

Características generales

Características del Equipo de Investigación

Características de la Investigación

IDENTIFICACIÓN DEL EQUIPO INVESTIGADOR			
NOMBRE DEL EQUIPO O GRUPO DE INVESTIGACIÓN	VRAIN. Valencian Research Institute for Artificial Intelligence		
UNIDAD/DEPARTAMENTO DE PERTENENCIA	ELP. Extensions of Logic Programming		
CENTRO/INSTITUTO/UNIVERSIDAD/ORGANISMO DE PERTENENCIA	Universitat Politècnica de València		
			
DATOS DE CONTACTO			
DATOS DE CONTACTO DEL EQUIPO			
PERSONA DE CONTACTO	Santiago Escobar Román	TELÉFONO	963877000
ROL EN EL EQUIPO	Investigador Principal	MAIL	sescobar@dsic.upv.es
WEB DEL EQUIPO	https://vrain.upv.es/elp/		
DIRECCIÓN POSTAL DEL EQUIPO			
EDIFICIO	1F	CENTRO	Departamento de Sistemas Informáticos y Computación
TIPO DE VÍA	Calle	NOMBRE DE LA VÍA	Camí de Vera
NÚMERO	s/n	CIUDAD	València
PROVINCIA	Valencia	CÓDIGO POSTAL	46022
DATOS DE CONTACTO DEL ORGANISMO AL QUE PERTENECE			
PERSONA DE CONTACTO	Botti Navarro, Vicente Juan		
MAIL	vbotti@dsic.upv.es		
TELÉFONO	96 387 97 25		
WEB	https://vrain.upv.es/		
DIRECCIÓN POSTAL DEL ORGANISMO			
EDIFICIO	1F	CENTRO	Departamento de Sistemas Informáticos y Computación
TIPO DE VÍA	Calle	NOMBRE DE LA VÍA	Camí de Vera
NÚMERO	s/n	CIUDAD	València
PROVINCIA	Valencia	CÓDIGO POSTAL	46022



INVESTIGADOR PRINCIPAL

NOMBRE

Santiago Escobar Román

TITULACIÓN

Doctor en Ingeniería Informática

TRAYECTORIA PROFESIONAL

Profesor Titular Universitario, Profesor en el Grado en Ingeniería Informática de la asignatura Métodos Formales Industriales • Profesor en el Máster Universitario en Ingeniería y Tecnología de Sistemas Software de la asignatura Modelos Formales de Computación • Profesor en el Máster Universitario en Ciberseguridad y Ciberinteligencia de la asignatura Desarrollo y Despliegue Seguro. • Sexenios de investigación: 3 (último periodo 2011-2016) • Citas: Google Scholar: 2.081 / h-index: 29. WoS: 587 / h-index: 12. SCOPUS: 1.042 (total) / h-index: 15 • Publicaciones: Indexadas JCR: 92 / 34 (Q1). Congresos internacionales: 192 / 51 (LNCS) • Proyectos de Investigación: Investigador Principal en 11 proyectos internacionales y nacionales • Dirección de Tesis Doctorales: 6

WEB Y REDES SOCIALES

<http://personales.upv.es/sanesro/>



MIEMBROS DEL EQUIPO

Escobar Román, Santiago

 LÍNEAS Y ÁREAS DE INVESTIGACIÓN	
ÁREAS DE INVESTIGACIÓN	PRINCIPALES LÍNEAS DE INVESTIGACIÓN
ATAQUES Y DEFENSA ANTE AMENAZAS	Identificación y localización del atacante Búsqueda del origen de la amenaza Desarrollo de herramientas de detección de amenazas Detección de anomalías Detección y eliminación de malware Filtraciones de Información
EVALUACIÓN DE SISTEMAS Y CIBERRIESGOS	Modelos interoperables formales Modelado de sistemas y de ataques a sistemas Simulación de amenazas y ataques Simulación de entornos peligrosos
GESTIÓN DE LA IDENTIDAD	Controles de acceso basados en comportamiento Autenticación criptográfica Generación de identidades fiables a nivel global Computación verificable Computación segura multiparte Protocolos de autenticación Métodos de validación seguros Control de Acceso y Autenticación
INFRAESTRUCTURAS CRÍTICAS	Mejora de protocolos y estándares de seguridad Modelado de sistemas y de ataques a sistemas Detección de software malicioso
PROCESADO DE DATOS	Procesamiento seguro de datos
PRIVACIDAD	Protocolos criptográficos de preservación de la privacidad
SISTEMAS FIABLES Y ACTUALIZABLES	Lenguajes y Frameworks de desarrollo seguros Seguridad / Privacidad mediante el diseño Desarrollo de entornos integrados de seguridad Diseño de requisitos de seguridad Computación Segura Modelos computacionales de confianza Desarrollo de entornos de simulación para la experimentación con sistemas fiables
ÁREAS DE INTERÉS	Criptografía post-cuántica



PUBLICACIONES RELACIONADAS DESTACADAS

PUBLICACIONES AÑO 2022

- María Alpuente, Santiago Escobar, José Meseguer, Julia Sapiña:
Order-sorted equational generalization algorithm revisited. Ann. Math. Artif. Intell. 90(5): 499-522 (2022)
- María Alpuente, Demis Ballis, Santiago Escobar, Julia Sapiña:
Optimization of rewrite theories by equational partial evaluation. J. Log. Algebraic Methods Program. 124: 100729 (2022)
- María Alpuente, Santiago Escobar, Julia Sapiña, Demis Ballis:
Symbolic Specialization of Rewriting Logic Theories with Presto. Theory Pract. Log. Program. 22(3): 444-495 (2022)
- Francisco Durán, Steven Eker, Santiago Escobar, Narciso Martí-Oliet, José Meseguer, Rubén Rubio, Carolyn L. Talcott:
Equational Unification and Matching, and Symbolic Reachability Analysis in Maude 3.2 (System Description). IJCAR 2022: 529-540
- María Alpuente, Demis Ballis, Santiago Escobar, Julia Sapiña:
Variant-Based Equational Anti-unification. LOPSTR 2022: 44-60
- Duong Dinh Tran, Kazuhiro Ogata, Santiago Escobar, Sedat Akleyek, Ayoub Otmani:
Formal specification and model checking of Saber lattice-based key encapsulation mechanism in Maude. SEKE 2022: 382-387
- Raúl López-Rueda, Santiago Escobar:
Canonical Narrowing with Irreducibility and SMT Constraints as a Generic Symbolic Protocol Analysis Method. WRLA@ETAPS 2022: 45-64
- Raúl López-Rueda, Santiago Escobar, José Meseguer:
An Efficient Canonical Narrowing Implementation for Protocol Analysis. WRLA@ETAPS 2022: 151-170
- Canh Minh Do, Adrián Riesco, Santiago Escobar, Kazuhiro Ogata:
Parallel Maude-NPA for Cryptographic Protocol Analysis. WRLA@ETAPS 2022: 253-273

PUBLICACIONES AÑO 2021

- Damián Aparicio-Sánchez, Santiago Escobar, Catherine A. Meadows, José Meseguer, Julia Sapiña:
Protocol Analysis with Time and Space. Protocols, Strands, and Logic 2021: 22-49

PUBLICACIONES AÑO 2020

- María Alpuente, Angel Cuenca-Ortega, Santiago Escobar, José Meseguer:
Order-sorted Homeomorphic Embedding Modulo Combinations of Associativity and/or Commutativity Axioms. Fundam. Informaticae 177(3-4): 297-329 (2020)
- María Alpuente, Angel Cuenca-Ortega, Santiago Escobar, José Meseguer:
A partial evaluation framework for order-sorted equational programs modulo axioms. J. Log. Algebraic Methods Program. 110 (2020)
- Francisco Durán, Steven Eker, Santiago Escobar, Narciso Martí-Oliet, José Meseguer, Rubén Rubio, Carolyn L. Talcott:
Programming and symbolic computation in Maude. J. Log. Algebraic Methods Program. 110 (2020)
- Damián Aparicio-Sánchez, Santiago Escobar, Raúl Gutiérrez, Julia Sapiña:
An Optimizing Protocol Transformation for Constructor Finite Variant Theories in Maude-NPA. ESORICS (2) 2020: 230-250
- Damián Aparicio-Sánchez, Santiago Escobar, Catherine A. Meadows, José Meseguer, Julia Sapiña:
Protocol Analysis with Time. INDOCRYPT 2020: 128-150
- Damián Aparicio-Sánchez, Santiago Escobar, Julia Sapiña:
Variant-based Equational Unification under Constructor Symbols. ICLP Technical Communications 2020: 38-51
- Santiago Escobar, Narciso Martí-Oliet:
Rewriting Logic and Its Applications - 13th International Workshop, WRLA 2020, Virtual Event, October 20-22, 2020, Revised Selected Papers. Lecture Notes in Computer Science 12328, Springer 2020, ISBN 978-3-030-63594-7

PUBLICACIONES AÑO 2019

- María Alpuente, Santiago Escobar, Julia Sapiña, Demis Ballis:
Symbolic Analysis of Maude Theories with Narval. Theory Pract. Log. Program. 19(5-6): 874-890 (2019)
- Santiago Escobar, José Meseguer:
Canonical Narrowing with Irreducibility Constraints as a Symbolic Protocol Analysis Method. Foundations of Security, Protocols, and Equational Reasoning 2019: 15-38
- María Alpuente, Demis Ballis, Angel Cuenca-Ortega, Santiago Escobar, José Meseguer:
ACUOS2: A High-Performance System for Modular ACU Generalization with Subtyping and Inheritance. JELIA 2019: 171-181
- Santiago Escobar, Julia Sapiña:
Most General Variant Unifiers. ICLP Technical Communications 2019: 154-167

PUBLICACIONES AÑO 2018

- María Alpuente, Angel Cuenca-Ortega, Santiago Escobar, José Meseguer:
Homeomorphic Embedding Modulo Combinations of Associativity and Commutativity Axioms. LOPSTR 2018: 38-55
- Antonio González-Burgueño, Damián Aparicio-Sánchez, Santiago Escobar, Catherine A. Meadows, José Meseguer:
Formal verification of the YubiKey and YubiHSM APIs in Maude-NPA. LPAR 2018: 400-417
- Fan Yang, Santiago Escobar, Catherine A. Meadows, José Meseguer:
Modular Verification of Sequential Composition for Private Channels in Maude-NPA. STM 2018: 20-36
- Santiago Escobar:
Multi-paradigm Programming in Maude. WRLA@ETAPS 2018: 26-44
- Francisco Durán, Steven Eker, Santiago Escobar, Narciso Martí-Oliet, José Meseguer, Carolyn L. Talcott:
Associative Unification and Symbolic Reasoning Modulo Associativity in Maude. WRLA@ETAPS 2018: 98-114

PUBLICACIONES AÑO 2017

- Santiago Escobar:
Rewriting Logic and its Applications (extended selected papers from WRLA 2014). J. Log. Algebraic Methods Program. 86(1): 157-158 (2017)
- María Alpuente, Santiago Escobar, Julia Sapiña, Angel Cuenca-Ortega:
Inspecting Maude variants with GLINTS. Theory Pract. Log. Program. 17(5-6): 689-707 (2017)
- Horatiu Cirstea, Santiago Escobar:
Proceedings Third International Workshop on Rewriting Techniques for Program Transformations and Evaluation, WPTE@FSCD 2016, Porto, Portugal, 23rd June 2016. EPTCS 235, 2017

PUBLICACIONES AÑO 2016

- Santiago Escobar:
Rewriting logic and its applications (extended selected papers from WRLA 2014). J. Log. Algebraic Methods Program. 85(1): 1-2 (2016)
- Francisco Durán, Steven Eker, Santiago Escobar, Narciso Martí-Oliet, José Meseguer, Carolyn L. Talcott:
Built-in Variant Generation and Unification, and Their Applications in Maude 2.7. IJCAR 2016: 183-192
- María Alpuente, Angel Cuenca-Ortega, Santiago Escobar, José Meseguer:
Partial Evaluation of Order-Sorted Equational Programs Modulo Axioms. LOPSTR 2016: 3-20
- Fan Yang, Santiago Escobar, Catherine A. Meadows, José Meseguer, Sonia Santiago:
Strand spaces with choice via a process algebra semantics. PPDP 2016: 76-89



PUBLICACIONES RELACIONADAS DESTACADAS

PUBLICACIONES AÑO 2015

- Andrew Cholewa, Santiago Escobar, José Meseguer:
Constrained narrowing for conditional equational theories modulo axioms. Sci. Comput. Program. 112: 24-57 (2015)
- Manuel Clavel, Francisco Durán, Steven Eker, Santiago Escobar, Patrick Lincoln, Narciso Martí-Oliet, Carolyn L. Talcott:
Two Decades of Maude. Logic, Rewriting, and Concurrency 2015: 232-254
- Santiago Escobar, Catherine A. Meadows, José Meseguer, Sonia Santiago:
Symbolic Protocol Analysis with Disequality Constraints Modulo Equational Theories. Programming Languages with Applications to Biology and Security 2015: 238-261
- Antonio González-Burgueño, Sonia Santiago, Santiago Escobar, Catherine A. Meadows, José Meseguer:
Analysis of the PKCS#11 API Using the Maude-NPA Tool. SSR 2015: 86-106
- Yuki Chiba, Santiago Escobar, Naoki Nishida, David Sabel, Manfred Schmidt-Schauß:
2nd International Workshop on Rewriting Techniques for Program Transformations and Evaluation, WPTE 2015, July 2, 2015, Warsaw, Poland. OASICS 46, Schloss Dagstuhl - Leibniz-Zentrum für Informatik 2015, ISBN 978-3-939897-94-1
- Santiago Escobar:
Proceedings XIV Jornadas sobre Programación y Lenguajes, PROLE 2014, Cadiz, Spain, September 16-19, 2014. EPTCS 173, 2015

PUBLICACIONES AÑO 2014

- Santiago Escobar, Moreno Falaschi:
Functional and (Constraint) Logic Programming. Inf. Comput. 235: 1-2 (2014)
- María Alpuente, Santiago Escobar, Javier Espert, José Meseguer:
A modular order-sorted equational generalization algorithm. Inf. Comput. 235: 98-136 (2014)
- Santiago Escobar, Catherine A. Meadows, José Meseguer, Sonia Santiago:
State space reduction in the Maude-NRL Protocol Analyzer. Inf. Comput. 238: 157-186 (2014)
- Santiago Escobar:
Functional Logic Programming in Maude. Specification, Algebra, and Software 2014: 315-336
- Santiago Escobar, Catherine A. Meadows, José Meseguer, Sonia Santiago:
A rewriting-based forwards semantics for Maude-NPA. HotSoS 2014: 3
- María Alpuente, Santiago Escobar, Javier Espert, José Meseguer:
ACUOS: A System for Modular ACU Generalization with Subtyping and Inheritance. JELIA 2014: 573-581
- Fan Yang, Santiago Escobar, Catherine A. Meadows, José Meseguer, Paliath Narendran:
Theories of Homomorphic Encryption, Unification, and the Finite Variant Property. PPDP 2014: 123-133
- Antonio González-Burgueño, Sonia Santiago, Santiago Escobar, Catherine A. Meadows, José Meseguer:
Analysis of the IBM CCA Security API Protocols in Maude-NPA. SSR 2014: 111-130
- Sonia Santiago, Santiago Escobar, Catherine A. Meadows, José Meseguer:
A Formal Definition of Protocol Indistinguishability and Its Verification Using Maude-NPA. STM 2014: 162-177
- Santiago Escobar, Konstantin Korovin, Vladimir V. Rybakov:
UNIF 2012 Post-Workshop Proceedings. The 26th International Workshop on Unification, Manchester, UK, July 1, 2012. EPIC Series in Computing 24, EasyChair 2014
- Santiago Escobar:
Rewriting Logic and Its Applications - 10th International Workshop, WRLA 2014, Held as a Satellite Event of ETAPS, Grenoble, France, April 5-6, 2014, Revised Selected Papers. Lecture Notes in Computer Science 8663, Springer 2014, ISBN 978-3-319-12903-7

PUBLICACIONES AÑO 2013

- Serdar Erbatur, Santiago Escobar, Deepak Kapur, Zhiqiang Liu, Christopher Lynch, Catherine A. Meadows, José Meseguer, Paliath Narendran, Sonia Santiago, Ralf Sasse:
Asymmetric Unification: A New Unification Paradigm for Cryptographic Protocol Analysis. CADE 2013: 231-248
- Elena Lloret, Santiago Escobar, Manuel Palomar, Isidro Ramos:
Incremental and Adaptive Software Systems Development of Natural Language Applications. ISD 2013: 511-523
- Santiago Escobar:
Unification and Anti-unification modulo Equational Theories. UNIF@RTA/TLCA 2013: 1
- María Alpuente, Santiago Escobar, Javier Espert:
Detecting Modular ACU Structural Symmetries. UNIF@RTA/TLCA 2013: 3-7
- Kyungmin Bae, Santiago Escobar, José Meseguer:
Abstract Logical Model Checking of Infinite-State Systems Using Narrowing. RTA 2013: 81-96

PUBLICACIONES AÑO 2012

- Santiago Escobar, Ralf Sasse, José Meseguer:
Folding variant narrowing and optimal variant termination. J. Log. Algebraic Methods Program. 81(7-8): 898-928 (2012)
- Serdar Erbatur, Santiago Escobar, Paliath Narendran:
The use of types in designing unification algorithms: two case studies. UNIF 2012: 7-16
- Serdar Erbatur, Santiago Escobar, Deepak Kapur, Zhiqiang Liu, Christopher Lynch, Catherine A. Meadows, José Meseguer, Paliath Narendran, Sonia Santiago, Ralf Sasse:
Effective Symbolic Protocol Analysis via Equational Irreducibility Conditions. ESORICS 2012: 73-90



PROYECTOS RELEVANTES

TÍTULO DEL PROYECTO: LogicExtreme: Tecnología Lógica y Software Seguro ENTIDAD FINANCIADORA GENERALITAT VALENCIANA PERIODO: Enero2011 - Diciembre 2015

TÍTULO DEL PROYECTO: Protocol Verification: Beyond Reachability Properties ENTIDAD FINANCIADORA NSA (National Security Agency, USA) PERIODO: Enero 2012 - Enero 2013

TÍTULO DEL PROYECTO: Development of a Next-Generation Security Protocol Analyzer Tool ENTIDAD FINANCIADORA NSA (National Security Agency, USA) PERIODO: Abril 2014 - Abril 2017

TÍTULO DEL PROYECTO: Smartlogic: Tecnologías lógicas para la seguridad, modelado, análisis y rendimiento del software ENTIDAD FINANCIADORA GENERALITAT VALENCIANA PERIODO: Enero2015 - Diciembre 2019

TÍTULO DEL PROYECTO: Symbolic Specification and Analysis of Safe and Secure Interactions among CPS Agents and Devices ENTIDAD FINANCIADORA: ONR (Office of Naval Research) PERIODO: Enero 2017 - Diciembre 2019

TÍTULO DEL PROYECTO: Advanced symbolic methods for the cryptographic protocol analyzer Maude-NPA ENTIDAD FINANCIADORA AFOSR (Air Force Office of Scientific Research, USA) PERIODO: Julio 2017 - Junio 2020

TÍTULO DEL PROYECTO: Ayudas para la excelencia de equipos de investigación avanzada en ciberseguridad-contratación postdoctoral- Martínez Plumed and postdoctoral-Gutiérrez Gil ENTIDAD FINANCIADORA Instituto Nacional de Ciberseguridad de España (INCIBE) PERIODO: Enero2018 - Diciembre 2020

TÍTULO DEL PROYECTO: Foundations of trustworthy AI-integrating reasoning, learning and optimization ENTIDAD FINANCIADORA: Comisión Europea PERIODO: Septiembre 2020 - Septiembre 2023

TÍTULO DEL PROYECTO: Formal analysis and verification of post-quantum cryptographic protocols ENTIDAD FINANCIADORA: EIG CONCERT Japan PERIODO: Abril 2021 - Abril 2023