Computer Security Lab (COSEC)

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

IDENTIFICACIÓN DEL EQUIPO INVESTIGADOR

NOMBRE DEL EQUIPO O GRUPO DE INVESTIGACIÓN	Computer Security Lab (COSEC)
UNIDAD/DEPARTAMENTO DE PERTENENCIA	Departamento de Informática
CENTRO/INSTITUTO/UNIVERSIDAD/ORGANISMO DE PERTENENCIA	Universidad Carlos III de Madrid

COSEC

DATOS DE CONTACTO

DATOS DE CONTACTO DEL EQUIPO

PERSONA DE CONTACTO	Juan Manuel Estévez Tapiador	TELÉFONO	
ROL EN EL EQUIPO	Director	MAIL	jestevez@inf.uc3m.es
WEB DEL EQUIPO	cosec.inf.uc3m.es		

DIRECCIÓN POSTAL DEL EQUIPO

EDIFICIO	Sabatini	CENTRO	Escuela Politécnica Superior
TIPO DE VÍA	Avenida	NOMBRE DE LA VÍA	de la Universidad
NÚMERO	30	CIUDAD	Leganés
	Madrid	CÓDIGO POSTAL	28911

DATOS DE CONTACTO DEL ORGANISMO AL QUE PERTENECE

PERSONA DE CONTACTO	Juan Romo
MAIL	rector@uc3m.es
TELÉFONO	+34 91 624 95 15
WEB	https://www.uc3m.es

DIRECCIÓN POSTAL DEL ORGANISMO

EDIFICIO	Edificio Rectorado	CENTRO	Rectorado
TIPO DE VÍA	Calle	NOMBRE DE LA VÍA	Madrid
NÚMERO	126	CIUDAD	Getafe
PROVINCIA	Madrid	CÓDIGO POSTAL	28903

Computer Security Lab (COSEC)

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

INVESTIGADOR PRINCIPAL

NOMBRE	TITULACIÓN
Juan Manuel Estévez Tapiador	Doctor en Informática

TRAYECTORIA PROFESIONAL

Juan Tapiador es Catedrático de Universidad y director del grupo COSEC (Computer Security) del Departamento de Informática de la Universidad Carlos III de Madrid. Previamente a su incorporación en 2012 a la UC3M, trabajó como investigador en la Universidad de York (UK) financiado por los Departamentos de Defensa de EE.UU. y Reino Unido. Inició sus carrera investigadora en el Network Engineering & Security Group (http://nesg.ugr.es/) de la Universidad de Granada, donde realizó su tesis doctoral en detección de anomalías en redes. Ha sido visitante en las universidades de York (UK) y en el IBM Thomas J. Watson Research Center (NY, USA). Es Ingeniero en Informática (2000) y Doctor en Informática (2004) por la Universidad de Granada.

Sus principales líneas de investigación están relacionadas con la seguridad de sistemas, redes y software, especialmente el análisis de malware y vulnerabilidades, el cibercrimen, y la privacidad. Su trabajo actual en estas líneas ha sido financiado en los últimos años por los proyectos SPINY, SMOG y ODIO (Agencia Estatal de Investigación), CIBERDINE y CYNAMON (Comunidad de Madrid), y ARVI y ECYSAP (EU), así como numerosas iniciativas del sector privado. Los resultados de su investigación se han plasmado hasta la fecha en más de 130 artículos en revistas y congresos internacionales y la dirección de 7 tesis doctorales (más otras 5 en curso). Es miembro del comité de programa de varias conferencias científicas de prestigio en el campo de la ciberseguridad (USENIX Security, ACSAC, ACNS, DIMVA, ESORICS, AsiaCCS) y miembro del comité editorial de las revistas Computer Communications y Computers & Security. Sus publicaciones han recibido hasta la fecha alrededor de 5,200 citas de acuerdo con Google Scholar. Algunos de sus trabajos en las áreas de protocolos criptográficos para sistemas RFID y detección de anomalías han tenido una influencia significativa en sus respectivos campos, resultando en varias publicaciones que han alcanzado en un corto espacio de tiempo entre 100 y 400 citas cada una. Ha sido invitado a dar charlas de investigación en diversos centros de investigación internacionales de prestigio en su campo, incluyendo el Information Security Group de Royal Holloway University of London e IBM T.J. Watson Research Center). En 2013 recibió el Premio a Jóvenes Investigadores por el Consejo Social de la UC3M y en 2017 su trabajo fue finalista en la Applied Research Competition at CSAW Europe'17. Más recientemente ha recibido premios de las agencias de protección de datos española y francesa por su análisis del software preinstalado en sistemas Android. Los resultados de su investigación han aparecido en medios nacionales (El País, ABC) e internacionales, incluyendo The Times, Le Figaro, ZDNet, y The Register.

Desde 2004 ha impartido regularmente docencia de grado y postgrado en centros universitarios nacionales e internacionales, fundamentalmente en asignaturas relacionadas con sus áreas de investigación. Hasta la fecha ha impartido 36 cursos de grado y 19 de máster, y es desde 2018 el director del Máster Oficial en Ciberseguridad de la UC3M y co-director del Máster Interuniversitario en Analista de Inteligencia.

WEB Y REDES SOCIALES

@0xjet

MIEMBROS DEL EQUIPO

Ribagorda Garnacho, Arturo	Peris López, Pedro	González Manzano, Lorena
González-Tablas Ferreres, Ana Isabel	de Fuentes García Romero de Tejada, José María	Pastrana Portillo, Sergio
Rashed, Mohammed Fahim Ahmed	Blázquez González, Eduardo	Fuster Barceló, Caterina
Nappa, Antonio	Fuentes Astorga, Roberto	Colmena de Celis, José Miguel
Garzón Rubio, Daniel	Cámara Núñez, María del Carmen	Giménez Aguilar, Mar
Fernández Fernández, María Porfiria		

Computer Security Lab (COSEC)		
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	Antivirus Desarrollo de defensas automáticas Desarrode herramientas de detección de amenazas Desarrollo de mecanismos de recolección de datos Detección de anomalías Detección y eliminación de malware Detección y monitorizado de ataques Detección, Identificación y eliminación de propagadores de malware IDS/IPS/Firewalls Nuevos tipos de Malware Esteganografía en la Red Fraude online
SISTEMAS FIABLES Y ACTUALIZABLES	Seguridad / Privacidad mediante el diseño Ingeniería de Seguridad Internet of Things
EVALUACIÓN DE SISTEMAS Y CIBERRIESGOS	Estudio de patrones Mecanismos de recolección de datos Análisis de riesgos estadísticos y predictivos Recolección de información sobre amenazas Creación de repositorios de información Inteligencia de Seguridad
GESTIÓN DE LA IDENTIDAD	Controles de acceso basados en comportamiento Autenticación biométrica Autenticación criptográfica Identificación por radiofrecuencia Control de Acceso y Autenticación Protocolos de autenticación
PROCESADO DE DATOS	Análisis de datos a gran escala Computación de metadatos relevantes Origen de los datos Políticas basadas en datos
PRIVACIDAD	Análisis Big Data enfocado al respeto de la privacidad Aplicaciones móviles de preservación de la privacidad Proxies Redes de comunicación privada Privacidad en Cloud Privacidad en IoT Herramientas de monitorización de la preservación de la privacidad Buenas prácticas en privacidad Políticas de privacidad Tecnologías de seguridad respetuosas con la privacidad

Computer Security Lab (COSEC)

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

PUBLICACIONES RELACIONADAS DESTACADAS

PUBLICACIONES AÑO 2020

Anja Feldmann, Oliver Gasser, Franziska Lichtblau, Enric Pujol, Ingmar Poese, Christoph Dietzel, Daniel Wagner, Matthias Wichtlhuber, Juan Tapiador, Narseo Vallina-Rodriguez, Oliver Hohlfeld, Georgios Smaragdakis. "The Lockdown Effect: Implications of the COVID-19 Pandemic on Internet Traffic". Proceedings of the 2020 ACM Internet Measurement Conference.

Pelayo Vallina, Victor Le Pochat, Álvaro Feal, Marius Paraschiv, Julien Gamba, Tim Burke, Oliver Hohlfeld, Juan Tapiador, Narseo Vallina-Rodriguez. "Mis-shapes, Mistakes, Misfits: An Analysis of Domain Classification Services". Proceedings of the 2020 ACM Internet Measurement Conference.

Álvaro Feal, Julien Gamba, Narseo Vallina-Rodriguez, Primal Wijesekera, Joel Reardon, Serge Egelman, Juan Tapiador. "Don't accept candy from strangers: An analysis of third-party SDKs". Computers, Privacy and Data Protection Conference (CPDP 2020).

Julien Gamba, Mohammed Rashed, Abbas Razaghpanah, Juan Tapiador, Narseo Vallina-Rodriguez. "An analysis of pre-installed android software". IEEE Symposium on Security and Privacy 2020.

M Safkhani, C Camara, P Peris-Lopez, N Bagheri. "RSEAP2: An enhanced version of RSEAP, an RFID based authentication protocol for vehicular cloud computing. Vehicular Communications, 100311, 2020

C Camara, H Martín, P Peris-Lopez, L Entrena. "A True Random Number Generator Based on Gait Data for the Internet of You". IEEE Access 8, 71642-71651, 2020

L Ortiz-Martin, P Picazo-Sanchez, P Peris-Lopez. "Are the Interpulse Intervals of an ECG signal a good source of entropy? An in-depth entropy analysis based on NIST 800-90B recommendation". Future Generation Computer Systems 105, 346-360, 2020

C Camara, P Peris-Lopez, JM De Fuentes, S Marchal. "Access Control for Implantable Medical Devices". IEEE Transactions on Emerging Topics in Computing, 2020

M Salimi, H Mala, H Martin, P Peris-Lopez. "Full-Resilient Memory-Optimum Multi-Party Non-Interactive Key Exchange", IEEE Access 8, 8821-8833

Kieron Turk, Sergio Pastrana, Ben Collier. "A tight scrape: methodological approaches to cybercrime research data collection in adversarial environments". d Workshop on Attackers and Cyber-Crime Operations (2020)

Luis Hernández-Álvarez, José María de Fuentes, Lorena González-Manzano, Luis Hernández Encinas. "Privacy-Preserving Sensor-Based Continuous Authentication and User Profiling: A Review". Sensors 21 (1), 92, 2021

L Gonzalez-Manzano. "A primer on Open Source Intelligence (OSINT) leveraging existing tools". International Congress of Space and Cyberspace (ACIS)

Jose María de Fuentes Lorena Gonzalez-Manzano, Sergio Bernardez. "SmartLED: Smartphone-based covert channels leveraging the notification LED. The 4th International Workshop on Cyberspace Security (IWCSS 2020)

PUBLICACIONES AÑO 2019

P Picazo-Sanchez, J Tapiador, G Schneider. "After you, please: browser extensions order attacks and countermeasures" International Journal of Information Security, 1-16, 2019

S Pastrana, A Hutchings, D Thomas, J Tapiador. "Measuring eWhoring". IMC 2019

O Mirzaei, G Suarez-Tangil, JM de Fuentes, J Tapiador, G Stringhini. "Andrensemble: Leveraging api ensembles to characterize android malware families. AsiaCCS 2019

L Ortiz-Martin, P Picazo-Sanchez, P Peris-Lopez, J Tapiador, G Schneider. "Feasibility analysis of Inter-Pulse Intervals based solutions for cryptographic token generation by two electrocardiogram sensors". Future Generation Computer Systems 96, 283-296, 2019

A Hutchings, S Pastrana. "Understanding eWhoring". EuroS&P 2019

O Mirzaei, JM de Fuentes, J Tapiador, L Gonzalez-Manzano. AndrODet: An adaptive Android obfuscation detector, Future Generation Computer Systems 90, 240-261

A Hutchings, S Pastrana, R Clayton. "Displacing big data: How criminals cheat the system". The Human Factor of Cybercrime, 3 2019

S Pastrana, G Suarez-Tangil. "A first look at the crypto-mining malware ecosystem: A decade of unrestricted wealth". IMC 2019

L González-Manzano, JM de Fuentes. "Design recommendations for online cybersecurity courses" Computers & Security 80, 238-256

L Gonzalez-Manzano, JMD Fuentes, A Ribagorda. "Leveraging user-related internet of things for continuous authentication: A survey" ACM Computing Surveys (CSUR) 52 (3), 1-38

C Patsakis, K Dellios, JM De Fuentes, F Casino, A Solanas. "External Monitoring Changes in Vehicle Hardware Profiles: Enhancing Automotive Cyber-Security" Journal of Hardware and Systems Security 3 (3), 289-303

L Ortiz-Martin, P Picazo-Sanchez, P Peris-Lopez, J Tapiador, G Schneider. Feasibility analysis of Inter-Pulse Intervals based solutions for cryptographic token generation by two electrocardiogram sensors. Future Generation Computer Systems 96, 283-296 4 2019

SF Aghili, H Mala, M Shojafar, P Peris-Lopez. LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT. Future Generation Computer Systems 96, 410-424 392019

H Martin, P Peris-Lopez, GD Natale, M Taouil, S Hamdioui. "Enhancing PUF Based Challenge–Response Sets by Exploiting Various Background Noise Configurations" Electronics 8 (2), 145 2019

C Camara, H Martín, P Peris-Lopez, M Aldalaien. Design and analysis of a true random number generator based on GSR signals for body sensor networks. Sensors 19 (9), 2033

H Martín González, P Peris López, G Di Natale, M Taouil, S Hamdioui. Enhancing PUF Based Challenge-Response Sets by Exploiting Various Background Noise Configurations. 2019

PUBLICACIONES AÑO 2018

A Calleja, J Tapiador, J Caballero. The malsource dataset: Quantifying complexity and code reuse in malware development. IEEE Transactions on Information Forensics and Security 14 (12), 3175-3190

H Wang, Z Liu, J Liang, N Vallina-Rodriguez, Y Guo, L Li, J Tapiador, et al. Beyond google play: A large-scale comparative study of chinese android app markets. IMC 2018

C Camara, P Peris-Lopez, L Gonzalez-Manzano, J Tapiador. Real-time electrocardiogram streams for continuous authentication. Applied Soft Computing 68, 784-794, 2018

A Calleja, A Martín, HD Menéndez, J Tapiador, D Clark. Picking on the family: Disrupting android malware triage by forcing misclassification Expert Systems with Applications 95, 113-126, 2018

L Ortiz-Martin, P Picazo-Sanchez, P Peris-Lopez, J Tapiador. Heartbeats do not make good pseudo-random number generators: an analysis of the randomness of inter-pulse intervals Entropy 20 (2), 94, 2018

A Caines, S Pastrana, A Hutchings, PJ Buttery. Automatically identifying the function and intent of posts in underground forums Crime Science 7 (1), 19

A Caines, S Pastrana, A Hutchings, P Buttery. Aggressive language in an online hacking forum. Proceedings of the 2nd Workshop on Abusive Language Online (ALW2), 66-74

S Pastrana, A Hutchings, A Caines, P Buttery. Characterizing Eve: Analysing Cybercrime Actors in a Large Underground Forum. RAID 2018

S Pastrana, DR Thomas, A Hutchings, R Clayton. CrimeBB: Enabling Cybercrime Research on Underground Forums at Scale. The Web Conference 2018

JM de Fuentes, L Gonzalez-Manzano, A Solanas, F Veseli. "Attribute-based credentials for privacy-aware smart health services in iot-based smart cities" Computer 51 (7), 44-53, 2018

JM De Fuentes, L Gonzalez-Manzano, A Ribagorda. Secure and usable user-in-a-context continuous authentication in smartphones leveraging non-assisted sensors. Sensors 18 (4), 1219

P Peris-Lopez, L González-Manzano, C Camara, JM de Fuentes. Effect of attacker characterization in ECG-based continuous authentication mechanisms for Internet of Things. Future Generation Computer Systems 81, 67-77

R Tabuyo-Benito, H Bahsi, P Peris-Lopez. Forensics Analysis of an On-line Game over Steam Platform. International Conference on Digital Forensics and Cyber Crime, 106-127

SF Aghili, H Mala, P Peris-Lopez. Securing heterogeneous wireless sensor networks: Breaking and fixing a three-factor authentication protocol. Sensors 18 (11), 3663

C Camara, P Peris-Lopez, H Martín, M Aldalaien. ECG-RNG: A random number generator based on ECG signals and suitable for securing wireless sensor networks Sensors 18 (9), 2747

Computer Security Lab (COSEC)		
Características generales	Características del Equipo de Investigación	Características de la Investigación

PROYECTOS RELEVANTES
Nota: solo los de los últimos 5 años y conseguidos en convocatorias públicas
ECYSAP: European Cyber Situational Awareness Platform (2021-2023). EU H2020. 200.000 Euros.
ODIO: The Open Digital Identity Observatory (2020-2022). Agencia Estatal de Investigación. 79.134 Euros.
CYNAMON-CM: Cybersecurity, Network Analysis and Monitoring for the Next Generation Internet (2019-2022). Comunidad de Madrid. 241.546 Euros.
SMOG-DEV: Security Mechanisms for Fog Computing – Avanced Security for Devices (2016-2020). Agencia Estatal de Investigación (). 77.682 Euros.
SPINY: Security and Privacy in the Internet of You (2014-2017). Agencia Estatal de Investigación. 86.381,90 Euros
CIBERDINE: Ciberseguridad: Datos, Información, Riesgos (2014-2018). Comunidad de Madrid. 280.220 Euros