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

Jornadas Nacionales de Investigación en Ciberseguridad

JNIC2023

ACTAS DE LAS VIII JORNADAS NACIONALES DE INVESTIGACIÓN EN CIBERSEGURIDAD

Vigo, 21 a 23 de junio de 2023

ISBN: 978-84-8158-970-2

gradiant

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

atlanTTic
Universidade Vigo

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

Patrocinadores

Patrocinio técnico

Comités técnicos

Comité de programa científico

Manuel Fernández Veiga	atlanTTic, UVigo
José María de Fuentes	Universidad Carlos III de Madrid
Lilian Adkinson	GRADIANT
Cristina Alcaraz	Universidad de Málaga
Ana Ayerbe	TECNALIA
Marta Beltrán	Universidad Rey Juan Carlos
Carlos Blanco	Universidad de Cantabria
Jorge Blasco	Universidad Politécnica de Madrid
Pino Caballero	Universidad de La Laguna
Agustín Cañas	GRADIANT
Andrés Caro	Universidad de Extremadura
Jesús Esteban Díaz	Universidad de Granada
Josep Lluís Ferrer	Universitat de les Illes Balears
Joaquín García-Alfaro	Telecom-Sud Paris
David García	Universidad de Castilla-La Mancha
Luis Javier García	Universidad Complutense de Madrid
Manuel Gil	Universidad de Murcia
Félix Gómez	Universidad de Murcia
Lorena González	Universidad Carlos III de Madrid
Luis Hernández	CSIC
Javier López	Universidad de Málaga
Jorge López	Verisure
Agustín Martín	CSIC
Gregorio Martínez	Universidad de Murcia
David Megías	Universitat Oberta de Catalunya
Pantaleón Nespoli	Universidad de Murcia
Francisco J. Nóvoa	Universidade da Coruña
Raúl Orduña	VICOMTECH
Inés Ortega	GRADIANT
Luis Panizo	Universidad de León
Aljosa Pasic	ATOS
Luis Pérez Freire	GRADIANT
Fernando Pérez González	atlanTTic y Universidade de Vigo
Cristina Regueiro	TECNALIA
Erkuden Ríos	TECNALIA
Margarita Robles	Universidad de Granada
Ricardo J. Rodríguez	Universidad de Zaragoza
Luis E. Sánchez	Universidad de Castilla-La Mancha
Miquel Soriano	Universitat Politécnica de Catalunya
Juan Ramón Troncoso	Tuneinsight
Narseo Vallina	IMDEA
José M. Vázquez-Naya	Universidade da Coruña
Víctor Villagrá	Universidad Politécnica de Madrid
Urko Zurutuza	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 Urbieta	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 Ruiz	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

Mesas Redondas

Programa científico

Sesión I: Seguridad en entornos distribuidos

Sesión II: Inteligencia artificial y ciberseguridad I

Sesión III: Técnicas de ciberseguridad y ciencia forense I

Sesión IV: Transferencia I

Sesión V: Transferencia II

Sesión VI: Técnicas de ciberseguridad y ciencia forense II

Sesión VII: Inteligencia artificial y ciberseguridad II

Sesión VIII: Gestión avanzada de riesgos y seguridad

Sesión IX: Criptografía en la era cuántica

Sesión X: Innovación educativa

Programa científico: pósters

Sesión I: Investigación publicada I

Sesión II: Investigación publicada II

Sesión III: Investigación original I

Sesión IV: Investigación original II

Sesión V: Investigación original III

Call for Flags

Retos CFF

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

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 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).

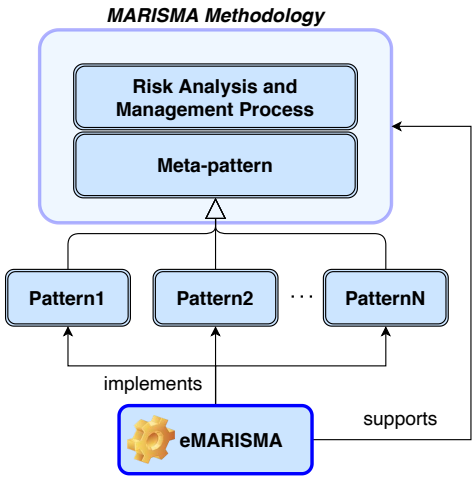

Fig. 1. General schema of MARISMA methodology.

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

ISBN:978-84-8158-970-2

Fig. 2. Components of the MARISMA-CPS pattern

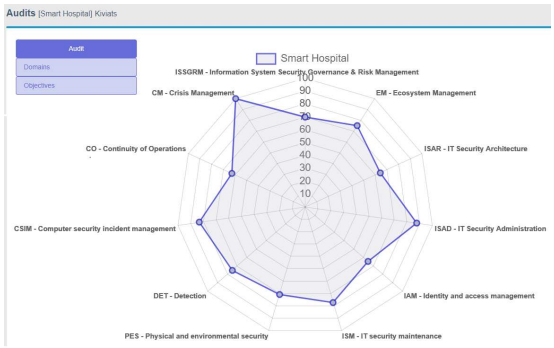

Fig. 3. Levels of coverage with Kiviat diagrams for the case study

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: Cibersecurity, 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 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 kiviat 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