

Yolanda Blanco · Manuel Fernández Veiga
· Ana Fernández Vilas · José M. de Fuentes
(eds.)

**Jornadas Nacionales
de Investigación en
Ciberseguridad**

ACTAS DE LAS VIII JORNADAS NACIONALES DE INVESTIGACIÓN EN CIBERSEGURIDAD

Vigo, 21 a 23 de junio de 2023

ISBN: 978-84-8158-970-2

© atlanTTic – Universidade de Vigo





Patrocinadores



Patrocinio técnico





Comités técnicos

Comité de programa científico

Manuel Fernández Veiga
José María de Fuentes

Lilian Adkinson
Cristina Alcaraz
Ana Ayerbe
Marta Beltrán
Carlos Blanco
Jorge Blasco
Pino Caballero
Agustín Cañas
Andrés Caro
Jesús Esteban Díaz
Josep Lluís Ferrer
Joaquín García-Alfaro
David García
Luis Javier García
Manuel Gil
Félix Gómez
Lorena González
Luis Hernández
Javier López
Jorge López
Agustín Martín
Gregorio Martínez
David Megías
Pantaleón Nespoli
Francisco J. Nóvoa
Raúl Orduña
Inés Ortega
Luis Panizo
Aljosa Pasic
Luis Pérez Freire
Fernando Pérez González
Cristina Regueiro
Erkuden Ríos
Margarita Robles
Ricardo J. Rodríguez
Luis E. Sánchez
Miquel Soriano
Juan Ramón Troncoso
Narseo Vallina
José M. Vázquez-Naya
Víctor Villagrà
Urko Zurutuza

atlanTTic, UVigo
Universidad Carlos III de Madrid

GRADIANT
Universidad de Málaga
TECNALIA
Universidad Rey Juan Carlos
Universidad de Cantabria
Universidad Politécnica de Madrid
Universidad de La Laguna
GRADIANT
Universidad de Extremadura
Universidad de Granada
Universitat de les Illes Balears
Telecom-Sud Paris
Universidad de Castilla-La Mancha
Universidad Complutense de Madrid
Universidad de Murcia
Universidad de Murcia
Universidad Carlos III de Madrid
CSIC
Universidad de Málaga
Verisure
CSIC
Universidad de Murcia
Universitat Oberta de Catalunya
Universidad de Murcia
Universidade da Coruña
VICOMTECH
GRADIANT
Universidad de León
ATOS
GRADIANT
atlanTTic y Universidade de Vigo
TECNALIA
TECNALIA
Universidad de Granada
Universidad de Zaragoza
Universidad de Castilla-La Mancha
Universitat Politècnica de Catalunya
Tuneinsight
IMDEA
Universidade da Coruña
Universidad Politécnica de Madrid
Mondragón Unibertsitatea

Comité del programa de transferencia

Yolanda Blanco Fernández	atlanTTic y UVigo
Juan González Martínez	GRADIANT
Ana Ayerbe	TECANALIA
Javier Sedano	ICTL
Gregorio Martínez	U. Murcia
Urko Zurutuza	U. Mondragón
Raúl Orduña	VICOMTECH
Jordi Guijarro	I2CAT
Juan Díez	INCIBE
Pino Caballero	U. de La Laguna
David Pérez	FUNDITEC
Cristina Alcaraz	U. Málaga
Felipe Gil	U. Vigo
Juan Caubet	EURECAT
Marta Fuentes	FIDESOL
Marc Barceló	IKERLAN
Aitor Urbietta	IKERLAN
Víctor Carneiro	U. da Coruña

Comité del programa de formación

Yolanda Blanco Fernández	atlanTTic y UVigo
José Carlos Sancho Núñez	Universidad de Extremadura
José Carlos Sancho Núñez	Universidad de Extremadura
Noemí De Castro García	Universidad de León
Adriana Suárez Corona	Universidad de León
Isaac Agudo Ruíz	Universidad de Málaga
Ana Isabel González-Tablas Ferreres	Universidad Carlos III de Madrid
Mar Ávila Vegas	Universidad de Extremadura
Xavier Larriva	Universidad Politécnica de Madrid
David García Rosado	Universidad de Castilla – La Mancha
Óscar Mogollón Gutiérrez	Universidad de Extremadura
Ángel Jesús Varela Vaca	Universidad de Sevilla
Roberto Magán Carrión	Universidad de Granada
Raquel Poy Castro	Universidad de León
Javier Corral García	CénitS – COMPUTAEX
Sara García Bécares	INCIBE – Responsable de Talento en Ciberseguridad
Victoria Alicia Marcos Sbarbaro	INCIBE – Técnico de Talento en Ciberseguridad
Iñaki Garitano Garitano	Mondragon Unibertsitatea
Ana Lucila Sandoval Orozco	Universidad Complutense de Madrid

Índice general

Conferencias invitadas

Mordechai Guri <i>Air-gap security</i>	17
Carmela Troncoso <i>Privacidad por diseño</i>	19

Mesas Redondas

Programa científico

Sesión I: Seguridad en entornos distribuidos

A. García, C. Alcaraz, J. López <i>MAS para la convergencia de opiniones y detección de anomalías en sistemas ciberfísicos distribuidos</i>	29
R. García Peñas, R.A. Rodríguez Gómez, G. Maciá Fernández <i>HODINT: Arquitectura distribuida para la recolección y análisis del tráfico de fondo de Internet</i>	37
A. Buitrago López, J. Pastor Galindo, F. Gómez Mármol <i>Exploring the availability, protocols and advertising of Tor v3 domains</i>	45
J. Bernabé Rodríguez, C. Regueiro Senderos, I. Seco Aguirre <i>Ampliando los límites de MP-SPDZ</i>	53

Sesión II: Inteligencia artificial y ciberseguridad I

L.A. Martínez Hernández, A.L. Sandoval Orozco, L.J. García Villalba <i>Técnicas de Inteligencia Artificial Supervisadas y No Supervisadas para el Análisis de Información Digital en Dispositivos de Almacenamiento</i>	61
Ó. Mogollón Gutiérrez, J. Alonso Díaz, J.C. Sancho Núñez, A. Caro Lindo <i>Una nueva propuesta para la detección y clasificación de ciberataques basada en ensemble learning</i>	69
L. Gutiérrez Galeano, J.J. Domínguez Jiménez, I. Medina Bulo <i>Detección de ciberataques mediante el uso de un modelo de procesamiento de lenguaje natural</i>	77
D. Escudero García, N. De Castro García <i>Aplicación de aprendizaje transferido a la asignación de maliciosidad de IPs</i>	85
F. González López, A.M. Mora García, R. Magán Carrión <i>Influencia de la selección de hiper-parámetros en el rendimiento de autoencoders para la detección de ataques en red</i>	93
R. Pérez Jove, C.R. Munteanu, J. Dorado, A. Pazos, J. Vázquez Naya <i>Operating System Fingerprinting Tool Based on Classical Machine Learning Algorithms</i>	101

Sesión III: Técnicas de ciberseguridad y ciencia forense I

S. Ruiz Villafranca, J.M. Castelo Gómez, J. Roldán Gómez <i>Automatizando las Investigaciones Forenses en Entornos IoT Mediante el Análisis del Tráfico de Red en Tiempo Real</i>	111
J.M. Velo, Á.J. Varela Vaca, R.M. Gasca <i>Ciberseguridad Cognitiva aplicada al Phishing</i>	119
S. Escuder Folch, A. Calvo Ibáñez, N. Ortiz Rabella, J. Escrig Escrig <i>Web Bot Detection Using Mouse Movement</i>	127
A. Míguez Díez, A. Campazas Vega, B. Jové De Castro, C. Álvarez Aparicio, I.S. Crespo Martínez, Á.M. Guerrero Higuera <i>Evaluación de la seguridad en el robot cuadrúpedo AI de Unitree Robotics</i>	133
Á. García, E. Rodríguez, S. Vidal, G. Álvarez <i>ARISTEO: Ciberseguridad industrial para la extracción de inteligencia y detección proactiva de amenazas</i>	139
X. Gandiaga, U. Zurutuza, I. Garitano <i>Habilitando honeypots embebidos de alta interacción mediante emulaciones de firmware</i>	145

Sesión IV: Transferencia I

M. Fuentes García, R. Magán Carrión, C. Fernández, D. Álvarez, M. Torres <i>SIMAGRO: Un prototipo para la detección de anomalías en entornos IoT para el sector agroalimentario</i>	155
M. Martín Pérez, J. Marias I Parella, J. Fernández, Jordi Casademont, A. Álvarez Romero, R. Díaz <i>A Testbed for a Nearby-Context Aware: Threat Detection and Mitigation System for Connected Vehicles</i>	163
N. Costas Lago, A. Gómez Tato <i>Infraestructuras de tecnologías cuánticas para la investigación en ciberseguridad</i>	171
P. de Juan Fidalgo, A. Pasic, J.M. del Álamo, R. Tourís, A. Álvarez <i>TERME: a cyber-physical resilience toolset for risk assessment</i>	179
J. Garcíandia, U. Zurutuza, G. Vidal <i>Desarrollo de ataques sobre la simulación de procesos industriales</i>	185
M.C. Palacios, M. Álvarez Piernavieja <i>Aplicación de Criptografía Homomórfica e Inteligencia Artificial para la Detección de Intrusiones en entornos OT</i>	193

Sesión V: Transferencia II

J. Porres, H. Saiz, C. Arellano, A. Urbietta, J.J. Rodríguez <i>Lamassu IoT: PKI de Código Abierto para Industria 4.0</i>	201
A. Pasic, N. Kourtellis <i>Collaborative Ranking of Results in Pilot Projects for the EU Cybersecurity Competence Community</i>	209
J. Murguía Hughes <i>Mantener la privacidad de la información aun cuando la seguridad haya sido vulnerada</i>	213
C.M. Alba Jiménez, D.C. Sánchez Ventura, L. Carriazo, A. Ortiz Aguilar <i>QuPIDE FLANBE para la preservación de la privacidad en Fintech</i>	221

M. Saavedra Golán, I. Ortega Fernández
Detección de bots avanzados en comercio electrónico: un caso de uso real 229

C. Regueiro, A. Gómez Goiri, S. de Diego, B. Urquijo
Compartición segura de suscripciones a plataformas audiovisuales con Self-Sovereign Identity 237

Sesión VI: Técnicas de ciberseguridad y ciencia forense II

R. López Rueda, S. Escobar
Canonical Narrowing with Irreducibility and SMT Constraints as a Generic Symbolic Protocol Analysis Method 247

D. Mateos Romero, G. Maciá Fernández
KVM-FUZZ: fuzzing de binarios x86-64 con emulación y aceleración por hardware 251

X. Etxezarreta, I. Garitano, M. Iturbe, U. Zurutuza
Evaluación del entorno de pruebas MiniCPS para el desarrollo de experimentos de seguridad de redes industriales definidas por software 259

S. López Bernal, V.M. López Madejska, G. Martínez Pérez, A. Huertas Celdrán
Avances en Ciberseguridad en Interfaces Cerebro-Máquina: Evolución y Trabajo Futuro 267

R. Gesteira Miñarro, G. López, R. Palacios
Ingeniería inversa sobre protocolos de radiofrecuencia para sistemas Remote Keyless Entry 275

P.M. Sánchez Sánchez, A. Huertas Celdrán, G. Bovet, G. Martínez Pérez, B. Stiller
A Trustworthy Federated Learning Framework for Individual Device Identification 281

Sesión VII: Inteligencia artificial y ciberseguridad II

M. Gorricho Segura, X. Echeberria Barrio, L. Seguro Gil
Edge-based Analysis for Network Intrusion Detection using a GNN Approach 291

F. Lemus Prieto, J. Sánchez Rivero, C. Castañares Cañas, A. Caro Lindo, J.L. González Sánchez
Detección de ataques en entornos IoT mediante técnicas de canal lateral y de Inteligencia Artificial 299

S. Pérez Arteaga, A.L. Sandoval Orozco, L.J. García Villalba
Análisis de Técnicas de Aprendizaje Automático para Clasificación de Información en Aplicaciones Móviles . 305

C. Piñón Blanco, F. Otero Vázquez, I. Ortega Fernández, M. Sestelo
Detecting Anomalies in Industrial Control Systems with LSTM Neural Networks and UEBA 313

I. Amonariz Pagola, J.Á. Fernández Carrasco
A Reinforcement Learning Approach for Network Slicing in 5G Networks 321

N. Reyes Dorta, P. Caballero Gil, C. Rosa Remedios
Detección de URLs fraudulentas mediante Machine Learning 329

Sesión VIII: Gestión avanzada de riesgos y seguridad

C. Sánchez Zas, X. Larriva Novo, V. Villagrà, M. Sanz Rodrigo, S. Solera Cotanilla
Desarrollo de una ontología para modelar una metodología interoperable de gestión dinámica de riesgos . . 339

M. Robles Carrillo, G. Maciá Fernández, R. Magán Carrión, R.A. Rodríguez Gómez, J.A. Gómez Hernández, P. García Teodoro
El Marco Europeo de Identidad Digital: análisis del enfoque coordinado a través del Toolbox de la UE . . . 347

J.S. Zurdo, J. San Martín <i>CIO-Rank una herramienta para monitorizar las entidades locales dentro de la Directiva NIS2</i>	355
V. García Fernández, N. Rodríguez Pérez, R. Gesteira Miñarro, J. Matanza Domingo, R. Palacios Hielscher, G. López López <i>Dynamic risk assessment tool for customer IoT infrastructures for Smart Grids</i>	363
M. Robles Carrillo <i>Análisis de la Directiva (UE) 2022/2055 sobre las medidas para garantizar un elevado nivel común de ciberseguridad en la Unión Europea (NIS 2)</i>	367
E. Castillo Fernández, J. Díaz Verdejo, R. Estepa Alonso, A. Estepa Alonso <i>Riesgos en la Smart Home: estudio experimental</i>	375
E.T. Martínez Beltrán, P.M. Sánchez Sánchez, S. López Bernal, G. Bovet, M. Gil Pérez, G. Martínez Pérez, A. Huertas Celdrán <i>Framework Seguro para Entrenar Modelos de Inteligencia Artificial Federados y Descentralizados</i>	383

Sesión IX: Criptografía en la era cuántica

G. Luis Freitas, P. Caballero Gil, J. Molina Gil <i>Propuesta de mejora para la implementación en software del cifrado SNOW-Vi</i>	393
M.A. Serrano, L.E. Sánchez, A. Santos Olmo, D. García Rosado, C. Blanco, V. Santa Barletta, D. Caivano, E. Fernández Medina <i>Minimización del tiempo de respuesta a incidentes en entornos reales usando computación cuántica</i>	401
V. Marchan Sekulic, P. Caballero Gil, D. Escáñez Expósito <i>Implementación de los Algoritmos Cuáticos de Simon y de Shor</i>	409
A. Hernández Martín, P. Caballero Gil, D. Escáñez Expósito <i>Implementación del protocolo criptográfico Six-State</i>	415
V. García, S. Escobar <i>Analysis and verification of code-based key encapsulation mechanism BIKE in Maude</i>	421
M. Caruso, M. Torres Anaya, D. Álvarez León, C. Fernández Rosales <i>Criptografía para las cosas</i>	429

Sesión X: Innovación educativa

P. Martínez Sánchez, P. Nespoli, J. García Alfaro, F. Gómez Mármol <i>Metodología para automatizar agentes atacantes en plataformas de entrenamiento Cyber Range</i>	437
E. Castillo Fernández, E. Muñoz, J. Díaz Verdejo, R. Estepa Alonso, A. Estepa Alonso <i>Diseño y despliegue de un laboratorio para formación e investigación en ciberseguridad</i>	445
R. Gaspar Marco, M. Albaladejo González, P. Nespoli, J.A. Ruipérez Valiente <i>Agentes de Aprendizaje por Refuerzo en Cyber Ranges para la Formación Realista en Ciberseguridad</i>	453
D. Sobrín Hidalgo, L. Fernández Becerra, M.Á. González Santamarta, C. Álvarez Aparicio, Á.M. Guerrero Higuera, M.Á. Conde González, F.J. Rodríguez Lera, V. Matellán Olivera <i>Ciberseguridad en sistemas ciberfísicos: entorno simulado para la evaluación de competencias en ciberseguridad en sistemas con capacidades autónomas</i>	461

M. Fernández Tárraga, A.D. Cayuela Tudela, P. Nespoli, J. García Alfaro, F. Gómez Mármol <i>Entrenamiento bajo demanda en competencias de ciberseguridad en redes sociales</i>	469
--	-----

Programa científico: pósters

Sesión I: Investigación publicada I

J. Reverte Cazorla, J.M. de Fuentes, L. González Manzano <i>Summary of: Eye-based keystroke prediction for natural texts – a feasibility analysis</i>	481
M.I. García Cid, M. Gil Pérez, J.M. Jorquera Valero, A. López Martínez, J. Maestre Vidal, G. Martínez Pérez, L. Méndez García, F. Muñoz Plaza, P. Nespoli, J. Pastor Galindo, P.J. Ramón y Cajal Ramo, F.A. Rodríguez López, P.M. Sánchez Sánchez, M.A. Sotelo Monge <i>European framework and proofs-of-concept for the intelliGent aUtomAtion of cybeR Defence Incident mAnagemeNt</i>	483
A. Martínez Mendoza, F. Jáñez Martino, R. Alaiz Rodríguez, V. González Castro, E. Fidalgo, E. Alegre <i>A survey on spam detection, spammer strategies and the dataset shift problem</i>	485
A. Martínez Mendoza, M. Sánchez Paniagua, A. Carofilis, F. Jáñez Martino, E. Fidalgo, E. Alegre <i>Applying Machine Learning to login URLs for phishing detection</i>	487
D.G. Rosado, A. Santos Olmo, L.E. Sánchez, M.A. Serrano, C. Blanco, H. Mouratidis, E. Fernández Medina <i>Managing Cybersecurity Risks of Cyber-Physical Systems: The MARISMA-CPS pattern</i>	489

Sesión II: Investigación publicada II

P. de Juan Fidalgo, C. Cámara, P. Peris López <i>A Review Of "Generation and Classification of Illicit Bitcoin Transactions"</i>	493
A. Ranea, V. Rijmen <i>Characteristic automated search of cryptographic algorithms for distinguishing attacks (CASCADA)</i>	495
A. Carofilis, D. Chaves, A. Martínez Mendoza, E. Fidalgo, V. González Castro, E. Alegre <i>Impact of facial occlusions in age estimation algorithms for forensic applications</i>	497
J. Carrillo Mondéjar, H. Turitainen, A. Costin, J.L. Martínez, G. Suárez Tangil <i>A Review of "HALE-IoT: HArdening LEgacy Internet-of-Things devices by retrofitting defensive firmware modifications and implants"</i>	499
R. Raducu, R.J. Rodríguez, P. Álvarez <i>A Review of "Defense and Attack Techniques Against File-Based TOCTOU Vulnerabilities: A Systematic Review"</i>	501
J.M. Jorquera Valero, P.M. Sánchez Sánchez, M. Gil Pérez, A. Huertas Celdrán, G. Martínez Pérez <i>A Review of "Toward Pre-standardization of Reputation-based Trust Models Beyond 5G"</i>	503

Sesión III: Investigación original I

É. Pérez Ramos, P. Caballero Gil <i>Estudio del esquema de firma CRYSTALS-Dilithium</i>	507
---	-----

J.G. Medina Arco, R. Magán Carrión, R.A. Rodríguez Gómez <i>Explorando anomalías ocultas en UGR'16 con Kitsune</i>	515
S. de Diego, Ó. Lage, C. Regueiro, S. Anguita, G. Maciá Fernández <i>Bypassing current limitations for implementing a credential delegation for the Industry 4.0</i>	523
D. Álvarez Pérez, M. Fernández Veiga, A. Fernández Vilas <i>Structures of the data and the information reuse based in-memory fuzzing</i>	525
F. Jáñez Martino, L.Á. Redondo Gutiérrez, A. Martínez Mendoza, L. Fernández Robles, E. Fidalgo, E. Alegre <i>Malware detection in spam emails using natural language processing</i>	529
M. Rivera Dourado, M. Gestal, A. Pazos, J. Vázquez Naya <i>Adapting a Captive Portal for Phishing-Resistant Network Authentication Using Security Keys</i>	531
R. García Mateo, A. Echeverría Rey <i>Boosted CSIRT with AI powered open source framework</i>	539
A. Huertas Celdrán, P.M. Sánchez Sánchez, C. Feng, G. Bovet, G. Martínez Pérez, B. Stiller <i>A Summary of Privacy-preserving and Syscall-based Intrusion Detection System for IoT Sensors Affected by Data Falsification Attacks</i>	547

Sesión IV: Investigación original II

D. García, A. Robles Gómez, L. Tobarra, R. Pastor Vargas <i>Automatización de la adquisición de evidencias para el análisis forense</i>	551
J. Alonso Díaz, Ó. Mogollón Gutiérrez, J.C. Sancho Núñez, A. Caro Lindo <i>Adaptación y evaluación de un modelo de madurez DevSecOps a las particularidades de proyectos software</i>	553
A. Calvo, N. Ortiz, A. Espinosa, A. Dimitrievikj, I. Oliva, J. Guijarro, S. Sidiqqi <i>Safe AI: Ensuring Safe and Responsible Artificial Intelligence</i>	557
D. Povedano Álvarez, A.L. Sandoval Orozco, L.J. García Villalba <i>Detección de Contenido Sexual Explícito mediante Técnicas de Aprendizaje Profundo</i>	561
A. Pérez Sánchez, R. Palacios Hielscher, G. López López <i>Evaluation of Local Security Event Management System vs. Standard Antivirus Software</i>	569
L.F. Rojas Muñoz, S. Sánchez Solano, M.C. Martínez Rodríguez, P. Brox <i>Análisis y evaluación de un RO-PUF como TRNG</i>	571
J.A. Font, J. Jarauta, R. Gesteira, R. Palacios, G. López <i>Threat models for vulnerability analysis of IoT devices for Manipulation of Demand attacks</i>	573

Sesión V: Investigación original III

I. Seco Aguirre, J. Bernabé Rodríguez, C. Regueiro Senderos, E. Jacob Taquet <i>Implementación de un algoritmo de machine learning utilizando criptografía homomórfica</i>	583
M.Á. Cañabate Rabell <i>Directiva NIS 2: Marco general, estructura orgánica y cooperación en un análisis comparativo</i>	591

A. Martínez Mendoza, M. Sánchez Paniagua, F. Jáñez Martino, R. Alaiz Rodríguez, E. Fidalgo, E. Alegre <i>Novel benchmark dataset and features to detect phishing on webpages</i>	599
X. Larriva Novo, A. Vara Plaza, Ó. Jover, C. Sánchez Zas, V.A. Villagrà <i>Simulador de APTs realistas avanzados basado en el marco de MITRE ATT&CK</i>	601
A. Pérez Sánchez, R. Palacios Hielscher, G.I. López López <i>Dataset para el análisis de eventos maliciosos en sistemas Windows basados en la matriz de MITRE</i>	609
F. Martínez, L.E. Sánchez, A. Santos Olmo, D.G. Rosado, E. Fernández Medina <i>Ciberseguridad Marítima: Antecedentes y estrategias de una respuesta global a una necesidad mundial</i>	617

Call for Flags

Retos CFF

A. Parra Sánchez <i>FlaskCh4r - CTF Challenge</i>	629
R. Raducu, M. Sánchez Paniagua <i>Full Stack Tester</i>	643
A.J. Di Bartolo <i>Dockerstyle</i>	659
R.A. Rodríguez Gómez <i>Descifrando TLS: Cuando nos facilitan la factorización entera...</i>	677
R. Gesteira Miñarro <i>Is this Crypto?</i>	689
D. Mohedano Vázquez, L. González Manzano <i>Buffer Overflow a Check DNI</i>	699
D. Mohedano Vázquez, L. González Manzano <i>Buffer Overflow a IP info</i>	717
G. Aguilar <i>BashDFir</i>	731
Á. González Bravo <i>CTF Análisis de código</i>	739

Premios RENIC a la mejor tesis doctoral y el mejor trabajo de fin de máster

P. González López <i>Técnica basada en modelos de características para validar y diagnosticar la configuración de un sistema cliente-servidor de autenticación e identificación biométrica</i>	749
J.E. Rubio Cortés <i>Analysis and Design of Security Mechanisms in the Context of Advanced Persistent Threats Against Critical Infrastructures</i>	757

Managing Cybersecurity Risks of Cyber-Physical Systems: The MARISMA-CPS pattern

David G. Rosado
GSyA Research Group
UCLM, Ciudad Real, España
david.grosado@uclm.es

Antonio Santos-Olmo
GSyA Research Group
UCLM, Ciudad Real, España
antonio.santosolmo@uclm.es

Luis Enrique Sánchez
GSyA Research Group
UCLM, Ciudad Real, España
luise.sanchez@uclm.es

Manuel A. Serrano
Alarcos Research Group
UCLM, Ciudad Real, Spain
manuel.serrano@uclm.es

Carlos Blanco
ISTR research group
University of Cantabria, Santander, España
carlos.blanco@unican.es

Haralambos Mouratidis
Institute for Analytics and Data Science
University of Essex, Colchester, UK
h.mouratidis@essex.ac.uk

Eduardo Fernández-Medina
GSyA Research Group
UCLM, Ciudad Real, España
eduardo.fdezmedina@uclm.es

Abstract—Cyber-physical systems (CPSs) have an increasingly presence on critical infrastructures and an impact in almost every aspect of our daily life. However, CPSs face a growing and serious security issue due to the widespread connectivity between the cyber world and the physical world. Although risk assessment methods for traditional IT systems are now very mature, these are not adequate for risk assessment of CPSs due to the different characteristics of the later. In this paper we propose a novel risk analysis technique for CPSs based on MARISMA, a security management methodology. Our work proposes the definition of the MARISMA-CPS pattern that incorporates a set of reusable and adaptable elements that allows risks in CPSs to be managed and controlled. A case study for a smart hospital is presented, showing how the reusability and adaptability of the proposal allows the proposed MARISMA-CPS pattern to be easily adapted to any CPS environment.

Index Terms—Risk analysis, Risk assessment, MARISMA, Cyber-Physical System

Type of contribution: *Research already published.*

I. INTRODUCTION

CPSs are smart systems that include computing, storage, and communication features which can monitor and/or manage objects in the physical world, and which can build a wide range of innovative applications and services that are available for citizens and businesses alike.

Cybersecurity plays a key role in making companies more competitive, and is, therefore, a fundamental discipline because of its role in concincing users that CPS, their information, and the supporting communications and information infrastructures be fully protected.

An appropriate risk assessment of CPS should provide a comprehensive understanding of the CPS security status and support the effective allocation of protected resources. Although risk assessments in traditional IT systems are mature a distinct and novel risk analysis and management (RAM) method for CPSs is needed in order to cover the growing security issues that arise due to the large differences between IT systems and CPS.

II. MARISMA FRAMEWORK

We have developed a methodology called "MARISMA" which is a RAM methodology that can be adapted to any type of IT environment which defines the meta-pattern, in which

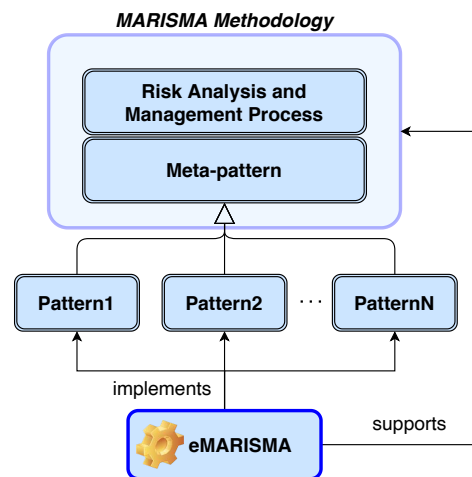


Fig. 1. General schema of MARISMA methodology.

security controls are considered from the beginning of the risk analysis process, and which allows the reuse of artefacts and the definition of patterns for specific contexts. Moreover, as it is supported by the eMARISMA tool, the process and decision making are made agile and simple (see Fig. 1).

III. MARISMA-CPS PATTERN

This work defines a specific pattern (MARISMA-CPS) aiming to provide a complete RAM environment based on the MARISMA methodology. The proposed pattern allows risks in CPS to be managed and controlled. To build the pattern from the elements defined in the meta-pattern, the first thing to do is to review the literature, search for standards, recommendations, proposals and good practices in the context of RAM, trying to focus the search towards IoT and CPS environments to find domain standards and appropriate controls for CPSs, taxonomies of assets, threats and dimensions, which are the main elements of the meta-pattern. For the MARISMA-CPS pattern we have been guided by the ENISA and NIST recommendations for IoT and ISO/IEC 27.000 and IEC 62443 standards, where they establish sets of possible

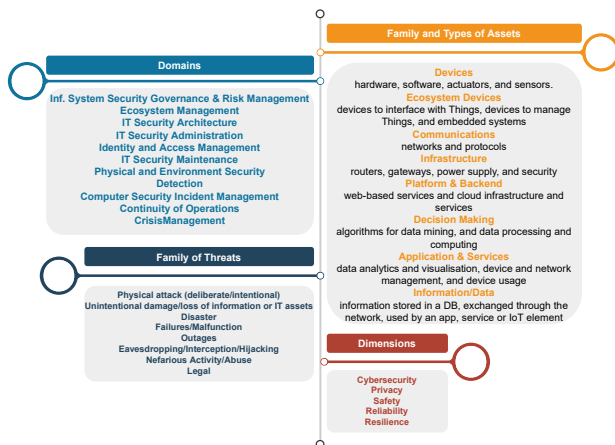


Fig. 2. Components of the MARISMA-CPS pattern

controls, taxonomies of assets, threats, dimensions, etc. that can serve as a first approximation for the construction of the pattern. eMARISMA tool facilitates the creation of the pattern and manages and relates all the elements of the pattern in a simple, intuitive and direct way. The elements considered for the MARISMA-CPS pattern are shown in the Fig. 2.

- Domains, control objectives, and controls: there are 3 categories: Policy-related controls (PS) with 12 controls, Organisational controls (OP) with 14 controls, and Technical controls or measures (TM) with 57 controls.
- Families and types of asset: Devices, Ecosystem Devices, Communications, Infrastructure, Platform & Backend, Decision Making, Applications & Services, and Information/Data.
- For the dimensions of the MARISMA-CPS pattern, we have considered in light of Trustworthiness which is defined in the framework for CPSs published by the NIST. The dimensions considered are: Cybersecurity, Privacy, Safety, Reliability and Resilience.
- Families and types of threats: classification of threat families into 7 groups: Physical attack, Damage loss (IT assets), Disaster, Failures/malfunction, Outages, Eavesdropping/interception/hijacking, Nefarious activity/abuse, and Legal.

In order to complete the pattern, it is necessary to define the objectives, domains and threats matrix, which establishes the dependency relationship not only among controls but also among threats. Another matrix that needs to be defined for MARISMA is the matrix of type of assets, type of threats and dimensions, which establishes the existing relationships among the types of threats and dimensions that for each type of asset are those most likely to be attacked. These matrices must also be defined in eMARISMA tool.

IV. CASE STUDY

The next step is to instantiate the pattern to a concrete case, for which we have chosen a smart hospital which seeks to improve existing patient care procedures, and create more sustainable, more secure and more intelligent healthcare facilities by introducing new capabilities that are achieved through optimised and automated processes built in an ICT

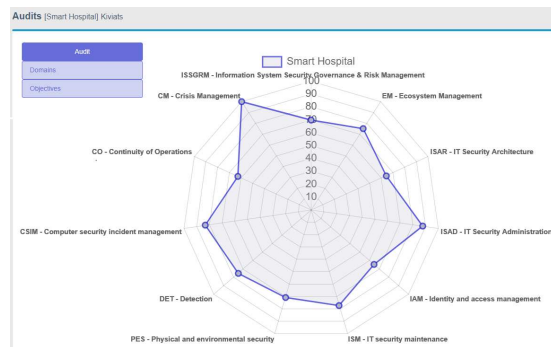


Fig. 3. Levels of coverage with Kiviat diagrams for the case study

environment of interconnected assets, mostly IoT. In order to do so, it is necessary to study in depth the types of assets involved in the system and to analyse and identify the types of threats that may affect the system and cause damage to the assets.

When using the MARISMA-CPS pattern to perform the risk analysis, as soon as the assets have been added to the tool, the relationships established in the pattern among assets, threats and dimensions will serve to allow the tool to start executing the risk analysis with the assets in the case study. The tool will show the results of the current risk for this set of assets in real-time. The tool provides a dashboard that shows the real-time coverage levels of the controls in real-time, allowing them to be tracked graphically and visually. It also allows a visualisation of the current level by means of kiviati diagrams in three categories: (i) by overall audit (see Fig. 3); (ii) by domain; and (iii) by control objectives.

V. CONCLUSIONS

We have developed a pattern totally oriented towards CPS, using as a basis to the meta-pattern of the MARISMA methodology. This pattern is made up of three taxonomic catalogues (controls, assets and threats) evolved from international standards and recommendations and oriented towards CPS. The dependency matrices between the elements of the pattern have also been obtained, which allows it to obtain the necessary properties for the reuse of knowledge and its subsequent adaptation over time. Its integration within the MARISMA framework, and the tool that supports it, has allowed its validation in practical cases.

AGRADECIMIENTOS

This work has been developed within the AETHER-UCLM (PID2020-112540RB-C42), ALBA-UCLM (TED2021-130355B-C31) and ALBA-UC (TED2021-130355A-C33) funded by MCIN/AEI/10.13039/501100011033/Unión Europea NextGenerationEU/PRTR, Spain, and supported by the European Union's Horizon 2020 Project "CyberSANE" under Grant Agreement No.833683.

REFERENCES

- [1] Rosado, D. G., Santos-Olmo, A., Sánchez, L. E., Serrano, M. A., Blanco, C., Mouratidis, H., Fernández-Medina, E. "Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern", en *Computers in Industry*, 142, 103715, 2022. (2021 Journal Impact Factor: 11.245) <https://doi.org/10.1016/J.COMPIND.2022.103715>

Índice de autores

A

Aguilar, G., 731
Alaiz Rodríguez, R., 485, 599
Alba Jiménez, C.M., 221
Albaladejo González, M., 453
Alcaraz, C., 29
Alegre, E., 485, 487, 497, 529, 599
Alonso Díaz, J., 69, 553
Álvarez Aparicio, C., 133, 461
Álvarez León, D., 429
Álvarez Pérez, D., 525
Álvarez Piernavieja, M., 193
Álvarez Romero, A., 163
Álvarez, A., 179
Álvarez, D., 155
Álvarez, G., 139
Álvarez, P., 501
Amonariz Pagola, I., 321
Anguita, S., 523
Arellano, C., 201

B

Bernabé Rodríguez, J., 53, 583
Blanco, C., 401, 489
Bovet, G., 281, 383, 547
Brox, P., 571
Buitrago López, A., 45

C

Caballero Gil, P., 329, 393, 409, 415, 507
Caivano, D., 401
Calvo Ibáñez, A., 127
Calvo, A., 557
Cámara, C., 493
Campazas Vega, A., 133
Cañabate Rabell, M.Á., 591
Caro Lindo, A., 69, 299, 553
Carofilis, A., 487, 497
Carriazo, L., 221
Carrillo Mondéjar, J., 499
Caruso, M., 429
Casademont, Jordi, 163
Castañares Cañas, C., 299
Castelo Gómez, J.M., 111
Castillo Fernández, E., 375, 445
Cayuela Tudela, A.D., 469
Chaves, D., 497
Conde González, M.Á., 461
Costas Lago, N., 171
Costin, A., 499

Crespo Martínez, I.S., 133

D

De Castro García, N., 85
de Diego, S., 237, 523
de Fuentes, J.M., 481
de Juan Fidalgo, P., 179, 493
del Álamo, J.M., 179
Di Bartolo, A.J., 659
Díaz Verdejo, J., 375, 445
Díaz, R., 163
Dimitrievikj, A., 557
Domínguez Jiménez, J.J., 77
Dorado, J., 101

E

Echeberria Barrio, X., 291
Echeverría Rey, A., 539
Escáñez Expósito, D., 409, 415
Escobar, S., 247, 421
Escrig Escrig, J., 127
Escuder Folch, S., 127
Escudero García, D., 85
Espinosa, A., 557
Estepa Alonso, A., 375, 445
Estepa Alonso, R., 375, 445
Etchezarreta, X., 259

F

Feng, C., 547
Fernández Becerra, L., 461
Fernández Carrasco, J.Á., 321
Fernández Medina, E., 401, 489, 617
Fernández Robles, L., 529
Fernández Rosales, C., 429
Fernández Tárraga, M., 469
Fernández Veiga, M., 525
Fernández Vilas, A., 525
Fernández, C., 155
Fernández, J., 163
Fidalgo, E., 485, 487, 497, 529, 599
Font, J.A., 573
Fuentes García, M., 155

G

G. Martínez Pérez, 383
Gandiaga, X., 145
García Alfaro, J., 437, 469
García Cid, M.I., 483
García Fernández, V., 363

García Mateo, R., 539
García Peñas, R., 37
García Rosado, D., 401
García Teodoro, P., 347
García Villalba, L.J., 61, 305, 561
García, A., 29
García, Á., 139
García, D., 551
García, V., 421
Garcíandia, J., 185
Garitano, I., 145, 259
Gasca, R.M., 119
Gaspar Marco, R., 453
Gestal, M., 531
Gesteira Miñarro, R., 275, 363, 689
Gesteira, R., 573
Gil Pérez, M., 383, 483, 503
Gómez Goiri, A., 237
Gómez Hernández, J.A., 347
Gómez Mármol, F., 45, 437, 469
Gómez Tato, A., 171
González Bravo, Á., 739
González Castro, V., 485, 497
González López, F., 93
González López, P., 749
González Manzano, L., 481, 699, 717
González Sánchez, J.L., 299
González Santamarta, M.Á., 461
Gorricho Segura, M., 291
Guerrero Higuera, Á.M., 133, 461
Guijarro, J., 557
Guri, Mordechai, 17
Gutiérrez Galeano, L., 77

H

Hernández Martín, A., 415
Huertas Celdrán, A., 267, 281, 383, 503, 547

I

Iturbe, M., 259

J

Jacob Taquet, E., 583
Jáñez Martino, F., 485, 487, 529, 599
Jarauta, J., 573
Jorquera Valero, J.M., 483, 503
Jové De Castro, B., 133
Jover, Ó., 601

K

Kourtellis, N., 209

L

Lage, Ó., 523

Larriva Novo, X., 339, 601
Lemus Prieto, F., 299
López Bernal, S., 267, 383
López López, G., 363, 569
López López, G.I., 609
López Madejska, V.M., 267
López Martínez, A., 483
López Rueda, R., 247
López, G., 275, 573
López, J., 29
Luis Freitas, G., 393

M

Maciá Fernández, G., 37, 251, 347, 523
Maestre Vidal, J., 483
Magán Carrión, R., 93, 155, 347, 515
Marchan Sekulic, V., 409
Marias I Parella, J., 163
Martín Pérez, M., 163
Martínez Beltrán, E.T., 383
Martínez Hernández, L.A., 61
Martínez Mendoza, A., 485, 487, 497, 529, 599
Martínez Pérez, G., 267, 281, 483, 503, 547
Martínez Rodríguez, M.C., 571
Martínez Sánchez, P., 437
Martínez, F., 617
Martínez, J.L., 499
Matanza Domingo, J., 363
Matellán Olivera, V., 461
Mateos Romero, D., 251
Medina Arco, J.G., 515
Medina Buló, I., 77
Méndez García, L., 483
Míguez Díez, A., 133
Mogollón Gutiérrez, Ó., 69, 553
Mohedano Vázquez, D., 699, 717
Molina Gil, J., 393
Mora García, A.M., 93
Mouratidis, H., 489
Muñoz Plaza, F., 483
Muñoz, E., 445
Munteanu, C.R., 101
Murguía Hughes, J., 213

N

Nespoli, P., 437, 453, 469, 483

O

Oliva, I., 557
Ortega Fernández, I., 229, 313
Ortiz Aguilar, A., 221
Ortiz Rabella, N., 127
Ortiz, N., 557
Otero Vázquez, F., 313

P

Palacios Hielscher, R., 363, 569, 609
Palacios, M.C., 193
Palacios, R., 275, 573
Parra Sánchez, A., 629
Pasic, A., 179, 209
Pastor Galindo, J., 45, 483
Pastor Vargas, R., 551
Pazos, A., 101, 531
Pérez Arteaga, S., 305
Pérez Jove, R., 101
Pérez Ramos, É., 507
Pérez Sánchez, A., 569, 609
Peris López, P., 493
Piñón Blanco, C., 313
Porres, J., 201
Povedano Álvarez, D., 561

R

Raducu, R., 501, 643
Ramón y Cajal Ramo, P.J., 483
Ranea, A., 495
Redondo Gutiérrez, L.Á., 529
Regueiro Senderos, C., 53, 583
Regueiro, C., 237, 523
Reverte Cazorla, J., 481
Reyes Dorta, N., 329
Rijmen, V., 495
Rivera Dourado, M., 531
Robles Carrillo, M., 347, 367
Robles Gómez, A., 551
Rodríguez Gómez, R.A., 37, 347, 515, 677
Rodríguez Lera, F.J., 461
Rodríguez López, F.A., 483
Rodríguez Pérez, N., 363
Rodríguez, E., 139
Rodríguez, J.J., 201
Rodríguez, R.J., 501
Rojas Muñoz, L.F., 571
Roldán Gómez, J., 111
Rosa Remedios, C., 329
Rosado, D.G., 489, 617
Rubio Cortés, J.E., 757
Ruipérez Valiente, J.A., 453
Ruiz Villafranca, S., 111

S

Saavedra Golán, M., 229
Saiz, H., 201

San Martín, J., 355
Sánchez Paniagua, M., 487, 599, 643
Sánchez Rivero, J., 299
Sánchez Sánchez, P.M., 281, 383, 483, 503, 547
Sánchez Solano, S., 571
Sánchez Ventura, D.C., 221
Sánchez Zas, C., 339, 601
Sánchez, L.E., 401, 489, 617
Sancho Núñez, J.C., 69, 553
Sandoval Orozco, A.L., 61, 305, 561
Santa Barletta, V., 401
Santos Olmo, A., 401, 489, 617
Sanz Rodrigo, M., 339
Seco Aguirre, I., 53, 583
Seguro Gil, L., 291
Serrano, M.A., 401, 489
Sestelo, M., 313
Sidiqqi, S., 557
Sobrin Hidalgo, D., 461
Solera Cotanilla, S., 339
Sotelo Monge, M.A., 483
Stiller, B., 281, 547
Suárez Tangil, G., 499

T

Tobarra, L., 551
Torres Anaya, M., 429
Torres, M., 155
Tourís, R., 179
Troncoso, Carmela, 19
Turitainen, H., 499

U

Urbieta, A., 201
Urquijo, B., 237

V

Vara Plaza, A., 601
Varela Vaca, Á.J., 119
Vázquez Naya, J., 101, 531
Velo, J.M., 119
Vidal, G., 185
Vidal, S., 139
Villagrà, V., 339
Villagrà, V.A., 601

Z

Zurdo, J.S., 355
Zurutuza, U., 145, 185, 259