Carlos E. Rubio-Medrano, Ph.D.

carloserm@gmail.com
https://carlosrubiomedrano.com
@crubiomedrano

PROFESSIONAL EXPERIENCE

- *Assistant Professor of Computer Science* — August 2020 - Date
  Texas A&M University - Corpus Christi, Corpus Christi, TX, USA.
- *Postdoctoral Researcher* — January 2017 - July 2020
  Arizona State University, Tempe, AZ, USA.
- *Course Lecturer* — September 2013 - May 2019
  Arizona State University, Tempe, AZ, USA.
- *Research Assistant* — September 2012 - December 2016
  Arizona State University, Tempe, AZ, USA.
- *Software Engineer* — October 2010 - August 2012
  PSMac, Inc., Chihuahua City, Mexico.

EDUCATION

- *Doctor of Philosophy,* Computer Science, — December 2016
  Specialization: Cybersecurity,
  Arizona State University (ASU), Tempe, AZ, USA.
  Advisor: Dr. Gail-Joon Ahn.
- *Master of Science,* Computer Science, — May 2008
  Specialization: Software Specification, Validation and Verification,
  The University of Texas at El Paso (UTEP), El Paso, TX, USA.
  Advisor: Dr. Yoonsik Cheon.
- *Bachelor of Science,* Computer Science, — May 2005
  Instituto Tecnológico de Chihuahua II, Chihuahua City, Mexico.

RESEARCH SPECIALTIES AND PROJECTS

In my experience as a researcher and as a software engineer, I have lead several industrial and academic projects that require an intensive learning and brain-storming process. As a result, I have experience on the inception, preparation and communication of ideas, and I can effectively contribute to projects that focus on effectiveness, efficiency, and innovation. My research interests lay at the intersection of cybersecurity and software specification, verification, and validation. Concretely, I have experience on the development of techniques for verifying the correct implementation of access control models at the source-code level using formal specifications. Also, I have interest in the enforcement of fundamental cybersecurity principles and methodologies for emerging technologies, e.g., authorization and access control. Also recently, I have explored approaches for enhancing the protection of mission-critical cyber-infrastructures such as Energy Delivery Systems (EDS) and Unmanned Aerial Vehicles (UAVs), a.k.a., *drones*. A list of successful projects I have led include:

- *Authorization and Access Control*: an approach for enforcing authorization constraints in emerging technologies [SACMAT19-1], a federated approach for handling authorization policies among independently-run organizations [PhDDiss, SACMAT15], a risk assessment framework for authorization policies [SACMAT20, ABAC18], and an approach for dynamically adjusting policies to prevent attacks [MTD17].

- *Software Specification, Verification and Validation*: an approach for modeling multi-model authorization constraints in production software [SACMAT19-2], an specification framework for verifying access control models at the source code level [COMSPAC13, EAI14], as well as a methodology for enforcing access control contract in Java modules [STPSA10, MSThesis].
- *Cybersecurity Monitoring and Assessment*: an analysis of online cyberfraud and abuse [USENIX21], an analysis of underground Internet forums [CODASPY19], a next-generation honeypot for protecting industrial control systems [CCS20], a framework for automated risk monitoring and assessment [MSCPES19, DTRAP21], an ontology engine comprising security requirements for mission-critical environments [CIC17], as well as a study on the peer review process of research papers in the security community [S&P22].

RESEARCH FUNDING

MSI21 *Dynamically Enforcing User-Oriented Geospatial Restrictions for Drone Fly-Overs*.
Carlos E. Rubio-Medrano (PI), Pablo Rangel, Jose Baca, Tianxing Chu.
National Science Foundation. Computer and Information Science and Engineering Minority-Serving Institutions (CSE-MSI) Research Expansion Program.
Award No. 2131263. $486,455.00.
October 2021 - September 2024.

CICI22 *Enabling Zero-Trust Resource Access Management for Scientific Collaborations*.
Gail-Joon Ahn (PI), **Carlos E. Rubio-Medrano (Co-PI)**, Jaejong Baek.
National Science Foundation. Cybersecurity Innovation for Cyberinfrastructure (CICI) Program.
Award No. 2232911. $591,664.00.
October 2022 - September 2025.

MRI22 *Acquisition of High-Performance Computing Cluster for Research in Engineering, Science, and Technology*.
Dulal Kar (PI), Philippe E Tissot, James C Gibeaut, Christopher Bird, Chuntao Liu, **Carlos E. Rubio-Medrano (Senior Personnel)**, Tianxing Chu (Senior Personnel), Chen Pan (Senior Personnel).
National Science Foundation. Major Research Instrumentation Program.
Award No. 2216335. $1,166,605.00.
October 2022 - September 2025.

PUBLICATIONS

My research work has led to 30+ publications in prestigious computer security venues including the ACM Conference in Computer and Communications Security (**CCS**), the USENIX Security Symposium (**USENIX**), the IEEE Security & Privacy Symposium (**S&P**), the ACM Symposium on Access Control Models and Technologies (**SACMAT**), the ACM Conference on Data and Applications Security and Privacy (**CODASPY**), and the IEEE International Computer Software and Applications Conference (**COMPSAC**).

Dissertations

PhDDiss *Federated Access Management for Collaborative Environments*.
Carlos E. Rubio-Medrano. Ph.D. Dissertation.
Arizona State University, December, 2016.

MSThesis *A Formal Approach to Specifying Access Control Security Features of Java Modules*.
Carlos E. Rubio-Medrano. MS Computer Science Thesis.
The University of Texas at El Paso, March, 2008.

Conference Papers

S&P22 *“Flawed, but like democracy we don’t have a better system”: The Experts’ Insights on the Peer Review Process of Evaluating Security Papers*. Ananta Sojeni, Faris Bugra Kokulu, **Carlos E. Rubio-Medrano**, Tiffany Bao, Ruoyu Wang, Yan Shoshitaishvili and Adam Doupé. In Proceedings of the IEEE Symposium on Security and Privacy (IEEE S&P 2022). San Francisco, California, USA, May 23-26, 2022.

SKM21 *DyPolDroid: Protecting Users and Organizations from Permission-Abuse Attacks in Android*. **Carlos E. Rubio-Medrano**, Matthew Hill, Luis Claramunt, Jaejong Baek, and Gail-Joon Ahn. In Proceedings of the International Conference on Secure Knowledge Management in the Artificial Intelligence Era (SKM 2021), San Antonio, Texas, USA, October 8-9, 2021.

USENIX21 *Having Your Cake and Eating It: An Analysis of Concession-Abuse-as-a-Service*. Eric Sun, Adam Oest, Penghui Zhang, **Carlos E. Rubio-Medrano**, Tiffany Bao, Ruoyu Wang, Ziming Zhao, Yan Shoshitaishvili, Adam Doupé, and Gail-Joon Ahn. In Proceedings of the 30th Usenix Security Symposium (USENIX 2021), Vancouver, Canada, August 11-13, 2021.

TPS20 *Toward Automated Enforcement of Cyber-Physical Security Requirements for Energy Delivery Systems*. **Carlos E. Rubio-Medrano**, Ziming Zhao and Gail-Joon Ahn. In Proceedings of the IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS), Virtual Event, December 3, 2020.

CCS20 *HoneyPLC: A Next-Generation Honeypot for Industrial Control Systems*. Efrén López Morales, **Carlos E. Rubio-Medrano**, Adam Doupé, Yan Shoshitaishvili, Ruoyu Wang Tiffany Bao and Gail-Joon Ahn. In Proceedings of the ACM Conference on Computer and Communications Security (CCS 2020), Virtual Event, November 9-13, 2020.

SACMAT20 *Proactive Risk Assessment for Preventing Attribute-Forgery Attacks to ABAC Policies*. **Carlos E. Rubio-Medrano**, Luis Claramunt, Shaishavkumar Jogani and Gail-Joon Ahn. In Proceedings of the 25th ACM Symposium on Access Control Models and Technologies (SACMAT), Barcelona, Spain, June 10-12, 2020.

SACMAT19-1 *Effectively Enforcing Authorization Constraints for Emerging Space-Sensitive Technologies*. **Carlos E. Rubio-Medrano**, Shaishavkumar Jogani, Maria Leitner, Ziming Zhao and Gail-Joon Ahn. In Proceedings of the 24th ACM Symposium on Access Control Models and Technologies (SACMAT), Toronto, Canada, June 3-6, 2019.

SACMAT19-2 *Towards Effective Verification of Multi-Model Access Control Properties*. Bernhard J. Berger, Christian Maeder, Rodrigue Wete Nguempnang, Karsten Sohr, and **Carlos E. Rubio-Medrano**. In Proceedings of the 24th ACM Symposium on Access Control Models and Technologies (SACMAT), Toronto, Canada, June 3-6, 2019.

CODASPY19 *Understanding and Detecting Private Interactions in Underground Forums*. Eric Sun, Ziming Zhao, **Carlos E. Rubio-Medrano**, Tiffany Bao and Gail-Joon Ahn In Proceedings of the 9th ACM Conference on Data and Application Security and Privacy (CODASPY 2019), Dallas, Texas, USA, March 25 - 27, 2019.

SGC18 *EDSGuard: Enforcing Network Security Requirements for Energy Delivery Systems*. Vu Coughlin, **Carlos E. Rubio-Medrano**, Ziming Zhao and Gail-Joon Ahn In Proceedings of the IEEE International Conference on Communications, Control and Computing Technologies for Smart Grids (SmartGridComm 2018), Aalborg, Denmark, October 29 - November 1, 2018.

MedSPT18 *The Danger of Missing Instructions: A Systematic Analysis of Security Requirements for MCPS*. Josephine Lamp, **Carlos E. Rubio-Medrano**, Ziming Zhao and Gail-Joon Ahn. In Proceedings of the International Workshop on Security, Privacy, and Trustworthiness in Medical Cyber-Physical Systems (MedSPT), in conjuction with the 3rd International IEEE/ACM Conference on Connected Health: Applications, Systems and Engineering Technologies: CHASE-MedSPT 2018, Washington, DC, USA, September 26-28, 2018.

CIC17 *OntoEDS: Protecting Energy Delivery Systems by Collaboratively Analyzing Security Requirements*. Josephine Lamp, **Carlos E. Rubio-Medrano**, Ziming Zhao and Gail-Joon Ahn. In Proceedings of the 3rd IEEE International Conference on Collaboration and Internet Computing, San Jose, CA, USA, October 15-17, 2017.

SACMAT15 *Federated Access Management for Collaborative Network Environments: Framework and Case Study*. **Carlos E. Rubio-Medrano**, Ziming Zhao, Adam Doupé and Gail-Joon Ahn. In Proceedings of the ACM Symposium on Access Control Models and Technologies (SACMAT), Vienna, Austria, June 1-4, 2015.

CollCom14 *Achieving Security Assurance with Assertion-based Application Construction*.
Carlos E. Rubio-Medrano, Gail-Joon Ahn and Karsten Sohr. In Proceedings of the IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), Miami, FL, USA, October 21-24, 2014.

CollCom13 *Supporting Secure Collaborations with Attribute-based Access Control*.
Carlos E. Rubio-Medrano, Clinton D'Souza and Gail-Joon Ahn. In Proceedings of the IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), Austin, TX, USA, October 20-23, 2013.

COMSPAC13 *Verifying Access Control Properties with Design by Contract*. **Carlos E. Rubio-Medrano**, Gail-Joon Ahn and Karsten Sohr. In Proceedings of the IEEE International Computer Software and Applications Conference (COMPSAC), Kyoto, Japan, July 22-26, 2013.

STPSA10 *Access Control Contracts for Java Program Modules*. **Carlos E. Rubio-Medrano** and Yoonsik Cheon. In Proceedings of the 5th IEEE International Workshop on Security, Trust, and Privacy for Software Applications (STPSA 2010), Seoul, Korea, July 19-23, 2010.

SERP07 *Random Test Data Generation for Java Classes Annotated with JML Specifications*. Yoonsik Cheon and **Carlos E. Rubio-Medrano**. In Proceedings of the 2007 International Conference on Software Engineering Research and Practice, Volume II, pages 385-392 Las Vegas, Nevada, June 25-28, 2007.

Workshop Papers

MSCPES19 *ExSol: Collaboratively Assessing Cybersecurity Risks for Protecting Energy Delivery Systems*. Josephine Lamp, **Carlos E. Rubio-Medrano**, Ziming Zhao and Gail-Joon Ahn. In Proceedings of the 7th IEEE Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES 2019), Montreal, Canada, April 15th, 2019.

ABAC18 *RiskPol: A Risk Assessment Framework for Preventing Attribute-Forgery Attacks to ABAC Policies*. **Carlos E. Rubio-Medrano**, Ziming Zhao and Gail-Joon Ahn In Proceedings of the 3rd ACM Workshop on Attribute-based Access Control (ABAC), in conjuction with CODASPY 2018, Tempe, AZ, USA, March 21, 2018.

MTD17 *Mutated Policies: Towards Proactive Attribute-based Defenses for Access Control*. **Carlos E. Rubio-Medrano**, Josephine Lamp, Adam Doupé, Ziming Zhao and Gail-Joon Ahn. In Proceedings of the 2017 Workshop on Moving Target Defense, in conjuction with CCS 2017, Dallas, TX, USA, October 30, 2017.

MSCPES17 *Towards Adaptive and Proactive Security Assessment for Energy Delivery Systems*. Josephine Lamp, **Carlos E. Rubio-Medrano**, Ziming Zhao and Gail-J. Ahn. In Proceedings of the 2017 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), Pittsburgh, PA, USA, April 21, 2017.

ABAC16 *Towards a Moving Target Defense Approach for Attribute-based Access Control*.
Carlos E. Rubio-Medrano, Josephine Lamp, Marthony Taguinod, Adam Doupé, Ziming Zhao and Gail-J. Ahn. In Proceedings of the 1st Workshop on Attribute-based Access Control (ABAC), New Orleans, LA, USA, March 11, 2016.

WSSA07 *Architectural Assertions: Checking Architectural Constraints at Run-Time*. Hyotaeg Jung, **Carlos E. Rubio-Medrano**, Eric Wong, and Yoonsik Cheon. In Proceedings of the 6th International Workshop on System and Software Architectures, Published in Proceedings of SERP 2007, Volume II, pages 604-607. Las Vegas, Nevada, June 25-28, 2007.

Journal Papers

ISFJ22 *DyPolDroid: Protecting Against Permission-Abuse Attacks in Android (Extended Version)*. **Carlos E. Rubio-Medrano**, Pradeep Kumar Duraisamy Soundrapandian, Matthew Hill, Luis Claramunt, Jaejong Baek, Geetha S, and Gail-Joon Ahn. Information Systems Frontiers Journal, Special Issue on Secure Knowledge Management in the Age of Artificial Intelligence. February, 2022.

DTRAP21 *ExSol: Collaboratively Assessing Cybersecurity Risks for Protecting Energy Delivery Systems*. Josephine Lamp, **Carlos E. Rubio-Medrano**, Ziming Zhao and Gail-Joon Ahn. ACM Digital Threats: Research and Practice, January, 2021.

EAI14 *Achieving Security Assurance with Assertion-based Application Construction (Extended Version)*. **Carlos E. Rubio-Medrano**, Gail-J. Ahn and Karsten Sohr. EAI Endorsed Transactions on Collaborative Computing, Special Issue of TrustCol 2014, European Alliance for Innovation, September 2015.

AISCS07 *A Formal Specification in JML of the Java Security Package*.
Poonam Agarwal, **Carlos E. Rubio-Medrano**, Yoonsik Cheon, and Patricia J. Teller. Proceedings of the Journal on Advances and Innovations in Systems, Computing Science, and Software Engineering, Pages 363-368, Springer, 2007.

Book Chapters

BOOK22 *HoneyPLC: A Next-Generation Honeypot for Industrial Control Systems (Extended Version)*. Efrén López Morales, **Carlos E. Rubio-Medrano**, Adam Doupé, Yan Shoshitaishvili, Ruoyu Wang Tiffany Bao and Gail-Joon Ahn. Book Chapter. *Cyber Deception: Techniques, Strategies, and Human Aspects*, Springer, September, 2022.

Conference Poster Papers

EUROSP21-1 *Preventing Spatial and Privacy Attacks in Mobile Augmented Reality Technologies*. Luis Claramunt, Larissa Pokam-Epse, **Carlos E. Rubio-Medrano**, Jaejong Baek and Gail-Joon Ahn. In Proceedings of the 6th IEEE European Symposium on Security and Privacy (IEEE Euro S&P), September 6-10, 2021.

EUROSP21-2 *DyPolDroid: User-Centered Counter-Policies Against Android Permission-Abuse Attacks*. Matthew Hill, **Carlos E. Rubio-Medrano**, Luis Claramunt, Jaejong Baek and Gail-Joon Ahn. In Proceedings of the 6th IEEE European Symposium on Security and Privacy (IEEE Euro S&P), September 6-10, 2021.

TEACHING EXPERIENCE

- *COSC 4310: Digital Forensics*,
  Texas A&M University - Corpus Christi, Spring 2022
- *COSC 6370: Advanced Software Engineering*,
  Texas A&M University - Corpus Christi, Spring 2022, Fall 2022, Spring 2023
- *COSC 6379: Advanced Information Assurance*,
  Texas A&M University - Corpus Christi, Fall 2021
- *COSC 6374: Computer Forensics*,
  Texas A&M University - Corpus Christi, Spring 2021, Spring 2023
- *COSC 4342: Computer Networks*,
  Texas A&M University - Corpus Christi, Fall 2020
- *CSE 365/465: Introduction to Information Assurance*,
  Arizona State University Spring 2018, Spring 2019
- *CSE 110: Introduction to Computer Programming with Java*,
  Arizona State University Fall 2013, Spring 2014, Fall 2014

STUDENT MENTORING

Doctoral Students (Active)

- Efrén López Morales (Hispanics).
  Texas A&M University - Corpus Christi. SAGE Scholarship Recipient. CONACyT Scholarship Recipient.
  Research Topics: Cybersecurity, Cyber-Physical Systems.
  Expected Graduation: May 2025

- Jacob Hopkins.
  Texas A&M University - Corpus Christi. SAGE Scholarship Recipient.
  Research Topics: Cybersecurity, Authorization and Access Control.
  Expected Graduation: December 2026

- Ahmed Saad.
  Texas A&M University - Corpus Christi.
  Research Topics: Cybersecurity, Unmanned Aerial Vehicles (UAVs).
  Expected Graduation: December 2026

Masters Students (Graduated)

- Luis Claramunt (Hispanics).
  SpaceMediator: Preventing Spatial and Privacy Attacks in Mobile Augmented Reality
  MS Thesis Completed. Arizona State University. March 2022
  Current Position: Software Engineer. Intel Inc. Chandler, AZ.

- Efrén López Morales (Hispanics).
  HoneyPLC: A Next Generation Honeypot for Industrial Control Systems.
  MS Thesis Completed. Arizona State University. May 2020

- Vu Coughlin.
  MCS Degree Completed. Arizona State University. December 2018
  Current Position: Cybersecurity Analyst. Mitsubishi Bank of America.

Masters Students (Active)

- Laila Romero (Female, Hispanics).
  Texas A&M University - Corpus Christi.
  Research Topics: Cybersecurity, Artificial Intelligence, Neural Networks.
  Expected Graduation: May 2023

- Akash Kotak.
  Texas A&M University - Corpus Christi.
  Research Topics: Cybersecurity, Formal Specifications, AI Chatbots.
  Expected Graduation: May 2024

Undergraduate Students (Graduated)

- Josephine Lamp (Female).
  Ardent Health Aegis: Security Analysis and Monitoring for Medical Cyber-Physical Systems.
  BS Honors Thesis Completed. Arizona State University. March 2017
  Current Position: PhD Student. University of Virginia. Jefferson Scholarship Recipient.

- Matthew Hill.
  BS Degree Completed. Arizona State University. May 2020
  Research Topics: Cybersecurity, Android Malware Detection. Android Enterprise.
  Current Position: DevOps Engineer Cycorp Inc.

- Larissa Pokam Epse (Female). BS Degree. Arizona State University. December 2020
  Research Topics: Cybersecurity. Mobile Augmented Reality.
  Current Position: Software Engineer. Tata Consultancy Services Ltd.

PROFESSIONAL SERVICE

Invited Talks

- *Why Choosing Computer Science at Texas A&M University-Corpus Christi?*
  TAMU-CC *IslandDay* Recruitment Fair, March, 2021, February 2022, October 2022 , February 2023
- *Circles of Trust: A Voice-based Authorization Scheme for Securing IoT Smart Homes*
  XVIII Semana de Ingeniería de la Universidad de Sonora, October 2021
- *Choosing a Career Pathway* Discussion Panel
  Arizona State University Postdoc Career Conference, March, 2021
- *Cybersecurity Perspectives on Mobile Augmented Reality: The Coolest Emerging Technology Just Around the Corner*,
  QUANTUM-CIMAT-Zacatecas Seminar Session, November, 2020
- *Mentoring a Hispanic Student for a Successful Masters Thesis and a Top-Conference Research Paper in the Middle of a Pandemic*,
  CAHSI Southwest Regional Meeting, November, 2020
- *Mentoring a Hispanic Student for a Successful Masters Thesis and a Top-Conference Research Paper in the Middle of a Pandemic*,
  2020 Building HSI Learning Resilience in the Face of Crises Conference, November, 2020

Student Competitions

- *CAHSI Cybersecurity Hackathon*
  Texas A&M University - Corpus Christi, April, 2021, October 2021, April 2022, December 2022

Service Committees

- Faculty Search Committee,
  Department of Computer Sciences, Texas A&M University - Corpus Christi, 2020-2021, 2021-2022, 2022-2023
- Director Search Committee,
  Conrad Blutcher Institute for Surveying and Science, Texas A&M University - Corpus Christi, 2021-2022
- Dean of the College of Engineering Search Committee,
  Texas A&M University - Corpus Christi, 2022
- Diversity Hiring Committee,
  College of Science and Engineering, Texas A&M University - Corpus Christi, 2022
- Wes Tunnell Distinguished Speaker Series Committee,
  College of Science and Engineering, Texas A&M University - Corpus Christi, 2021-2022
- Academic Appeals Committee,
  Texas A&M University - Corpus Christi, 2022-2023

Conference Reviewer

- ACM Conference on Computer and Communications Security (CCS), 2017, 2018
- IEEE Symposium on Security and Privacy (S&P), 2016
- ACM Symposium on Access Control Models and Technologies (SACMAT), 2014, 2015, 2018
- ACM Conference on Data and Application Security and Privacy (CODASPY), 2014-2019

- European Symposium on Research in Computer Security (ESORICS), 2018
- ACM Symposium on Information, Computer and Communications Security (ASIACCS), 2014, 2017
- IEEE Transactions on Dependable and Secure Computing (TDSC), 2019

Conference Organizing Committee

- IEEE European Security and Privacy Conference (EURO S&P), 2021
- ACM Conference on Data and Applications Security and Privacy (CODASPY), 2018

Session Chair

- ACM Conference on Data and Applications Security and Privacy (CODASPY), 2018

SCHOLARSHIPS AND AWARDS

- *Summer Grant Fellows Award* April 2022
  Presented by the Division of Research & Innovation of Texas A&M University - Corpus Christi.
- *Outstanding Masters Thesis Award* May 2008
  Presented by the College of Engineering of The University of Texas at El Paso.
- *Bachelors Degree Conferment Distinction* February 2005
  Presented by the Instituto Tecnológico de Chihuahua II
- *Foreign Studies Scholarship* July 2008
  Awarded by the Mexican Consejo Nacional de Ciencia y Tecnologia (CONACyT).
- *UTEP-Chihuahua State Government Scholarship* October 2005
  Presented by the Chihuahua State Government and The University of Texas at El Paso.

MISCELLANEOUS

- U.S. Lawful Permanent Resident (Green Card Holder).

Last Update: February 8, 2023.