Análisis de Datos y Ciberseguridad

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

IDENTIFICACIÓN DEL EQUIPO INVESTIGADOR

NOMBRE DEL EQUIPO O GRUPO DE INVESTIGACIÓN	Análisis de Datos y Ciberseguridad
UNIDAD/DEPARTAMENTO DE PERTENENCIA	Electrónica e Informática
CENTRO/INSTITUTO/UNIVERSIDAD/ORGANISMO DE PERTENENCIA	Mondragon Unibertsitatea

DATOS DE CONTACTO

DATOS DE CONTACTO DEL EQUIPO

PERSONA DE CONTACTO	Urko Zurutuza	TELÉFONO	649210323
ROL EN EL EQUIPO	Investigador Principal	MAIL	uzurutuza@mondragon.edu
WEB DEL EQUIPO	www.mondragon.edu/danz		

DIRECCIÓN POSTAL DEL EQUIPO

EDIFICIO		CENTRO	
TIPO DE VÍA	Calle	NOMBRE DE LA VÍA	Goiru
NÚMERO	2	CIUDAD	Arrasate-Mondragon
PROVINCIA	Gipuzkoa	CÓDIGO POSTAL	20500

DATOS DE CONTACTO DEL ORGANISMO AL QUE PERTENECE

PERSONA DE CONTACTO	Carlos García Crespo
MAIL	cgarcia@mondragon.edu
TELÉFONO	943794700
WEB	www.mondragon.edu

DIRECCIÓN POSTAL DEL ORGANISMO

EDIFICIO		CENTRO	
TIPO DE VÍA	Calle	NOMBRE DE LA VÍA	Loramendi
NÚMERO	4	CIUDAD	Arrasate-Mondragon
PROVINCIA	Gipuzkoa	CÓDIGO POSTAL	20500

Análisis de Datos y Ciberseguridad

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

INVESTIGADOR PRINCIPAL

NOMBRE	TITULACIÓN
Urko Zurutuza	Doctor

TRAYECTORIA PROFESIONAL

Dr. Urko Zurutuza es el investigador principal del Grupo de Investigación en Análisis de Datos y Ciberseguridad de EPS-MU, acreditado por el Gobierno Vasco como grupo de Tipo A. Urko es Ingeniero Técnico en Informática de Sistemas, Ingeniero Superior en Informática, y Doctor en Informática por Mondragon Unibertsitatea. Realizó su doctorado con el equipo de ciberseguridad de IBM Research Lab en Zürich entre el 2003 y 2008, desarrollando técnicas de minería y análisis de grandes conjuntos de datos de red. Desde entonces, ha participado en más de 50 proyectos de investigación con financiación pública, es autor de más de 45 publicaciones en conferencias y revistas académicas, y es miembro de más de 20 comités científicos de conferencias internacionales, como DIMVA (SIG SIDAR Conference on Detection of Intrusions and Malware & Vulnerability Assessment) o CRITIS (International Conference on Critical Information Infrastructures Security), siendo el General Chair en conferencias como RAID 2021, RAID 2020, JNIC 2018, DIMVA 2016, y RECSI 2012. Urko es miembro de la Junta Directiva de la RENIC (Red de Excelencia Nacional de Investigación en Ciberseguridad). Ha coordinado proyectos de investigación a nivel regional, nacional y europeo, tiene experiencia en el 6PM, 7PM, H2020, Programas conjuntos (JTI's) como Artemis y Ambient Assisted Living (AAL), y ha sido el coordinador principal del proyecto Europeo MANTIS (47 partners, 30M€ de presupuesto) recientemente finalizado.

WEB Y REDES SOCIALES

http://www.mondragon.edu/danz
https://twitter.com/MU_gep
https://www.linkedin.com/showcase/mondragon-goi-eskola-politeknikoa/

MIEMBROS DEL EQUIPO

Garitano Garitano, Iñaki	Iturbe Urretxa, Mikel	Ezpeleta Gallastegi, Enaitz
Santos Grueiro, Igor	Velez de Mendizabal, Iñaki	Lizarraga, Jesús
Fernandez, Miguel	Rodriguez Ceberio, Antton	Aguirre Ortuzar, Aitor
Alberdi Aramendi, Ane	Basagoiti Astigarraga, Rosa	Reguera Bakache, Dani
Zugasti Uriguen, Ekhi	Cernuda García, Carlos	Manzano Castro, Marc
Capo Rangel, Marco Vinicio	Serradilla Casado, Oscar	Izagirre Aizpitarte, Unai

Análisis de Datos y Ciberseguridad		
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	Creación de barreras de entrada Elaboración de mecanismos de respuesta ante ataques Identificación y localización del atacante Búsqueda del origen de la amenaza Contención de ataques Decoys y tripwires Defensa ante ataques propagables
EVALUACIÓN DE SISTEMAS Y CIBERRIESGOS	Estudio de patrones Mecanismos de recolección de datos Análisis de riesgos estadísticos y predictivos Evaluación y gestión dinámica de riesgos Recolección de información sobre amenazas Métricas de riesgos integradas e indicadores Detección temprana de ciberriesgos Herramientas de gestión de toma de decisiones
GESTIÓN DE LA IDENTIDAD	Controles de acceso basados en comportamiento Sistemas de seguridad adaptados a patrones de uso
FOMENTO Y CONCIENCIACIÓN DE LA SEGURIDAD	Protección de correo electrónico
INFRAESTRUCTURAS CRÍTICAS	Detección de amenazas Monitorizado y seguridad de redes Arquitectura de Protección Desarrollo de herramientas de protección Sistemas de control industrial en redes (agua, electricidad, alimentación, transporte, finanzas, salud, eSalud, ect.) Estrategias de reacción ante ataques Detección de software malicioso
INTERACCIÓN CON EL USUARIO USABILIDAD	Algoritmos de clave pública usable
PROCESADO DE DATOS	Análisis de datos a gran escala Procesado seguro de datos y señales cifrados Políticas basadas en datos
PRIVACIDAD	Análisis Big Data enfocado al respeto de la privacidad Protocolos criptográficos de preservación de la privacidad Privacidad en IoT
SISTEMAS FIABLES Y ACTUALIZABLES	
ÁREAS DE INTERÉS	Cloud Computing Criptografía Data mining Internet de las Cosas Seguridad de redes Seguridad en Big Data Virtualización y gestión de redes Seguridad en dispositivos móviles Seguridad en Sistemas Críticos (Aeronáutica, Ferrocarril, Automoción…) Criptografía post-cuántica Arquitectura en la nube y aplicaciones web

PUBLICACIONES RELACIONADAS DESTACADAS

PUBLICACIONES AÑO 2020

Enaitz Ezpeleta, Iñaki Velez de Mendizabal, José María Gómez Hidalgo, Urko Zurutuza. Novel email spam detection method using sentiment analysis and personality recognition. Logic Journal of the IGPL. Vol. 28. N. 1. Pp. 83–94. February, Publicado 2020 https://doi.org/10.1093/jigpal/jzz073

Deep packet inspection for intelligent intrusion detection in software-defined industrial networks: A proof of concept
Markel Sainz, Iñaki Garitano, Mikel Iturbe, Urko Zurutuza. Logic Journal of the IGPL. jzz060. 02 January, Publicado 2020 https://doi.org/10.1093/jigpal/jzz060

Iñaki Velez de Mendizabal, Vitor Basto-Fernandes, Enaitz Ezpeleta, José R. Méndez, Urko Zurutuza. SDRS: A new lossless dimensionality reduction for text corpora. Information Processing & Management. Vol. 57. N. 4. N. artículo 102249, Publicado Elsevier 2020 https://doi.org/10.1016/j.ipm.2020.102249

Iskander Sanchez-Rola, Davide Balzarotti, Igor Santos. Cookies from the Past: Timing Server-Side Request Processing Code for History Sniffing. Especial issue of the ACM Digital Threats: Research and Practice (DTRAP) journal. Argitaratzeke/Pendiente de publicación 2020

PUBLICACIONES AÑO 2019

Iñaki Garitano, Mikel Iturbe, Enaitz Ezpeleta, and Urko Zurutuza. Who's There? Evaluating Data Source Integrity and Veracity in IIoT Using Multivariate Statistical Process Control. Security and Privacy Trends in the Industrial Internet of Things. Advanced Sciences and Technologies for Security Applications. Editor, C. Alcaraz. Springer. First Online: 14 May, Publicado 2019 https://doi.org/10.1007/978-3-030-12330-7_9

PUBLICACIONES AÑO 2018

Enaitz Ezpeleta. Nuevos Paradigmas de Análisis Basados en Contenidos para la Detección del Spam en RRSS = New approaches for content-based analysis towards Online Social Network spam detection. Procesamiento del Lenguaje Natural. Nº 60. Pp. 71-74. Marzo, Publicado 2018 https://doi.org/10.26342/2018-60-8

Wissam Aoudi, Mikel Iturbe, Magnus Almgren. Truth Will Out: Departure-Based Process-Level Detection of Stealthy Attacks on Control Systems. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS2018). Toronto, Canada. October 15 - 19, 2018. Pp. 817-831. New York, ACM, Publicado 2018 http://dx.doi.org/10.1145/3243734.3243781

Mikel Iturbe. Primer premio al mejor trabajo de estudiante: Deteccion de anomalías en redes industriales guiada por datos. Actas de las Cuartas Jornadas Nacionales de Investigación en Ciberseguridad (JNIC2018). Donostia-San Sebastián. Gipuzkoa, 13-15 de Junio, 2018. Pp. 67-68.

Markel Sainz, Mikel Iturbe, Iñaki Garitano, Urko Zurutuza. Software Defined Networking Opportunities for Intelligent Security Enhancement of Industrial Control Systems. International Workshop on Soft Computing Models in Industrial and Environmental Applications. Computational Intelligence in Security for Information Systems Conference International Conference on EUropean Transnational Education. SOCO 2017, CISIS 2017, ICEUTE 2017: International Joint Conference SOCO'17-CISIS'17-ICEUTE'17 León, Spain, September 6–8, Proceeding. Pp 577-586. Springer, Publicado 2018 https://go.openathens.net/redirector/mondragon.edu?url=https://dx.doi.org/10.1007/978-3-319-67180-2_56

Enaitz Ezpeleta, Inaki Garitano, Ignacio Arenaza-Nuno, José María Gómez, Urko Zurutuza. Novel Comment Spam Filtering Method on Youtube: Sentiment Analysis and Personality Recognition. International Conference on Web Engineering ICWE 2017: Current Trends in Web Engineering. Lecture Notes in Computer Science book series (LNCS). Vol. 10544. Pp. 228-240. Springer, Publicado 2018 https://go.openathens.net/redirector/mondragon.edu?url=https://doi.org/10.1007/978-3-319-74433-9_21

Iñaki Vélez de Mendizabal, Enaitz Ezpeleta, Urko Zurutuza, David Ruano-Ordás. La intención hace el agravio: técnicas de clustering conceptual para la generalización y especialización de intencionalidades en el spear phishing. Actas de las Cuartas Jornadas Nacionales de Investigación en Ciberseguridad. Donostia-San Sebastián. Gipuzkoa, 13-15 de Junio, 2018. Pp. 41-43. Editores, Urko Zurutuza, Mikel Iturbe, Enaitz Ezpeleta e Iñaki Garitano. Servicio Editorial de Mondragon Unibertsitatea, Publicado 2018
https://go.openathens.net/redirector/mondragon.edu?url=http://2018.jnic.es/assets/Actas_JNIC2018.pdf

Ekhi Zugasti, Mikel Iturbe, Inaki Garitano, Urko Zurutuza. MEDEA: Monitorizando el espacio nulo para la detección de anomalías en sistemas industriales. Actas de la XV Reunión Española de Criptología y Seguridad de la Información (RECSI). Granada. 3-5 octubre. Pp. 212- 216. Universidad de Granada, Publicado 2018
https://go.openathens.net/redirector/mondragon.edu?url=https://nesg.ugr.es/recsi2018/docs/ActasXVRECSI.pdf

Enaitz Ezpeleta, Mikel Iturbe, Iñaki Garitano, Iñaki Velez de Mendizabal, Urko Zurutuza. Mejorando la Detección de Spam Social Utilizando la Subjetividad. Actas de la XV Reunión Española de Criptología y Seguridad de la Información (RECSI). Granada. 3-5 octubre. Pp. 169-173. Universidad de Granada, Publicado 2018
https://go.openathens.net/redirector/mondragon.edu?url=https://nesg.ugr.es/recsi2018/docs/ActasXVRECSI.pdf

O. Somarriba, L. P. C. Ramos, U. Zurutuza, R. Uribeetxeberria. Dynamic DNS Request Monitoring of Android Applications via networking. 2018 IEEE 38th Central America and Panama Convention (CONCAPAN XXXVIII). Pp. 452-457. Editor M. N. Cardona. IEEE, Publicado 2018 http://dx.doi.org/10.1109/CONCAPAN.2018.8596558

Ekhi Zugasti, Mikel Iturbe, Inaki Garitano, Urko Zurutuza. Null is Not Always Empty: Monitoring the Null Space for Field-Level Anomaly Detection in Industrial IoT Environments. 2018 Global Internet of Things Summit, GIoTS. Pp. 104-109. IEEE, Publicado 2018 https://go.openathens.net/redirector/mondragon.edu?url=http://dx.doi.org/10.1109/GIOTS.2018.8534574

PUBLICACIONES AÑO 2017

Mikel Iturbe, Iñaki Garitano, Urko Zurutuza, Roberto Uribeetxeberria. Towards Large-Scale, Heterogeneous Anomaly Detection Systems in Industrial Networks: A Survey of Current Trends. Security and Communication Networks. Vol. 2017. Article ID 9150965. November, Publicado 2017 https://doi.org/10.1155/2017/9150965

Andrea Fiaschetti, Josef Noll, Paolo Azzoni, Roberto Uribeetxeberria, John Gialelis, Kyriakos Stefanidis, Dimitrios Serpanos, and Andreas Papalambrou,Security, Privacy and Dependability Concepts. Measurable and Composable Security, Privacy, and Dependability for Cyberphysical Systems: The SHIELD Methodology. Edited by Andrea Fiaschetti, Josef Noll, Paolo Azzoni and Roberto Uribeetxeberria. CRC Press, Publicado 2017

Josef Noll, Iñaki Garitano, Christian Johansen, Javier del Ser, and Ignacio Arenaza-Nuño. Perspectives in secure SMART environments. Measurable and Composable Security, Privacy, and Dependability for Cyberphysical Systems: The SHIELD Methodology. Edited by Andrea Fiaschetti, Josef Noll, Paolo Azzoni and Roberto Uribeetxeberria. CRC Press, Publicado 2017
https://doi.org/10.1201/9781138042858

Andrea Morgagni, Andrea Fiaschetti, Josef Noll, Ignacio Arenaza-Nuño, Javier Del Ser. Security, Privacy and Dependability Metrics. Measurable and Composable Security, Privacy, and Dependability for Cyberphysical Systems: The SHIELD Methodology. Edited by Andrea Fiaschetti, Josef Noll, Paolo Azzoni and Roberto Uribeetxeberria. CRC Press, Publicado 2017

Enaitz Ezpeleta, Urko Zurutuza, José María Gómez Hidalgo. A study of the personalization of spam content using Facebook public information. Logic Journal of the IGPL. Vol. 25. Nº. Pp. 30–41. 1 February, Publicado 2017 https://go.openathens.net/redirector/mondragon.edu?url=http://dx.doi.org/10.1093/jigpal/jzw040

Enaitz Ezpeleta, Inaki Garitano, José Maria Gómez, Urko Zurutuza. Short Messages Spam Filtering Combining Personality Recognition and Sentiment Analysis. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems. Vol. 25. Nº. Suppl. 2. December, Publicado 2017 https://doi.org/10.1142/S0218488517400177

Enaitz Ezpeleta. Segundo premio al mejor trabajo de estudiante: nuevos paradigmas de análisis basados en contenidos para la detección del spam en RRSS. III Jornadas Nacionales de Investigación en Ciberseguridad (JNIC). Madrid. 31 mayo - 2 junio de 2017. Universidad Rey Juan Carlos, Publicado 2017

Aitor Osa, Iñaki Garitano, Ignacio Arenaza-Nuño, Urko Zurutuza, Mikel Iturbe. Cifrado CP-ABE para el ecosistema Apache Hadoop. II Jornadas Nacionales de Investigación en Ciberseguridad (JNIC). Madrid, 31 de mayo y 1-2 de junio, Publicado 2017 http://hdl.handle.net/10115/14540

PUBLICACIONES RELACIONADAS DESTACADAS

Mikel Iturbe, Iñaki Garitano, Ignacio Arenaza-Nuño, Urko Zurutuza. Hacia un conjunto estandar de ataques contra sistemas de control para la evaluación de contramedidas. II Jornadas Nacionales de Investigación en Ciberseguridad (JNIC). Madrid, 31 de mayo y 1-2 de junio, Publicado 2017 http://hdl.handle.net/10115/14540

PUBLICACIONES AÑO 2016

Mikel Iturbe, José Camacho, Iñaki Garitano, Urko Zurutuza, Roberto Uribeetxeberria. Distinguiendo entre perturbaciones de proceso e intrusiones en sistemas de control: caso de estudio con el proceso Tennessee-Eastman. XIV Reunión Española sobre Criptología y Seguridad de la Información (RECSI). Mahón, 26-28 de octubre. Universidad de les Illes Balears, Publicado 2016

Elin Sundby Boysen, Iñaki Garitano and Josef Noll. Basic Internet Access: Capacity and Traffic Shaping. The Sixth International Conference on Mobile Services, Resources, and Users (MOBILITY). Proceedings of a meeting held 22-26 May 2016, Valencia, Spain. International Academy, Research, and Industry Association (IARIA), Publicado 2016

Enaitz Ezpeleta, Urko Zurutuza, José María Gómez Hidalgo. Short Messages Spam Filtering Using Sentiment Analysis. Text, Speech, and Dialogue: 19th International Conference, TSD 2016, Brno, Czech Republic, September 12-16, 2016, Proceedings. Vol. 9924. Lecture Notes in Computer Science. Pp 142-153, Publicado 2016 https://go.openathens.net/redirector/mondragon.edu?url=http://dx.doi.org/10.1007/978-3-319-45510-5_17

Enaitz Ezpeleta, Urko Zurutuza, José María Gómez Hidalgo. Using Personality Recognition Techniques to Improve Bayesian Spam Filtering. Procesamiento del Lenguaje Natural, Revista. Vol. 57. Pp. 125-132, Publicado 2016 https://go.openathens.net/redirector/mondragon.edu?url=http://journal.sepln.org/sepln/ojs/ojs/index.php/pln/article/view/5345/3129

Mikel Iturbe, Jose Camacho, Iñaki Garitano, Urko Zurutuza, Roberto Uribeetxeberria. On the Feasibility of Distinguishing Between Process Disturbances and Intrusions in Process Control Systems using Multivariate Statistical Process Control. Proceedings of the 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN). Toulouse. 28 June- 1 August. IEEE, Publicado 2016 https://go.openathens.net/redirector/mondragon.edu?url=http://dx.doi.org/10.1109/DSN-W.2016.32

Mikel Iturbe, Iñaki Garitano, Urko Zurutuza, Roberto Uribeetxeberria. Visualizing Network Flows and Related Anomalies in Industrial Networks using Chord Diagrams and Whitelisting. Proceedings of the 11th Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications (VISIGRAPP 2016) - Volume 2: IVAPP. Pp. 99-106. SCITEPRESS, Science and Technology Publications, Publicado 2016 https://go.openathens.net/redirector/mondragon.edu?url=http://dx.doi.org/10.5220/0005670000990106

Enaitz Ezpeleta Gallastegi. New approaches for content-based analysis towards online social network spam detection. PhD Thesis. Mondragon Unibertsitatea. Goi Eskola Politeknikoa 2016 http://hdl.handle.net/20.500.11984/1212

Oscar Somarriba, Urko Zurutuza, Roberto Uribeetxeberria, Laurent Delosières, and Simin Nadjm-Tehrani. Detection and Visualization of Android Malware Behavior. Journal of Electrical and Computer Engineering. Vol. 2016, Article ID 8034967. Hindawi, Publicado 2016 http://dx.doi.org/10.1155/2016/8034967

Miguel Fernández, Iñaki Arenaza, Iñaki Garitano, Jesus Lizarraga, Mikel Iturbe. MOOC sobre Hacking ético de MONDRAGON UNIBERTSITATEA - #moocHackingMU. II Jornadas Nacionales de Investigación en Ciberseguridad (JNIC). Granada. 15-17 junio, Publicado 2016 https://go.openathens.net/redirector/mondragon.edu?url=http://ucys.ugr.es/jnic2016/docs/ActasJNIC2016.pdf

Mikel Iturbe, Unai Izagirre, Iñaki Garitano, Ignacio Arenaza-Nuño, Urko Zurutuza, Roberto Uribeetxeberria. Diseño de un banco de pruebas híbrido para la investigación de seguridad y resiliencia en redes industriales. II Jornadas Nacionales de Investigación en Ciberseguridad (JNIC). Granada. 15-17 junio, Publicado 2016 https://go.openathens.net/redirector/mondragon.edu?url=http://ucys.ugr.es/jnic2016/docs/ActasJNIC2016.pdf

Enaitz Ezpeleta, Urko Zurutuza, José María Gómez Hidalgo. Does Sentiment Analysis Help in Bayesian Spam Filtering?. Hybrid Artificial Intelligent Systems. 11th International Conference, HAIS 2016, Seville, Spain, April 18-20. Proceedings. Vol.9648 of the series, Lecture Notes in Computer Science. Pp 79-90. Springer, Publicado 2016 https://go.openathens.net/redirector/mondragon.edu?url=http://dx.doi.org/10.1007/978-3-319-32034-2_7

Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA 2016). Editors, Juan Caballero, Urko Zurutuza, Ricardo J. Rodríguez . Publicado Springer International Publishing 2016 http://dx.doi.org/10.1007/978-3-319-40667-1

Enaitz Ezpeleta, Urko Zurutuza, José María Gómez Hidalgo. Los spammers no piensan: usando reconocimiento de personalidad para el filtrado de spam en mensajes cortos. Actas de la XIV Reunión Española sobre Criptología y Seguridad de la Información, RECSI. Maó, Menorca. 26-28 Octubre. Universidad de les Illes Balears, Publicado 2016 https://go.openathens.net/redirector/mondragon.edu?url=http://recsi16.uib.es/wp-content/uploads/2016/10/ACTAS-RECSI-2016.pdf

Enaitz Ezpeleta, Urko Zurutuza, José María Gómez Hidalgo. Short Messages Spam Filtering Using Personality Recognition. ACM International Conference Proceeding Series. 4th Spanish Conference in Information Retrieval. Granada.14-16 June. Vol.14-16-June-2016. Article number 7, Publicado 2016 http://dx.doi.org/10.1145/2934732.2934742

PUBLICACIONES AÑO 2015

E. Ezpeleta, U. Zurutuza, J. M. G. Hidalgo. An analysis of the effectiveness of personalized spam using online social network public information. International Joint Conference CISIS'2015 and ICEUTE'2015. Advances in Intelligent Systems and Computing. Springer. Vol. 369. Pp 497-506, Publicado 2015 https://go.openathens.net/redirector/mondragon.edu?url=https://doi.org/10.1007/978-3-319-19713-5_43

Mikel Iturbe, Iñaki Garitano, Urko Zurutuza, Roberto Uribeetxeberria. Sistema visual de monitorización de seguridad de flujos de red industriales. I Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2015). León. 14-16 Septiembre, Publicado 2015

George Suciu, Geaba Alin Nicusor, Iñaki Garitano and Josef Noll. Basic Internet: Mobile Content Delivery to Everyone. Eleventh International Conference on Wireless and Mobile Communications ICWMC). Proceedings of a meeting held 11-16 October 2015, St. Julians, Malta. International Academy, Research, and Industry Association (IARIA), Publicado 2015

PUBLICACIONES AÑO 2014

S. González, Á. Herrero, J. Sedano, U. Zurutuza, and E. Corchado. Different approaches for the detection of SSH anomalous connections. Logic Journal of the IGPL. Vol. 24. Nº 1. Pp. 104–114. February, Publicado 2014 http://www.dx.doi.org/10.1093/jigpal/jzv047

Silvia González, Javier Sedano, Urko Zurutuza, Enaitz Ezpeleta, Diego Martínez, Álvaro Herrero, Emilio Corchado. Classification of SSH anomalous connections. International Joint Conference SOCO'13-CISIS'13-ICEUTE'13. Advances in Intelligent Systems and Computing. Vol. 239. Pp. 479-488, Publicado 2014 https://go.openathens.net/redirector/mondragon.edu?url=http://dx.doi.org/10.1007/978-3-319-01854-6_49

Iñaki Garitano, Mikel Iturbe, Ignacio Arenaza-Nuño, Roberto Uribeetxeberria, Urko Zurutuza. Sistema de Detección de Anomalías para protocolos propietarios de Control Industrial. Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información RECSI XIII : Alicante, 2-5 de septiembre. Pp. 315-320. Universidad de Alicante, Publicado 2014 https://go.openathens.net/redirector/mondragon.edu?url=http://rua.ua.es/dspace/bitstream/10045/40461/1/RECSI-2014.pdf

Oscar Somarriba, Ignacio Arenaza, Roberto Uribeetxeberria, Urko Zurutuza. Análisis visual del comportamiento de aplicaciones para Android. Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información RECSI XIII : Alicante, 2-5 de septiembre. Pp. 253-258. Universidad de Alicante, Publicado 2014 https://go.openathens.net/redirector/mondragon.edu?url=http://rua.ua.es/dspace/bitstream/10045/40461/1/RECSI-2014.pdf

PUBLICACIONES AÑO 2013

Iñaki Garitano Garitano. PhD. Behavioral modeling for anomaly detection in industrial control systems. Mondragon Unibertsitatea, Mondragon Goi Eskola Politeknikoa 2013 http://hdl.handle.net/20.500.11984/1712

PUBLICACIONES AÑO 2012

Keldor Gerrigagoitia, Roberto Uribeetxeberria, Urko Zurutuza, Ignacio Arenaza. Reputation-based intrusion detection system for wireless sensor networks. Proceedings of the 2nd IEEE Workshop on Complexity in Engineering (COMPENG). Aachen. 11 -13 June. Pp.128-131, Publicado 2012 https://go.openathens.net/redirector/mondragon.edu?url=http://dx.doi.org/10.1109/CompEng.2012.6242969

PUBLICACIONES RELACIONADAS DESTACADAS

I. Garitano, C. Siaterlis, B. Genge, R. Uribeetxeberria, U. Zurutuza. A method to construct network traffic models for process control systems. Proceedings of 2012 IEEE 17th International Conference on Emerging Technologies & Factory Automation (ETFA) Pp. 1-8. IEEE, 2012 https://go.openathens.net/redirector/mondragon.edu?url=http://dx.doi.org/10.1109/ETFA.2012.6489550

Álvaro Herrero, Urko Zurutuza, Emilio Corchado. A neural-visualization IDS for honeynet data. International Journal of Neural Systems. Vol. 22. Nº. 2. Pp 121-128, Publicado 2012 https://go.openathens.net/redirector/mondragon.edu?url=http://dx.doi.org/10.1142/S0129065712500050
Actas de la XII Reunión Española sobre Criptología y Seguridad de la Información. Editores Urko Zurutuza, Roberto Uribeetxeberria e Ignacio Arenaza. Publicado Servicio Editorial de Mondragon Unibertsitatea 2012

PUBLICACIONES AÑO 2011

Iñaki Garitano, Roberto Uribeetxeberria, Urko Zurutuza. A review of SCADA anomaly detection systems. Soft Computing Models in Industrial and Environmental Applications, 6th International Conference SOCO 2011. Pp. 357-366. Part of the Advances in Intelligent and Soft Computing book series (AINSC). Vol. 87. Springer, Publicado 2011 https://go.openathens.net/redirector/mondragon.edu?url=http://dx.doi.org/10.1007/978-3-642-19644-7

I. Burguera, U. Zurutuza, and S. Nadjm-Tehrani. Crowdroid : behavior-based malware detection system for Android. Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, SPSM'11, Held in Association with the 18th ACM Conference on Computer and Communications Security, CCS 2011; Chicago, IL; United States; 17 October 2011 through 17 October 2011. Pp. 15-25. ACM, Publicado 2011 https://go.openathens.net/redirector/mondragon.edu?url=http://dx.doi.org/10.1145/2046614.2046619

Urko Zurutuza , Enaitz Ezpeleta, Álvaro Herrero, Emilio Corchado. Visualization of misuse-based intrusion detection: application to honeynet data. Advances in Intelligent and Soft Computing. Vol. 87. Pp 561-570, Publicado 2011 https://go.openathens.net/redirector/mondragon.edu?url=http://dx.doi.org/10.1007/978-3-642-19644-7

PUBLICACIONES AÑO 2010

Urko Zurutuza, Rosa Basagoiti and Asier Aztiria. Behavior analysis of domain servers through windows security event monitoring. Journal of Information Assurance and Security. Vol. 5. Nº 4. Pp. 418-425, Publicado 2010

Manuel J. Martínez, Roberto Uribeetxeberria, Urko Zurutuza, Miguel Fernández. The impact of the SHA-3 casting cryptography competition on the Spanish IT market. Computational Intelligence in Security for Information Systems 2010. Advances in Intelligent and Soft Computing, Vol. 85, pp 191-199 Publicado 2010 https://go.openathens.net/redirector/mondragon.edu?url=http://dx.doi.org/10.1007/978-3-642-16626-6_21

Álvaro Alonso, Santiago Porras, Enaitz Ezpeleta, Ekhiotz Vergara, Ignacio Arenaza, Roberto Uribeetxeberria, Urko Zurutuza, Álvaro Herrero, Emilio Corchado. Understanding honeypot data by an unsupervised neural visualization. Computational Intelligence in Security for Information Systems 2010. Advances in Intelligent and Soft Computing, vol 85. Pp 151-160. Herrero Á., Corchado E., Redondo C., Alonso Á. (eds). Springer, Berlin, Heidelberg, Publicado 2010 https://go.openathens.net/redirector/mondragon.edu?url=http://dx.doi.org/10.1007/978-3-642-16626-6_17

Urko Zurutuza, Enaitz Ezpeleta, Ignacio Arenaza, Iñaki Velez de Mendizabal, Jesús Lizarraga, Roberto Uribeetxeberria, Miguel Fernández. Euskalert, red vasca de honeypots. Actas de XI Reunión Española sobre Criptografía y Seguridad de la Información (XI RECSI). Tarragona. 7-10 Septiembre, Publicado 2010

R. Uribeetxeberria, I. Arenaza, I. Garitano, T. Arzuaga. Identifying cyber security events in IEC 61850 substations by analysing different traffic patterns. 43rd International Conference on Large High Voltage Electric Systems (CIGRE) Paris. 22-27 August. Paper D2-205, Publicado 2010

Álvaro Alonso, Santiago Porras, Iñaki Garitano, Ignacio Arenaza, Roberto Uribeetxeberria, Urko Zurutuza, Álvaro Herrero, Emilio Corchado. On the Visualization of Honeypot Data through Projection Techniques. 10th International Conference on Computational and Mathematical Methods in Science and Engineering. Almeria. 26-30 June, Publicado 2010

PUBLICACIONES AÑO 2009

Rosa Basagoiti, Urko Zurutuza, Asier Aztiria, Guzmán Santafé, Mario Reyes. Clustering of windows security events by means of frequent pattern mining. Computational Intelligence in Security for Information Systems. Herrero Á., Gastaldo P., Zunino R., Corchado E. (eds). Advances in Intelligent and Soft Computing. Vol. 63. Pp.19- 27. Springer, Publicado 2009 https://go.openathens.net/redirector/mondragon.edu?url=http://dx.doi.org/10.1007/978-3-642-04091-7_3

PUBLICACIONES AÑO 2008

M. Fernández, R. Uribeetxeberria, U. Zurutuza, Iñaki Vélez de Mendizabal. Mejora del clustering de ataques realizado en una red distribuida de sistemas trampa. X Reunión Española sobre Criptografía y Seguridad de la Información (RECSI). Salamanca. 2-5 Septiembre, Publicado 2008

Asier Martínez, Urko Zurutuza, Roberto Uribeetxeberria, Miguel Fernández, Jesús Lizarraga, Ainhoa Serna and Iñaki Vélez de Mendizabal. Beacon frame spoofing attack detection in IEEE 802.11 networks. Third International Conference on Availability, Reliability and Security (ARES). Barcelona. March. PG. 520-525, Publicado 2008 https://go.openathens.net/redirector/mondragon.edu?url=http://dx.doi.org/10.1109/ARES.2008.130

José Luis Flores Barroso, Ignacio Arenaza Nuño, Iñaki Vélez de Mendizabal. Servicios de red en Linux: DNS, DHCP, WWW, Correo y Proxy. Publicado Mondragon Unibertsitateko Zerbitzu Editoriala 2008

Corrado Leita, Olivier Thonnard, Eric Alata, Marco Serafini, Vladimir Stankovic, Jouni Viinikka and Urko Zurutuza. Malicious fault characterization exploiting honeypot data. Proceedings of the Seventh European Dependable Computing Conference (EDCC-7), Kaunas, Lituania, May 2008 Publicado 2008 https://go.openathens.net/redirector/mondragon.edu?url=http://www.researchgate.net/publication/228889592_Malicious_fault_characterization_exploiting_honeypot_data

Urko Zurutuza, Roberto Uribeetxeberria, Diego Zamboni, Miguel Fernández, Iñaki Vélez de Mendizabal. Un marco inteligente para el análisis de tráfico generado por gusanos en Internet. Actas de la X Reunión Española sobre Criptografía y Seguridad de la Información (RECSI). Salamanca. 2-5 Septiembre, Publicado 2008

Urko Zurutuza , Roberto Uribeetxeberria, and Diego Zamboni. A data mining approach for analysis of worm activity through automatic signature generation. 1st ACM Workshop on AISec, AISec'08. Co-located with the 15th ACM Computer and Communications Security Conference, CCS'08; Alexandria, VA; United States; 27 October 2008 through 31 October 2008. Proceedings of the ACM Conference on Computer and Communications Security2008. Pp. 61-70. ACM, Publicado 2008 https://go.openathens.net/redirector/mondragon.edu?url=http://dx.doi.org/10.1145/1456377.1456394

PUBLICACIONES AÑO 2007

U. Zurutuza, R. Uribeetxeberria, E. Azketa, G. Gil, J. Lizarraga, M. Fernández. Combined data mining approach for intrusion detection. International Conference on Security and Cryptography (SECRYPT). Barcelona. 28-31 July, Publicado 2007

Urko Zurutuza Ortega. Data minig approaches for analysis of worm activity toward automatic signature generation. PhD. Mondragon Goi Eskola Politeknikoa, Mondragon Unibertsitatea 2007 http://hdl.handle.net/20.500.11984/1925

M. Fernández, R. Uribeetxeberria y U. Zurutuza. Mejora del clustering de ataques realizado en la red Leurre.com a través de la eliminación de las anomalías de red. Actas del II Simposio sobre Seguridad Informática. Madrid : Thomson, Publicado 2007

PUBLICACIONES RELACIONADAS DESTACADAS

U. Zurutuza, R. Uribeetxeberria, M. Fernández y D. Zamboni. Análisis de datos procedentes de un Sistema de Detección de Gusanos mediante técnicas de clustering. Actas del II Simposio sobre Seguridad Informática. Madrid : Thomson, Publicado 2007

PUBLICACIONES AÑO 2006

Jesus María Lizarraga, Roberto Uribeetxeberria, Urko Zurutuza, Miguel Fernández. Security in embedded systems. IADIS International Conference Applied Computing. San Sebastián. 25-28 February, Publicado 2006

U. Zurutuza, R. Uribeetxeberria, J. Riordan, Y. Duponchel. Mining a worm detection system data. 9th International Symposium on Recent Advances in Intrusion Detection (RAID). Hamburg. 20-22 September, Publicado Springer 2006

PUBLICACIONES AÑO 2005

Urko Zurutuza, Roberto Uribeetxeberria. A review of three intrusion detection alert correlation methods. IADAT Journal of Advanced Technology on Telecommunications and Computer Networks. Vol. 1. Nº 1. September, Publicado 2005

Miguel Fernández, Roberto Uribeetxeberria. Sistemas trampa : revisión del estado actual. I Simposio Español sobre Seguridad Informática, en el marco del Primer Congreso Español de Informática (CEDI'05). Septiembre, Publicado 2005

Urko Zurutuza y Roberto Uribeetxeberria. Revisión del estado actual de la investigación en el uso de data mining para la detección de intrusiones. I Simposio Español sobre Seguridad Informática, en el marco del Primer Congreso Español de Informática (CEDI'05). Septiembre, Publicado 2005

PUBLICACIONES AÑO 2004

Urko Zurutuza, Roberto Uribeetxeberria, Jesús Lizarraga, Iñaki Velez de Mendizabal. A methodology for continuous computer security auditing. Proceedings of the IADIS International Conference on e-Society. Ávila. 16-19 July. Pp. 1024-1027, Publicado 2004

Urko Zurutuza, Roberto Uribeetxeberria. Intrusion detection alarm correlation: a survey. IADAT International Conference on Telecommunications and Computer Networks. San Sebastian. 1-3 diciembre, Publicado 2004

PROYECTOS RELEVANTES

VARIoT: Vulnerability and Attack Repository for IoT. Comisión Europea, Connecting Europe Facility. (01/07/2019 - 30/06/2022). Cuantía total: 1.493.453 €

SENDAI: Segurtasun integrala industria adimentsurako. Gobierno Vasco, Programa Elkartek (KK-2019/00072). (01/06/2019 - 31/12/2020). Cuantía total: 903.835,08 €

COIOTE: Ciberseguridad Orientada al IoT y producto Electrónico (KK-2019/00082). (01/03/2019 - 31/12/2020). Cuantía total: 195.800 €

SKI4SPAM: Integración de Conocimiento Semántico para el Filtrado de Spam basado en Contenido (TIN2017-84658-C2-2-R). Ministerio de Economía, Industria y Competitividad, Programa Retos Investigación. (01/01/2018 - 30/03/2021). Cuantía subproyecto: 123.178 €

PROPHESY: Platform for rapid deployment of self-configuring and optimized predictive maintenance services. Comisión Europea, Programa H2020-FoF-2017. (01/10/2017 - 30/09/2020). Cuantía total: 5.528.318,51 €

AS-FABRIK: Bilbao Alliance for Smart Specialisation in Advanced Services Towards the Digital Transformation of the Industry. Comisión Europea, Programa Urban Innovation Action. (01/08/2017 - 31/07/2020). Cuantía total: 4.646.114 €

PRODUCTIVE 4.0: Electronics and ICT as enabler for digital industry and optimized supply chain management covering the entire product lifecycle. ECSEL. (01/05/2017 - 30/04/2020)

CYBERPREST: Cybersegurtasunerako gaitasun osoa. Gobierno Vasco, Programa Elkartek (KK-2018/00076). (01/07/2018 - 31/12/2019). Cuantía total: 713.612 €

Programa para el desarrollo del talento especializado en Ciberseguridad Industrial. Diputación Foral de Gipuzkoa. Promoción del talento y el emprendizaje de las personas en las empresas (TALENTUA –IKASKUNTZA - 93/2018). (03/09/2018 - 20/06/2019). Cuantía total: 68.846 €

OPENINAC: Industrial Network Access Control. Contrato de Investigación Colaborativa. OCF Industrial Cybersecurity SL; Open Cloud Factory, S.L. Fecha de inicio: 01/10/2018

SEKUTEK: Sekurtasun teknologiak. Gobierno Vasco, Programa Elkartek. (01/03/2017 - 31/12/2018)

POSIC: Nuevas aproximaciones para tecnologías de Ciberseguridad Industrial. Diputación Foral de Gipuzkoa. (01/05/2017 - 30/09/2018). Cuantía total: 44.200 €

PLENISENSE: Desarrollo de una Plataforma en la nube para el Despliegue de Soluciones de Negocio Basadas en Internet de las Cosas (IoT). Gobierno Vasco a través del Programa Gaitek. (01/07/2015 - 29/06/2018).

CC4.0: Countercraft, Contrainteligencia Digital en la Industria 4.0. Gobierno Vasco. Hazitek - Proy. de I+D carácter competitivo (ZL-2017/00901). (19/04/2017 - 31/12/2017)

KEA: Knowledge for Emulab based Applicatoins. Diputación Foral de Gipuzkoa Tipo de entidad: Red Guipuzcoana de Ciencia, Tecnología e Innovación. (01/09/2015 - 31/08/2016). Cuantía total: 46.396 €

SOCIALSPAM: Seguimiento y Filtrado de Spam Personalizado en Medios Sociales Mediante Modelos de Difusión y Análisis de Contenidos. Departamento de Educación, Política Lingüística y Cultura, Gobierno Vasco, Proyectos de Investigación Básica y/o Aplicada (PI20141102). (01/11/2014 - 30/06/2016)

SIMPLE: Security in Mobile Platforms with Event analysis. Gobierno Vasco a través del Programa Gaitek. (01/01/2013 - 31/12/2014)

Análisis de Datos y Ciberseguridad

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

PROYECTOS RELEVANTES

SIND: Diseño y desarrollo de un novedoso sistema para la Seguridad en entornos Industriales. Gobierno Vasco a través del Programa Gaitek. (01/01/2013 - 31/12/2014)

DA2SEC: Desarrollo Automatizado de Agentes de Seguridad para sistemas embebidos. Gobierno Vasco a través del Programa Saiotek (01/09/2012 - 31/12/2013)

new embedded Systems arcHItecturE for multi-Layer Dependable solutions (nSHIELD). Comisión Europea, Artemis Joint (01/09/2011-31/08/2013). Cuantía total: 7.349.000 €

IS_INCLOUD: Infraestructuras Críticas Seguras In the Cloud. Ministerio de Ciencia e Innovación a través del programa INNPACTO. (01/07/2011- 31/12/2014)

Pilot Embedded Systems Architecture for multi-Layer Dependable solutions. (pSHIELD). Comision Europea, Artemis Joint Undertaking (01/01/2011-31/12/2012). Cuantía total: 900.599 €

CONCHO: CONtrol Systems Check for Operational availability. Gobierno Vasco a través del Programa Universidad-Empresa. (01/01/2010-31/12/2011).

PSACC: Plataforma De Servicios Avanzados Bajo Un Modelo Cloud Computing.Gobierno Vasco a través del Programa INNOTEK. (01/09/2009-31/12/2010)

Euskalert, Episodio II: Servicios Avanzados de Analisis en la Red Vasca de Honeypots. Diputación Foral de Gipuzkoa Tipo de entidad: Organismo Público. (01/09/2008-31/12/2010)

Plataforma de Seguridad Avanzada Para Sistemas de Control Basados en SCADA (SeCADA). Ministerio de Industria, Turismo y Comercio, a traves del Plan Avanza I+D (sello EUROSTARS). (01/04/2008-31/12/2009)

Honeypot Resist NoE mini-project. European Comission, FP6 (Como afiliado a la Red de Excelencia Europea Resist). (01/01/2008-31/12/2008)

Tecnicas Avanzadas de Correlacion Aplicables a la Seguridad en Sistemas de Gestion de Eventos. Gobierno Vasco a través del Programa Innotek (01/07/2007-31/12/2008)