alarcón
PROVINCIA	Madrid	CÓDIGO POSTAL	28223

DATOS DE CONTACTO DEL ORGANISMO AL QUE PERTENECE

PERSONA DE CONTACTO	Manuel Carro Liñares
MAIL	contacto@software.imdea.org
TELÉFONO	911012202
WEB	www.software.imdea.org/es/

DIRECCIÓN POSTAL DEL ORGANISMO

EDIFICIO		CENTRO	Instituto IMDEA Software
TIPO DE VÍA		NOMBRE DE LA VÍA	Campus de Montegancedo
NÚMERO	S/N	CIUDAD	Pozuelo de Alarcón
PROVINCIA	Madrid	CÓDIGO POSTAL	28223

Seguridad Informática y Criptografía

Características generales | Características del Equipo de Investigación | Características de la Investigación

INVESTIGADOR PRINCIPAL

NOMBRE	TITULACIÓN
Juan Caballero	Phd in Electrical & Computer Engineering, Carnegie Mellon University, EE.UU.
Dario Fiore	PhD in Computer Science, Universidad de Catania, Italia.

TRAYECTORIA PROFESIONAL

WEB Y REDES SOCIALES

MIEMBROS DEL EQUIPO

Barthe, Gilles (tiempo parcial)	Caballero, Juan	Cascudo, Ignacio
Fiore, Dario	Gorla, Alessandra	Guarnieri, Marco
Moreno-Sánchez, Pedro		

Seguridad Informática y Criptografía		
Características generales	Características del Equipo de Investigación	Características de la Investigación

LÍNEAS Y ÁREAS DE INVESTIGACIÓN	
ÁREAS DE INVESTIGACIÓN	**PRINCIPALES LÍNEAS DE INVESTIGACIÓN**
ATAQUES Y DEFENSA ANTE AMENAZAS	Elaboración de mecanismos de respuesta ante ataques Identificación y localización del atacante Fraude online Desarrode herramientas de detección de amenazas Detección y eliminación de malware Ciencia Forense
GESTIÓN DE LA IDENTIDAD	Autenticación criptográfica Computación verificable Computación segura multiparte Protocolos de autenticación Role-Based Access Control
INFRAESTRUCTURAS CRÍTICAS	Monitorizado y seguridad de redes Detección de amenazas Análisis y Gestión de Riesgos Desarrollo de herramientas de protección
PROCESADO DE DATOS	Análisis de datos a gran escala Procesamiento seguro de datos Protección de datos (confidencialidad) Protección de datos (integridad y disponibilidad)
PRIVACIDAD	Private Information Retrieval (PIR) Aplicaciones móviles de preservación de la privacidad Onion routing Protocolos criptográficos de preservación de la privacidad Privacidad en Cloud Cifrado homomórfico de celosías
SISTEMAS FIABLES Y ACTUALIZABLES	Plataformas de ejecución seguras Lenguajes y Frameworks de desarrollo seguros Seguridad / Privacidad mediante el diseño Ciberriesgos Internet of Things Computación Segura
ÁREAS DE INTERÉS	Criptografía Cloud Computing Mobile Computing Internet de las Cosas Seguridad de redes Seguridad en los sistemas operativos

Seguridad Informática y Criptografía		
Características generales	Características del Equipo de Investigación	Características de la Investigación

PUBLICACIONES RELACIONADAS DESTACADAS
PUBLICACIONES AÑO 2020
Spectector: Principled Detection of Speculative Information Flows. Marco Guarnieri, Boris Koepf, Jose F. Morales, Jan Reineke, Andres Sanchez. In Proceedings of the IEEE Security and Privacy Symposium (IEEE S&P), 2020
Towards Attribution in Mobile Markets: Identifying Developer Account Polymorphism. Silvia Sebastian, Juan Caballero. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2020.
Cross-Origin State Inference (COSI) Attacks: Leaking Web Site States through XS-Leaks. Avinash Sudhodanan, Soheil Khodayari, Juan Caballero. In Proceedings of the Network and Distributed Security Symposium (NDSS), 2020.
Boosting Verifiable Computation on Encrypted Data. Dario Fiore, Anca Nitulescu, David Pointcheval. In International Conference on Practice and Theory of Public-Key Cryptography (PKC), 2020.
Angel or Devil? A Privacy Study of Mobile Parental Control Apps. Alvaro Feal, Paolo Calciati, Narseo Vallina-Rodriguez, Carmela Troncoso, Alessandra Gorla. In Privacy Enhancing Technologies Symposium (PoPETS), 2020.2.
PUBLICACIONES AÑO 2019
A Machine-Checked Proof of Security for {AWS} Key Management Service. Jose Bacelar Almeida, Manuel Barbosa, Gilles Barthe, Matthew Campagna, Ernie Cohen, Benjamin Gregoire, Vitor Pereira, Bernardo Portela, Pierre-Yves Strub, Serdar Tasiran. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS), 2019.
Machine-Checked Proofs for Cryptographic Standards: Indifferentiability of Songe and Secure High Assurance Implementations of SHA-3. Jose Bacelar Almeida, Cecile Baritel-Ruet, Manuel Barbosa, Gilles Barthe, Francois Dupressoir, Benjamin Gregoire, Vincent Laporte, Tiago Oliveira, Alley Stoughton, Pierre-Yves Strub. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS), 2019.
The MalSource Dataset: Quantifying Complexity and Code Reuse in Malware Development. Alejandro Calleja, Juan Tapiador, Juan Caballero. IEEE Transactions on Information Forensics and Security 14:12, 3175-3190. 2019.
Mind your Own Business: A Longitudinal Study of Threats and Vulnerabilities in Enterprises. Platon Kotzias, Leyla Bilge, Pierre-Antoine Vervier, Juan Caballero. In Proceedings of the Network and Distributed Systems Security Symposium (NDSS), 2019.
LegoSNARK: Modular Design and Composition of Succinct Zero-Knowledge Proofs. Matteo Campanelli, Dario Fiore, Anais Querol. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS), 2019.
PUBLICACIONES AÑO 2018
Multi-Input Functional Encryption for Inner Products: Function-Hiding Realizations and Constructions without Pairings. Michel Abdalla, Dario Catalano, Dario Fiore, Romain Gay, Bogdan Ursu. In Proceedings of the Annual Cryptology Conference (CRYPTO), 2018.
K-Hunt: Pinpointing Insecure Cryptographic Keys from Execution Traces. Juanru Li, Zhiqiang Lin, Juan Caballero, Yuanyuan Zhang, Dawu Gu. In Proceedings of the ACM SIGSAC Conference on Computer and Communication Security (CCS), 2018.
Coming of Age: A Longitudinal Study of TLS Deployment. Platon Kotzias, Abbas Razaghpanah, Johanna Amann, Kenneth G. Paterson, Narseo Vallina-Rodriguez, Juan Caballero. In Proceedings of ACM Internet Measurement Conference (IMC), 2018.
Symbolic Proofs for Lattice-Based Cryptography. Gilles Barthe, Xiong Fan, Joshua Gancher, Benjamin Gregoire, Charlie Jacomme, Elaine Shi. Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS), 2018
Masking the GLP Lattice-Based Signature Scheme at Any Order. Gilles Barthe, Sonia Belaid, Thomas Espitau, Pierre-Alain Fouque, Benjamin Gregoire, Melissa Rossi, Mehdi Tibouchi. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques (EuroCrypt), 2018.

Seguridad Informática y Criptografía

Características generales | Características del Equipo de Investigación | Características de la Investigación

PROYECTOS RELEVANTES

SCUM: Securing Untrusted Machines. Financiado por Ministerio de Ciencia, Innovacion y Universidades, RTI2018-102043-B-I00. 2019-2022.

Contratos inteligentes y Blockchains Escalables y Seguros mediante Verificacion y Análisis. Financiado por Comunidad de Madrid. P2018/TCS-4339. 2019-2022.

ElasTest: An Elastic Platform for Testing Complex Distributed Large Software Systems. Financiado por Unión Europea Horizonte 2020. ICT-10-2016-731535. 2017-2019.

High-Assurance Crytography. Financiado por Office of Naval Research, EEUU. N00014-19-1-2292. 2019-2022. 2019-2021.

Red de Investigación en Ciberseguridad y Privacidad. Financiado por Ministerio de Ciencia, Innovación y Universidades. RED2018-102321-T. 2020-2022.

Criptografía para Asegurar la Privacidad y la Integridad de la Computación en Máquinas no Confiables. Financiado por Ministerio de Ciencia, Innovación y Universidades. EUR2019-103816. 2019-2021.