Grupo de Especial Interés en Ciberseguridad (SIGCYBSEC)

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

IDENTIFICACIÓN DEL EQUIPO INVESTIGADOR

NOMBRE DEL EQUIPO O GRUPO DE INVESTIGACIÓN	**Grupo de Especial Interés en Ciberseguridad (SIGCYBSEC)**
UNIDAD/DEPARTAMENTO DE PERTENENCIA	**Dpto. de Informática e Ingeniería de Sistemas y Dpto. de Ingeniería Electrónica y Comunicaciones**
CENTRO/INSTITUTO/UNIVERSIDAD/ORGANISMO DE PERTENENCIA	**Escuela de Ingeniería y Arquitectura, Universidad de Zaragoza**

DATOS DE CONTACTO

DATOS DE CONTACTO DEL EQUIPO

PERSONA DE CONTACTO	**Ricardo Julio Rodríguez Fernández**	TELÉFONO	976 76 1953
ROL EN EL EQUIPO	Coordinador local de RENIC	MAIL	rjrodriguez@unizar.es
WEB DEL EQUIPO	www.reversea.me		

DIRECCIÓN POSTAL DEL EQUIPO

EDIFICIO	Ada Byron	CENTRO	EINA
TIPO DE VÍA	Calle	NOMBRE DE LA VÍA	María de Luna
NÚMERO	1	CIUDAD	Zaragoza
PROVINCIA	Zaragoza	CÓDIGO POSTAL	50018

DATOS DE CONTACTO DEL ORGANISMO AL QUE PERTENECE

PERSONA DE CONTACTO	Gloria Cuenca Bescós (Vicerrectora de Transferencia e Innovación Tecnológica)
MAIL	vrtit@unizar.es
TELÉFONO	
WEB	

DIRECCIÓN POSTAL DEL ORGANISMO

EDIFICIO	Interfacultades	CENTRO	Campus San Francisco
TIPO DE VÍA	Calle	NOMBRE DE LA VÍA	Pedro Cerbuna
NÚMERO	12	CIUDAD	Zaragoza
PROVINCIA	Zaragoza	CÓDIGO POSTAL	50009

Grupo de Especial Interés en Ciberseguridad (SIGCYBSEC)

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

INVESTIGADOR PRINCIPAL

NOMBRE	TITULACIÓN
Ricardo Julio Rodríguez Fernández	Ingeniero en Informática, Doctor en Ingeniería e Informática de Sistemas

TRAYECTORIA PROFESIONAL

Doctor en Informática e Ingeniería de Sistemas por la Universidad de Zaragoza desde 2013. Actualmente, trabaja como Profesor Titular en la misma universidad. Participa como ponente habitual y profesor de talleres técnicos en numerosas conferencias de seguridad del sector industrial. Su experiencia profesional incluye la participación en diversos Proyectos de I+D tanto nacionales como internacionales y tanto de financiación pública (H2020, Ministerio de Ciencia e Innovación, Ministerio de Industria) como privada (colaboraciones con INCIBE y Centro Criptológico Nacional) como IP y como parte del equipo investigador. Es autor (o coautor) en 40 publicaciones internacionales en revistas y/o congresos del área, realizando tareas de revisión en diversas revistas internacionales de prestigio e indexadas en JCR. Sus intereses de investigación incluyen análisis de seguridad de sistemas mediante métodos formales, el análisis forense digital y el análisis de aplicaciones.

WEB Y REDES SOCIALES

https://ricardojrdez.github.io
www.reversea.me
https://twitter.com/reverseame

MIEMBROS DEL EQUIPO

Alesanco Iglesias, Álvaro	García Moros, José	Gran Tejero, Rubén
Razvan Raducu, Razvan	Salazar Riaño, José Luis	Suárez Gracia, Darío
Uroz Hinarejos, Daniel		

Grupo de Especial Interés en Ciberseguridad (SIGCYBSEC)		
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 Ciencia Forense Desarrollo de defensas automáticas Nuevos tipos de Malware Filtraciones de Información IDS/IPS/Firewalls
EVALUACIÓN DE SISTEMAS Y CIBERRIESGOS	Mejora del rendimiento de sistemas Auditoría de sistemas de seguridad Modelado de sistemas y de ataques a sistemas
INFRAESTRUCTURAS CRÍTICAS	Monitorizado y seguridad de redes Detección de software malicioso Mejora de protocolos y estándares de seguridad
ÁREAS DE INTERÉS	Data mining Seguridad en Big Data Seguridad en los sistemas operativos Arquitectura en la nube y aplicaciones web Seguridad de redes Criptografía
GESTIÓN DE LA IDENTIDAD	Autenticación criptográfica Computación segura multiparte
SISTEMAS FIABLES Y ACTUALIZABLES	Plataformas de ejecución seguras
OTRAS	Securización de arranque de sistema Detección y defensa ante ataques especulativos de microarquitectura Modelos formales aplicados a ciberseguridad

PUBLICACIONES RELACIONADAS DESTACADAS

PUBLICACIONES AÑO 2022

Hunting@home: Plug and Play setup for intrusion detection in home networks. Lorena Mehavilla, José García y Alvaro Alesanco. VII Jornadas nacionales de Investigación en Ciberseguridad. Junio 2022

Razvan Raducu, Ricardo J. Rodríguez, Pedro Álvarez (2022). Resource Consumption Evaluation of C++ Cryptographic Libraries on Resource- Constrained Devices. In Proceedings of the 2nd EAI International Conference on Cryptography in Computer and Communications (AC3 2022), pp. 65–75, Springer, 2022. doi: 10.1007/978-3-031-17081-2˙53

Daniel Uroz and Ricardo J. Rodríguez (2022). Characterization and Evaluation of IoT Protocols for Data Exfiltration. IEEE Internet of Things Journal, vol. 9, iss. 19, pp. 19062-19072, JCR ranked in Q1 (subject category Computer Science, Information Systems, 9/164), impact factor 10.238 (2021), IEEE. doi: 10.1109/JIOT.2022.3163469

Razvan Raducu, Ricardo J. Rodríguez, and Pedro Álvarez (2022). Defense and Attack Techniques against File-based TOCTOU Vulnerabilities: a Systematic Review. IEEE Access, vol. 10, pp. 21742–21758, JCR ranked in Q2 (subject category Computer Science, Information Systems, 79/164), impact factor 3.476 (2021), IEEE. doi: 10.1109/ACCESS.2022.3153064

Esteban Damián Gutiérrez Mlot, Jose Saldana, and Ricardo J. Rodríguez (2022). Towards a Testbed for Critical Industrial Systems: SunSpec Protocol on DER Systems as a Case Study. In Proceedings of the 27th International Conference on Emerging Technologies and Factory Automation (ETFA), ranked as conference type B, class 3 (GGS 2021), pp. PP, IEEE. Accepted for publication. To appear. doi:

Yixiang Wang, Jiqiang Liu, Xiaolin Chang, Ricardo J. Rodríguez and Jianhua Wang (2022). DI-AA: An Interpretable White-box Attack for Fooling Deep Neural Networks. Information Sciences, vol. 610, pp. 14–32. JCR ranked in Q1 (subject category Computer Science, Information Systems, 16/164), impact factor 8.233 (2021), Elsevier. doi: 10.1016/j.ins.2022.07.157

Yixiang Wang, Jiqiang Liu, Xiaolin Chang, Jianhua Wang, and Ricardo J. Rodríguez (2022). AB-FGSM: AdaBelief Optimizer and FGSM-Based Approach to Generate Adversarial Examples. Journal of Information Security and Applications, vol. 68, pp. 103227. JCR ranked in Q2 (subject category Computer Science, Information Systems, 44/164), impact factor 4.960 (2021), Elsevier. doi: 10.1016/j.jisa.2022.103227

Jianhua Wang, Xialoin Chang, Ricardo J. Rodríguez, and Yixiang Wang (2022). Assessing Anonymous and Selfish Free-rider Attacks in Federated Learning. In Proceedings of the 2022 IEEE Symposium on Computers and Communications, ranked as conference type B, class 3 (GGS 2021), pp. 6, IEEE. doi: 10.1109/ISCC55528.2022.9912903

Pedro Fernández-Álvarez and Ricardo J. Rodríguez (2022). Extraction and Analysis of Retrievable Memory Artifacts from Windows Telegram Desktop Application. Forensic Science International: Digital Investigation, vol. 40, pp. 8 301342, JCR ranked in Q4 (subject category Computer Science, Information Systems, 131/164), impact factor 2.192 (2021), Elsevier. doi: 10.1016/j.fsidi.2022.301342

Ailton Santos Filho, Ricardo J. Rodríguez, and Eduardo L. Feitosa (2022). Evasion and Countermeasures Techniques to Detect Dynamic Binary Instrumentation Frameworks. Digital Threats: Research and Practice, vol. 3, iss. 2, pp. 28, ACM. doi: 10.1145/3480463

PUBLICACIONES AÑO 2021

Patient Identification Workflow for Seamless EHR Access During Patient Follow-Up. January 2021 8th European Medical and Biological Engineering Conference Jorge Sancho, Jose García and Alvaro Alesanco

"Towards Optimal LSTM Neural Networks for Detecting Algorithmically Generated Domain Names". Jose Selvi, Ricardo J. Rodríguez, Emilio Soria-Olivas, IEEE Access, vol. 9, pp. 126446–126456, 2021. doi: 10.1109/ACCESS.2021.3111307

"Quantifying Paging on Recoverable Data from Windows User-Space Modules". Miguel Martín-Pérez, Ricardo J. Rodríguez, in Proceedings of the 12th EAI International Conference on Digital Forensics & Cyber Crime, Springer, 2021.

"A Vision for Improving Business Continuity through Cyber-resilience Mechanisms and Frameworks". Miguel Hernández-Bejarano, Ricardo J. Rodríguez, José Merseguer, in Proceedings of the 16th Iberian Conference on Information Systems and Technologies (CISTI), pp. 1–5, 2021. doi: 10.23919/CISTI52073.2021.9476324

"Evaluation of the Executional Power in Windows using Return Oriented Programming". Daniel Uroz, Ricardo J. Rodríguez, in Proceedings of the 15th IEEE Workshop on Offensive Technologies (WOOT), pp. 361–372, IEEE, 2021. doi: 10.1109/SPW53761.2021.00056

"Bringing Order to Approximate Matching: Classification and Attacks on Similarity Digest Algorithms". Miguel Martín-Pérez, Ricardo J. Rodríguez, Frank Breitinger, Forensic Science International: Digital Investigation, vol. 36, pp. 301120, 2021. doi: 10.1016/j.fsidi.2021.301120

PUBLICACIONES AÑO 2020

"Pre-processing Memory Dumps to Improve Similarity Score of Windows Modules". Miguel Martín-Pérez, Ricardo J. Rodríguez, Davide Balzarotti, Computers & Security, vol. 101, pp. 102119, 2021. doi: 10.1016/j.cose.2020.102119

"On Challenges in Verifying Trusted Executable Files in Memory Forensics". Daniel Uroz, Ricardo J. Rodríguez, Forensic Science International: Digital Investigation, vol. 32, pp. 300917, 2020. doi: 10.1016/j.fsidi.2020.300917

"On Fingerprinting of Public Malware Analysis Services". Álvaro Botas, Ricardo J. Rodríguez, Vicente Matellan, Juan F. García, M. T Trobajo, Miguel V. Carriegos, Logic Journal of the IGPL, vol. 28, iss. 4, pp. 473–486, 2020. doi: 10.1093/jigpal/jzz050

"Reducing the Attack Surface of Dynamic Binary Instrumentation Frameworks". Ailton Santos Filho, Ricardo J. Rodríguez, Eduardo L. Feitosa, in Developments and Advances in Defense and Security, vol. 152, pp. 3–13, Springer Singapore, 2020. doi: 10.1007/978-981-13-9155-2_1

PUBLICACIONES AÑO 2019

"Characteristics and Detectability of Windows Auto-Start Extensibility Points in Memory Forensics". Daniel Uroz, Ricardo J. Rodríguez, Digital Investigation, vol. 28, pp. S95–S104, 2019. doi: 10.1016/j.diin.2019.01.026

"Detection of Algorithmically Generated Malicious Domain Names using Masked N-Grams". Jose Selvi, Ricardo J. Rodríguez, Emilio Soria-Olivas, Expert Systems with Applications, vol. 124, pp. 156–163, 2019. doi: 10.1016/j.eswa.2019.01.050

"Quantitative security analysis of a dynamic network system under lateral movement-based attacks". Yu Shi, Xiaolin Chang, Ricardo J. Rodríguez, Zhenjiang Zhang, Kishor S. Trivedi, Reliability Engineering & System Safety, vol. 183, pp. 213–225, 2019. doi: 10.1016/j.ress.2018.11.022

PUBLICACIONES AÑO 2018

"Desanonimización y categorización de servicios ocultos de la red Tor". Ricardo J. Rodríguez, Jorge García de Quirós, in Actas del VI Congreso Nacional de i+d en Defensa y Seguridad (DESEi+d 2018), 2018.

"Survivability Model for Security and Dependability Analysis of a Vulnerable Critical System". Xiaolin Chang, Shaohua Lv, Ricardo J. Rodríguez, Kishor Trivedi, in Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN), pp. 1–6, 2018. doi: 10.1109/ICCCN.2018.8487446

"A Tool to Compute Approximation Matching between Windows Processes". Ricardo J. Rodríguez, Miguel Martín-Pérez, Iñaki Abadía, in Proceedings of the 2018 6th International Symposium on Digital Forensic and Security (ISDFS), pp. 313–318, 2018. doi: 10.1109/ISDFS.2018.8355372

"Model-based Sensitivity Analysis of IaaS Cloud Availability". Bo Liu, Xiaolin Chang, Zhen Han, Kishor Trivedi, Ricardo J. Rodríguez, Future Generation Computer Systems, vol. 83, pp. 1–13, 2018. doi: 10.1016/j.future.2017.12.062

"A Methodology for Model-based Verification of Safety Contracts and Performance Requirements". Elena Gómez-Martínez, Ricardo J. Rodríguez, Clara Benac Earle, Leire Etxeberria Elorza, Miren Illarramendi Rezaba, Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, vol. 232, iss. 3, pp. 227–247, 2018. doi: 10.1177/1748006X16667328

"Empirical Study to Fingerprint Public Malware Analysis Services". Álvaro Botas, Ricardo J. Rodríguez, Vicente Matellán, Juan F. García, in Proceedings of the International Joint Conference SOCO'17-CISIS'17-ICEUTE'17, Advances in Intelligent Systems and Computing series, vol. 649, pp. 589–599, Springer International Publishing, 2017. doi: 10.1007/978-3-319-67180-2_57

"Security Assessment of the Spanish Contactless Identity Card". Ricardo J. Rodríguez, Juan Carlos Garcia-Escartin, IET Information Security, vol. 11, iss. 6, pp. 386–393(7), 2017. doi: 10.1049/iet-ifs.2017.0299

"Evolution and Characterization of Point-of-Sale RAM Scraping Malware". Ricardo J. Rodríguez, Journal in Computer Virology and Hacking Techniques, vol. 13, iss. 3, pp. 179–192, 2017. doi: 10.1007/s11416-016-0280-4

PUBLICACIONES AÑO 2016

"Towards the Detection of Isolation-Aware Malware". Ricardo J. Rodríguez, Iñaki Rodríguez-Gastón, Javier Alonso, IEEE Latin America Transactions (Revista IEEE America Latina), vol. 14, iss. 2, pp. 1024–1036, 2016. doi: 10.1109/TLA.2016.7437254

"Model-Based Vulnerability Assessment of Self-Adaptive Protection Systems". Ricardo J. Rodríguez, Stefano Marrone. Paulo Novais, David Camacho, Cesar Analide, Amal El Fallah Seghrouchni, Costin Badica, editors, in Intelligent Distributed Computing IX, Studies in Computational Intelligence series, vol. 616, pp. 439–449, Springer International Publishing, 2016. doi: 10.1007/978-3-319-25017-5_41

Grupo de Especial Interés en Ciberseguridad (SIGCYBSEC)		
Características generales	Características del Equipo de Investigación	Características de la Investigación

PUBLICACIONES RELACIONADAS DESTACADAS
"Survivability Analysis of a Computer System under an Advanced Persistent Threat Attack". Ricardo J. Rodríguez, Xiaolin Chang, Xiaodan Li, Kishor S. Trivedi. Barbara Kordy, Mathias Ekstedt, Seong Dong Kim, editors, in Proceedings of the 3rd International Workshop on Graphical Models for Security, vol. 9987, pp. 134–149, 2016. doi: 10.1007/978-3-319-46263-9_9
"Formal Security Assessment of Modbus Protocol". Roberto Nardone, Ricardo J. Rodríguez, Stefano Marrone, in Proceedings of the 11th International Conference for Internet Technology and Secured Transactions, pp. 142–147, IEEE, 2016. doi: 10.1109/ICITST.2016.7856685
"A Peek Under the Hood of iOS Malware". Laura García, Ricardo J. Rodríguez, in Proceedings of the 2016 11th International Conference on Availability, Reliability and Security (ARES), pp. 590–598, 2016. doi: 10.1109/ARES.2016.15
PUBLICACIONES AÑO 2015
"On Synergies of Cyber and Physical Security Modelling in Vulnerability Assessment of Railway Systems". Stefano Marrone, Ricardo J. Rodríguez, Roberto Nardone, Francesco Flammini, and Valeria Vittorini. Computers and Electrical Engineering, vol. 47, pp. 275--285, Elsevier. doi: 10.1016/j.compeleceng.2015.07.011
"Modelling Security of Critical Infrastructures: A Survivability Assessment". Ricardo J. Rodríguez}, José Merseguer, and Simona Bernardi. The Computer Journal, vol. 58:10, pp. 2313-2327, Oxford University Press. doi: 10.1093/comjnl/bxu096
"Counterfeiting and Defending the Digital Forensic Process". Álvaro Botas, Ricardo J. Rodríguez, Teemu Vaisanen, and Patrycjusz Zdzichowski. In Proceedings of the 3rd International Workshop on Cybercrimes and Emerging Web Environments (CEWE), pp. 1966-1971, IEEE. doi: 10.1109/CIT/IUCC/DASC/PICOM.2015.291
"Practical Experiences on NFC Relay Attacks with Android: Virtual Pickpocketing Revisited" José Vila, and Ricardo J. Rodríguez. In Proceedings of the 11th Workshop on RFID Security (RFIDSec), Lecture Notes in Computer Science vol. 9440, pp. 87-103, Springer. doi: 10.1007/978-3-319-24837-0_6

PROYECTOS RELEVANTES

"Indicadores de compromiso de malware mejorados mediante análisis forense de memoria (MIMFA)", 01/01/2023 a 31/12/2024, financiado por el Ministerio de Ciencia e Innovación, convocatoria 2021 - Proyectos de Transición Ecológica y Transición Digital. Cantidad: 129 835,00€. Equipo: 6

"JIUZ-2020-TEC-08: Secure-TBed4IIoT: Testbed para evaluación de seguridad en entornos IoT industriales", 01/01/2021 a 31/12/2021, financiado por la Fundación Ibercaja y Universidad de Zaragoza. Cantidad: 2 000€. Equipo: 7.

"IN-FAST.- Medidas para incrementar la ciberseguridad y protección de las infraestructuras críticas de transporte", 01/01/2020 a 30/06/2021, financiado por SICE S.A. (CDTI Ministerio de Ciencia e Innovación 2019). Cantidad: 71 368,90€. Equipo: 4.

"EU-GDPR: New data privacy regulation in the European Union - impact on EU citizens and organizations", 01/09/2019 a 30/09/2021, financiado por la UE (programa Jean Monnet, ref. 611826-EPP-1-2019-1-ES-EPPJMO-PROJECT). Cantidad: 59 865,50€. Equipo: 12.

"Ingeniería de resiliencia dirigida por el modelado y analisis de datos para sistemas dinamicos complejos", 01/01/2019 a 30/06/2021, financiado por Ministerio de Ciencia, Innovación y Universidades (Retos Investigación 2018). Cantidad: 55 297,00€. Equipo: 6.

"CUD-2018-09: Mejora del Análisis y Desanonimización de Servicios Ocultos en TorHSScanner", 01/01/2019 a 31/12/2019, financiado por CUD-Zaragoza. Cantidad: 1 200€. Equipo: 2.

"CUD-2017-14; Título: Modelo del protocolo Tor y seguimiento de servicios ocultos", 01/01 a 31/12/2018, financiado por Centro Universitario de la Defensa-Zaragoza. Cantidad: 1 500€. Equipo: 2.

"UZCUD2017-TEC-09: Análisis y estudio de la seguridad de sistemas de información y gestión de datos en el contexto de las smart cities y el Big Data", 1/10/2017 a 22/01/2018, financiado por CUD y Universidad de Zaragoza. Cantidad: 2 000€. Equipo: 5.

"UZCUD2016-TEC-06: Desarrollo de Técnicas de Detección de Ciberataques en Sistemas de Información mediante Minería de Procesos", 01/10/2016 a 30/09/2017, financiado por CUD y Universidad de Zaragoza. Cantidad: 2 000€. Equipo: 6.

"TIN2014-58457-R: Infraestructuras críticas resistentes a ciberataques: aplicando la minería de procesos y el diseño software orientado a la seguridad", 07/10/2015 a 31/12/2017, financiado por MINECO. Cantidad: 69 575€.

"Asesoría para el análisis de muestras dañinas", OTRI 2021/0283, 12/04/2021 a 11/04/2022, Sistemas Informáticos Abiertos SAU, 12 000€.

"Extracción de elementos para análisis pericial", OTRI 2021/0176, 1/04/2021 a 30/04/2021, TLM LOGISTIC ZARAGOZA 2014, S.L., 350€.

"Consultoría sobre aspectos informáticos", OTRI 2021/0355, 01/07/2021 a 31/07/2021, TLM LOGISTIC ZARAGOZA 2014, S.L., 2 089,67€.

"Consultoría de análisis pericial informático", OTRI 2020/0757, Centro de Investigación y Tecnología Agroalimentaria de Aragón, 15/12/2020 a 14/02/2021, 4 235€. Equipo: 1

"Auditoría y consultoría en sistemas de ticketing", OTRI 2019/0174, SICOMORO SERVICIOS INTEGRALES S.L., 15/04 a 15/07/2019, 12 100€. Equipo: 2.

"Consultoría para la mejora en el proceso de análisis de procesos legítimos en volcados de memoria", OTRI 2019/0194, Centro Nacional de Inteligencia, 08/04 a 31/12/2019. 18 137,90€. Equipo: 3.

"Consultoría para el análisis de procesos legítimos en volcados de memoria", OPID 2018/3, CNI, 15/03 a 31/12/2018. 18 137,90€. Equipo: 2.

PROYECTOS RELEVANTES

"Análisis de procesos legítimos en volcados de memoria", OTRI 2017/097, CNI, 22/02 a 31/12/2017. 21 659€. Equipo: 3.

"Análisis informáticos periciales", OPID 2017, Sicomoro Servicios Integrales SL, diciembre 2017. 1 681,90€.

"Análisis informáticos", OTRI 2016/1019, varias empresas, 16/05 a 31/12/2016. 1 542,75€.