# Luis Antonio Garcia

*Curriculum Vitae*

✉ *la.garcia@utah.edu*
🖱 *lagarcia.us*

## Professional Experience

07/2023- **University of Utah Kahlert School of Computing**
Present Assistant Professor

07/2022- **University of Southern California Department of Computer Science**
06/2023 Research Assistant Professor
USC Viterbi School of Engineering

06/2020- **University of Southern California Information Sciences Institute**
06/2023 Research Computer Scientist
USC Viterbi School of Engineering

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

## Education

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

## Publications (Recent)

NeurIPS '22 Shushan Arakelyan, Anna Hakhverdyan, Miltiadis Allamanis, Christophe Hauser, **Luis Garcia**, and Xiang Ren, NS3: Neuro-Symbolic Semantic Code Search, Conference on Neural Information Processing Systems (NeurIPS), 2022.

IEEE M&N '22 **Luis Garcia**, Genevieve Bartlett, Srivatsan Ravi, Harun Ibrahim, Wes Hardaker, Erik Kline, Explaining Deep Learning Models for Per-packet Encrypted Network Traffic Classification, IEEE International Symposium on Measurements & Networking (M&N), 2022.

MobiSys '22 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, ACM International Conference on Mobile Systems, Applications, and Services (MobiSys), 2022.

SafeThings '22 ✯ Haoda Wang, Christophe Hauser, **Luis Garcia**, AutoCPS: Control Software Dataset Generation for Semantic Reverse Engineering, IEEE Workshop on the Internet of Safe Things (SafeThings), 2022.**(Best Paper Award)**

IMWUT '22 Swapnil Sayan Saha, Sandeep Singh Sandha, **Luis Garcia**, Mani Srivastava, TinyOdom: Hardware-Aware Efficient Neural Inertial Navigation, Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT), 2022.

SEC '21 Renju Liu, **Luis Garcia**, Mani Srivastava, Aerogel: Lightweight Access Control Framework for WebAssembly-Based Bare-Metal IoT Devices, The Sixth ACM/IEEE Symposium on Edge Computing (SEC), 2021.

CheckMATE '21 Nicolaas Weideman, Virginia K. Felkner, Wei-Cheng Wu, Jonathan May, Christophe Hauser, **Luis Garcia**, PERFUME: Programmatic Extraction and Refinement For Usability of Mathematical Expression, Research on Offensive and Defensive Techniques in the Context of Man At The End Attacks Workshop (CheckMATE), 2021.

RAID '21 Aolin Ding, Praveen Murthy, **Luis Garcia**, Pengfei Sun, Matthew Chan, Saman Zonouz, Mini-Me, You Complete Me! Data-Driven Drone Security via DNN-based Approximate Computing, International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2021.

USENIX Sec. '21 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.

IoTDI '21 Renju Liu, Zaoxing Liu, Botong Ou, **Luis Garcia**, Mani Srivastava, SecDeep: Secure and Performant On-device Deep Learning Inference Framework for Mobile and IoT Devices, International Conference on Internet-of-Things Design and Implementation (IoTDI), 2021.

IoTDI '21 Tianwei Xing, **Luis Garcia**, Federico Cerutti, Lance Kaplan, Alun Preece, Mani Srivastava, DeepSQA: Understanding Sensor Data via Question Answering, International Conference on Internet-of-Things Design and Implementation (IoTDI), 2021.

CoRL '20 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 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.

SenSys '20 Ziqi Wang, Zhe Chen, Akash Deep Singh, **Luis Garcia**, Jun Luo, Mani Srivastava, UWHear: Through-wall Extraction and Separation of Audio Vibrations Using Wireless Signals, 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.

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.

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.

## Honors & Awards

| | |
|---|---|
| 2022 | IEEE Workshop on the Internet of Safe Things (SafeThings) Best Paper Award |
| 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 |

## Service

2020-Present **NSF Panelist**
Served on 4 panels

2019-Present **Program Chair**
IEEE Workshop on the Internet of Safe Things 2021, ACM Workshop on Challenges in Artificial Intelligence and Machine Learning for Internet of Things (AIChallengeIoT) 2022, Sensors S&P

2019 - Present **Program Committee**
USENIX Artifact Evaluation Committee 2021, Workshop on Artificial Intelligence and Industrial Internet-of-Things Security (AIoTS) 2019, CheckMATE Workshop 2021

2018 - Present **Reviewer**
TSG ’18-’19, TOPS ’19, AIoTS ’19-’20, IJCAI ’20-’21, AAAI ’22, ACM TIoT ’20-’21, RICCS ’23, IAAI ’22-23

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