Luis Antonio Garcia

Curriculum Vitae

☎ *(305) 984-1845*
✉ *lgarcia@isi.edu*
🖱 *lagarcia.us*

Research Interests

My current and future research interests reside in the alignment of a human's semantic understanding of the world with a deep learning model's semantic understanding of its environment. The goal is to enable a deterministic relationship for providing mutual assurances in cyber-physical contexts. In particular, my research aims to answer the following three questions:

- **Integration of Human Logic & Deep Learning in Cyber-physical Contexts.** How can we design neural-symbolic frameworks that are semantically conscious of their subsuming cyber-physical systems?
- **Programming Abstractions for Performant Cyber-physical Systems.** In distributed and heterogeneous IoT environments enabled with such neural-symbolic frameworks, what are the correct programming abstractions that need to be exposed to developers?
- **Safety, Security, and Privacy for Performant Cyber-physical Systems.** How can we defend against collateral safety, security, and privacy threats that will subsequently be exposed by semantically-aware, sensor-rich, adaptive, and distributed heterogeneous IoT environments?

Professional Experience

06/2020-Present **University of Southern California Information Sciences Institute**
Research Computer Scientist
USC Viterbi School of Engineering

07/2018 - 06/2020 **University of Calfiornia, Los Angeles**
Postdoctoral Scholar in the Department of Electrical and Computer Engineering.

01/2019-05/2020 **Postdoctoral Association, University of California, Los Angeles**
Vice Chair of Communications on executive board of Postdoctoral Association (PDA) at UCLA that represents the postdoctoral scholar community (∼1400 scholars).

05/2017 - 11/2017 **Carnegie Mellon University, Pittsburgh, PA**
Visiting Scholar in Logical System Lab with Dr. André Platzer.

Developed a syntactic and semantic translation of programmable logic controller programming languages to verifiable hybrid program representations.

05/2015 - 08/2015 **Siemens Corporate Research, Princeton, NJ**
Graduate Intern Software Developer for cybersecurity group with Dr. Dong Wei.

Developed and investigated intrusion detection solutions for programmable logic controllers and assessed vulnerabilities on legacy and current programmable logic controller platforms.

05/2013 - **Blackberry, Sunrise, FL**
08/2013 Embedded OS Software Developer with Jose Pena.

Developed internal tools for software version-control systems and investigated factory operating system issues.

05/2011 - **Blackberry, Sunrise, FL**
12/2011 Competitive Analysis Research Assistant in competitive analysis group with Dalier Ramirez.

Automated tests to compare performance of wireless and radio frequency components of different mobile devices.

08/2010 - **Blackberry, Irving, TX**
11/2010 Baseband Interface Validation Associate on platform team with Gary Borst.

Performed functional and parametric testing on the peripherals of the circuit boards of several platform devices using Agilent and Tektronix oscilloscopes mobile devices.

Education

07/2018- **University of California, Los Angeles**
06/2020 Postdoctoral Scholar
UCLA Samueli School of Electrical & Computer Engineering
Advisor: Dr. Mani Srivastava

08/2014 - **Rutgers University**
06/2018 Ph.D. in Computer Engineering, Cybersecurity Track
Electrical and Computer Engineering Department
Dissertation: Physics for the Sake of Security, Security for the Sake of Physics
Advisor: Dr. Saman Zonouz

05/2017 - **Carnegie Mellon University**
11/2017 Visiting Scholar
Logical Systems Lab, Computer Science Department
Advisor: Dr. André Platzer

08/2012 - **University of Miami**
05/2014 Master of Science in Computer and Electrical Engineering
Electrical and Computer Engineering Department
Thesis: Context-aware Information-flow-based Micro-security Perimeters for Mobile Devices
Advisor: Dr. Saman Zonouz

08/2008 - **University of Miami**
05/2014 Bachelor of Science in Computer Engineering
Electrical and Computer Engineering Department

Selected Publications

ICCPS '19 ☆ Luis Garcia, Stefan Mitsch, André Platzer, HyPLC: Hybrid Programmable Logic Controller Program Translation for Verification, IEEE/ACM International Conference on Cyber-Physical Systems (ICCPS), 2019. **(Best Paper Finalist)**

NDSS '17 Luis Garcia, Ferdinand Brasser, Mehmet Hazar, Osama Mohammed, Ahmad-Reza Sadeghi, Saman Zonouz, Hey, My Malware Knows Physics! Attacking PLCs with Physical Model Aware Rootkit Network, Network and Distributed System Security Symposium (NDSS), 2017.

USENIX Sec. '17 Christian Bayens*, Tuan Le*, Luis Garcia*, Raheem Beyah, Mehdi Javanmard, and Saman Zonouz, See No Evil, Hear No Evil, Feel No Evil, Print No Evil? Malicious Fill Patterns Detection in Additive Manufacturing, USENIX Security Symposium (USENIX Security), 2017. *Equal Contributions.

All Publications

MobiCom '21 *Under Review* Renju Liu, Zaoxing Liu, Botong Ou, Luis Garcia, Mani Srivastava, So Little Time, SecDeep: Secure and Performant Deep Learning Inference Framework for Edge Devices, 27th Annual International Conference on Mobile Computing and Networking (MobiCom), 2021.

NDSS '21 *Under Review* Taegyu Kim, Aolin Ding, Sriharsha Etigowni, Pengfei Sun, Jizhou Chen, Luis Garcia, Saman Zonouz, Dongyan Xu, Dave (Jing) Tian, Patching Control-Semantic Bugs in RAV Firmware using DISPATCH, Network and Distributed System Security Symposium (NDSS), 2021.

NDSS '21 *Under Review* Hamid Reza Ghaeini, Matthew Chan, Hamed Nemati, Ahmad Ibrahim, Michael Backes, Luis Garcia, Saman Zonouz, Nils-Ole Tippenhauer, So Little Time, So Much to Secure: Scheduling Run-time Code and Data Integrity Verification for Robotic Vehicles with Real-time Control, Network and Distributed System Security Symposium (NDSS), 2021.

CoRL '20 *Under Review* Sandeep Singh, Bharathan Balaji, Luis Garcia, Mani Srivastava, Sim2Real Transfer for Deep Reinforcement Learning with Stochastic State Transition Delays, Conference on Robot Learning (CoRL), 2020.

NeurIPS '20 *Under Review* Jeya Vikranth Jeyakumar, Joseph Noor, Yu-Hsi Cheng, Luis Garcia, Mani Srivastava, How Can I Explain This to You? An Empirical Study of Deep Neural Network Explanation Methods, Advances in Neural Information Processing Systems (NeurIPS), 2020.

USENIX '20 *Under Review* Akash Deep Singh, Joseph Noor, Luis Garcia, Mani Srivastava, I Always Feel Like Somebody's Sensing Me! A Framework to Detect, Identify, and Localize Clandestine Wireless Sensors, USENIX Security Symposium (USENIX Security), 2021.

TPAMI '20 *Under Review* Alzantot, Moustafa, Luis Garcia, Mani Srivastava, PhysioGAN: Training High Fidelity Generative Model for Physiological Sensor Readings, Transactions on Pattern Analysis and Machine Intelligence (TPAMI), 2020.

SenSys '20 *Under Review* Tianwei Xing, Marc Roig Vilamala, Luis Garcia, Federico Cerutti, Lance Kaplan, Alun Preece and Mani Srivastava, Neuroplex: Learning Enabled Complex Event Detection using Neurally Reconstructed Logic, ACM Conference on Embedded Networked Sensor Systems (SenSys), 2020.

DSN '20 Pengfei Sun, Luis Garcia, Gabriel Salles-Loustau, Saman Zonouz, Hybrid Firmware Analysis for Known Mobile and IoT Security Vulnerabilities, IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2020.

ICCPS '20 Luis Garcia, Ferdinand Brasser, Michael Roeder, Sridhar Adepu, Lucas Davi, Ahmad-Reza Sadeghi, Saman Zonouz, Control Behavior Integrity for Distributed Cyber-Physical Systems, Annual Computer Security Applications Conference (ICCPS), 2020.

BuildSys '19 Renju Liu, Ziqi Wang, Luis Garcia, Mani Srivastava, RemedIoT: Remedial Actions for Internet-of-Things Conflicts, International Conference on Systems for Energy-Efficient Buildings, Cities, and Transportation (BuildSys), 2019.

mmNets '19 Akash Deep Singh, Sandeep Singh Sandha, Luis Garcia, Mani Srivastava, RadHAR: Human Activity Recognition from Point Clouds Generated through a Millimeter-wave Radar, ACM Workshop on Millimeter-Wave Networks and Sensing Systems (mmNets), 2019.

MILCOM '19 Joseph Noor, Ahmed Ali-Eldin, Luis Garcia, Chirag Rao, Venkat R. Dasari, Deepak Ganesan, Brian Jalaian, Prashant Shenoy, Mani Srivastava, The Case for Robust Adaptation: Autonomic Resource Management is a Vulnerability, The Global Stage for Innovation in Military Communication (MILCOM), 2019.

RAID '19 Hamid Reza Ghaeini, Matthew Chan, Raad Bahmani, Ferdinand Brasser, Luis Garcia, Jianying Zhou, Ahmad-Reza Sadeghi, Nils Ole Tippenhauer, Saman Zonouz, PAtt: Physics-based Attestation of Control Systems, International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2019.

DSN '19 Pengfei Sun, Luis Garcia, Saman Zonouz, Tell Me More Than Just Assembly! Reversing Cyber-physical Execution Semantics of Embedded IoT Controller Software Binaries, IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2019.

DAIS '19 Tianwei Xing, Marc Roig Vilamala, Luis Garcia, Federico Cerutti, Lance Kaplan, Alun Preece and Mani Srivastava, DeepCEP: Deep Complex Event Processing Using Distributed Multimodal Information, Workshop on Distributed Analytics InfraStructure and Algorithms for Multi-Organization Federations (DAIS), 2019.

IoTDI ’19 Joseph Noor, Hsiao-Yun Tseng, Luis Garcia, Mani Srivastava, DDFlow: Visualized Declarative Programming for Heterogeneous IoT Networks, International Conference on Internet-of-Things Design and Implementation (IoTDI), 2019.

IoTDI ’19 (Demo) ✯ Joseph Noor, Sandeep Singh Sandha, Luis Garcia, Mani Srivastava, Demo: DDFlow Visualized Declarative Programming for Heterogeneous IoT Networks on Heliot Testbed Platform, International Conference on Internet-of-Things Design and Implementation (IoTDI), 2019. **(Best Demo Award)**

ICCPS ’19 (Poster) Luis Garcia, Stefan Mitsch, André Platzer, Poster: Toward Multi-Task Support and Security Analyses in PLC Program Translation for Verification, IEEE/ACM International Conference on Cyber-Physical Systems (ICCPS), 2019.

USENIX Sec. ’19 (Poster) Pengfei Sun, Luis Garcia, Saman Zonouz, Poster: Towards Robust Semantic Reverse Engineering of Control System Binaries, USENIX Security Symposium (USENIX Security), 2019.

DSN ’18 Zhenqi Huang, Sriharsha Etigowni, Luis Garcia, Sayan Mitra, Saman Zonouz, Algorithmic Attack Synthesis using Hybrid Dynamics of Power Grid Critical Infrastructures, IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2018.

DASC ’18 Mingbo Zhang, Luis Garcia, Pengfei Sun, Xiruo Liu, Saman Zonouz, Dynamic Memory Protection via Intel SGX-Supported Heap Allocation, IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC), 2018.

SmartGrid Comm ’17 Gabriel Salles-Loustau, Luis Garcia, Pengfei Sun, Maryam Dehnavi, Saman Zonouz, Power Grid Safety Control via Fine-Grained Multi-Persona Programmable Logic Controllers, IEEE International Conference on Smart Grid Communications (SmartGridComm), 2017.

Res. Week ’16 Luis Garcia, Saman Zonouz, Dong Wei, Leandro Pfleger de Aguiar, Detecting PLC Control Corruption via On-Device Runtime Verification, IEEE Resilience Week 2016.

DSN ’16 Gabriel Salles-Loustau, Luis Garcia, Kaustubh Joshi, Saman Zonouz, Swirls: Context-Aware Information-Flow-Based Micro-Security Perimeters for Mobile Devices, IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2016.

TOSG ’15 Katherine R. Davis, Charles M. Davis, Saman A. Zonouz, Rakesh B. Bobba, Robin Berthier, Luis Garcia, Peter W. Sauer, A Cyber-Physical Modeling and Assessment Framework for Power Grid Infrastructures, IEEE Transactions on Smart Grid, 2015.

SmartGrid Comm ’14 Luis Garcia, Henry Senyondo, Stephen McLaughlin, Saman Zonouz, Covert Channel Communication Through Physical Interdependencies in Cyber-Physical Infrastructures, IEEE International Conference on Smart Grid Communications (SmartGridComm), 2014.

SmartGrid Comm '14 Saman Zonouz, Luis Garcia, TMQ: Threat Model Quantification in Smart Grid Critical Infrastructures, IEEE International Conference on Smart Grid Communications (SmartGridComm), 2014.

Honors & Awards

2019 ACM/IEEE Conference on Internet of Things Design and Implementation (IoTDI) Best Demo Award

2019 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS) Best Paper Finalist

2019 International Conference on Dependable Systems and Networks (DSN) Student Travel Grant

2017 USENIX Security Symposium Student Travel Grant

2017 ECEDHA iREDEFINE Workshop Student Travel Grant

2016 - 2018 Graduate Assistance in Areas of National Need Fellowship

2016 International Conference on Dependable Systems and Networks (DSN) Student Travel Grant

2016 Rutgers ECE PhD Research Excellence Award

2015 National Science Foundation Cyber-Physical Systems Week Student Travel Award

2013 Eta Kappa Nu Electrical and Computer Engineering Honor Society

2013 Blackberry Campus Ambassador for the University of Miami

2006 Eagle Scout

Proposal Writing Experience

2020 *Under Review* **CPS: Medium: Trustworthy Cyber-Physical Additive Manufacturing with Untrusted Controllers**

Requested Amount: $1,200,000

Duration: 2 Years.

Investigators: Luis Garcia [Lead PI], Aram Galstyan (USC ISI) [Co-PI], Cory Inman (UCLA) [Co-PI]

Sponsor: National Science Foundation (NSF) - Cyber-Physical Systems (CPS) program

2017 **CPS: Medium: Trustworthy Cyber-Physical Additive Manufacturing with Untrusted Controllers**

Amount: $1,000,000 (Rutgers share: $666,000)

Duration: August 1 2017 - July 31 2020.

Investigators: Saman Zonouz [Lead PI], Mehdi Javanmard (Rutgers), Athina Petropulu (Rutgers), Raheem Beyah (Georgia Tech). **My role**: I helped writing the technical sections of the proposal.

Sponsor: National Science Foundation (NSF) - Cyber-Physical Systems (CPS) program

Patents

P.1 Saman Aliari Zonouz, Mehdi Javanmard, Abdul Beyah, **Luis Garcia**, Tuan-Anh Le, Christopher Bayens. "Post-Print Physical Vetting of 3D Prints with Minimal Embedded Nano-Material Assessor", C 2019.

Talks and Presentations

09/2019 **Feeling Safe and Secure in a Learning-enabled Cyber-physical World**
University of Central Florida, hosted by Aziz Mohaisen

09/2019 **Feeling Safe and Secure in a Learning-enabled Cyber-physical World**
University of Southern California Information Sciences Institute (ISI), hosted by Jeremy Abramson

10/2018 **On the Cyber-physical Safety and Security of Learning-Enabled Internet-of-Things**
NSF IoT Workshop, co-located with ICCAD 2018

03/2018 **Physics for the Sake of Security, Security for the Sake of Physics**
Stevens Institute of Technology, hosted by Georgios Portokalidis

03/2018 **Physics for the Sake of Security, Security for the Sake of Physics**
Fordham University, hosted by Thaier Hayajneh

03/2018 **Physics for the Sake of Security, Security for the Sake of Physics**
University of Texas El Paso, hosted by Miguel Velez-Reyes

02/2018 **Physics for the Sake of Security, Security for the Sake of Physics**
Vanderbilt University, hosted by Taylor Johnson

01/2018 **Physics for the Sake of Security, Security for the Sake of Physics**
University of Pennsylvania, hosted by Insup Lee

01/2017 **Leveraging Physical Models for Attacking and Defending PLCs**
CREDC Affiliate Presentation, `http://y2u.be/VdbLuCGKflA`

Teaching and Mentoring

University of California, Los Angeles

Los Angeles Computing Circle (Lecturer) (Summer '19)

Security and Privacy for Embedded Systems, Cyber-Physical Systems, and Internet of Things (Guest Lecturer) (Spring '19)

Embedded Systems (Guest Lecturer) (Spring '19, Fall '19)

Human-Computer Interaction (Guest Lecturer) (Fall '19)

Rutgers University

Programming Methodology I (TA) (Spring '15)

Malware Analysis and Reverse Engineering (Lecturer) (Spring '15)

Wyzant Tutoring (Tutor)

35 hours of tutoring

Perfect 5-start rating

Sample student comments: “I feel more confident with my upcoming course knowing that I am getting tutored by an expert in my field.”; “I am very pleased with Luis’ preparation for lecture notes and sample programs for our Java lessons.”

Service

2019 - **Program Committee**
Present Workshop on Artificial Intelligence and Industrial Internet-of-Things Security (AIoTS) 2019

2018 - **Reviewer**
Present TSG ’18-’19, TOPS ’19, AIoTS ’19-’20, IJCAI ’20

01/2019 - **Postdoctoral Association**
05/2020 Executive Board Vice Chair of Communications

Ph.D. Coursework

Computer Systems Security; Software Design and Verification; Embedded Microprocessor System Design; Computer Architecture; Foundations of Cyber-physical Systems; Smart Grid: Fundamental Elements of Design; Malware Analysis and Reverse Engineering; Internet Computing with Java; Computability, Complexity, and Algorithms; Algorithms in C++; Data Structures in C++; Mobile Computing (Android); Computer Operating Systems; Data Mining; Database Design and Management; Machine Learning; Computer Organizational Design and Architecture