Carlos E. Rubio-Medrano, Ph.D.

carlos.rubiomedrano@tamucc.edu, crubiome@asu.edu

https://carlosrubiomedrano.com

Last Update: May 29, 2026

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.

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 such as Research Cyberinfrastructures, Energy Delivery Systems, and Unmanned Aerial Vehicles (UAVs), a.k.a., *drones*.

My research work has led to 50+ publications in prestigious venues including the ACM Conference in Computer and Communications Security (**ACM CCS**), the USENIX Security Symposium (**USENIX Security**), the IEEE Security & Privacy Symposium (**IEEE S&P**), the Network and Distributed Systems Symposium (**NDSS**), the ACM Symposium on Access Control Models and Technologies (**SACMAT**), the ACM Conference on Data and Applications Security and Privacy (**CODASPY**), and others.

A list of successful projects I have led include:

- *Cybersecurity Monitoring and Assessment*: a systematization of knowledge on Programmable Logic Controllers [USENIX24], 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 study on the peer review process of research papers in the security community [S&P22], and a full-fledged honeypot framework for satellites [NDSS26].
- *Authorization and Access Control*: a study on the management of resource-sharing privileges within Research Cyber-infrastructures [S&P25], an analysis of how academia and industry professionals understand and enforce Zero Trust paradigms [CCS26], an exploration of the security and human factors on emerging AI technologies for access control [SACMAT26], and novel approaches for enforcing authorization constraints for augmented reality [SACMAT19-1, SACMAT23]; handling authorization policies for federated organizations [PhDDiss, SACMAT15]; and, risk assessment and modification of authorization policies [SACMAT20, ABAC18, MTD17].
- *Software Specification, Verification and Validation*: correctly enforcing authorization constraints using emerging AI techniques [SACMAT24-1], modeling multi-model authorization constraints in production software [SACMAT19-2], verifying access control models at the source code level [COMSPAC13, EAI14], enforcing access control contract in Java modules [STPSA10, MSThesis].

RESEARCH FUNDING

CAHSI23 *CAHSI-Google Institutional Research Program*.
Awarded by Google and the Computing Alliance of Hispanic-Serving Institutions (CAHSI).
Carlos E. Rubio-Medrano (PI), Dvijesh Shastri (Co-PI)
Consoria Members: Texas A&M University - Corpus Christi, University of Houston - Downtown.
Site: $50,000.00. Consortia: $80,000.00.
August 2023 - July 2024.

TARC23 *TARC Pitch Award*.
Awarded by the Texas A&M Engineering Experiment Station (TEES) Annual Research Conference 2023.
Mehdi Sookhak (PI), **Carlos E. Rubio-Medrano (Co-PI)**.
Consortia Members: Texas A&M University - Corpus Christi, Texas A&M University - Commerce and Texas A&M University - Kingsville, **Consortia: $2,500.00**.
August 2023 - August 2024.

DOT23 *CYBER-CARE: Transportation Cybersecurity Center for Advanced Research and Education*.
Carlos E. Rubio-Medrano (Co-PI)
US Department of Transportation. Consortia Members: University of Houston (Lead), Embry-Riddle Aeronautical University, Rice University, Texas A&M University-Corpus Christi, University of Cincinnati, University of Hawaii, Honolulu.
Site: $1,300,000.00, **Consortia: $10,000,000.00**
August 2023 - July 2028.

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

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.

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, Chen Pan.
National Science Foundation. Major Research Instrumentation Program.
Award No. 2216335. $1,166,605.00.
October 2022 - September 2025.

PUBLICATIONS

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.

Full Conference Papers

CCS26 *Beyond the Buzzword: How do Professionals Understand and Translate Zero Trust?*. Ananta Soneji, Souradip Nath, Moritz Schloegel, Yan Shoshitaishvili, Gail-Joon Ahn, Adam Doupé, and **Carlos E. Rubio-Medrano**. In Proceedings of the ACM Conference on Computer and Communications Security (CCS 2026), The Hague, The Netherlands, November 15-19, 2026.

SACMAT26 *Towards Agentic AI for Access Control in Cyber-infrastructures: Exploring the Security and Human Factors [BlueSky Paper]*. **Carlos E. Rubio-Medrano**, Souradip Nath, Ananta Soneji, Jennifer Mondragon, Jaejong Baek, and Gail-Joon Ahn. In Proceedings of the 31st ACM Symposium on Access Control Models and Technologies (SACMAT'26), Ontario, Canada, July 8-10, 2026.

NDSS26 *HoneySat: A Network-based Satellite Honeypot Framework*. Efrén López-Morales, Ulysse Planta, Gabriele Marra, Carlos González, Jacob Hopkins, Majid Garoosi, Elías Obreque, **Carlos E. Rubio-Medrano** and Ali Abbasi. In Proceedings of the Network and Distributed System Security (NDSS) Symposium 2026. San Diego, CA, USA, February 23-27, 2026.

CIC25 *Towards Collaboration-Aware Resource Sharing in Research Computing Infrastructures*. Souradip Nath, Ananta Sojeni, Jaejong Baek, **Carlos E. Rubio-Medrano**, and Gail-Joon

Ahn. In Proceedings of the 10th IEEE International Conference on Collaboration and Internet Computing (CIC 2025). Pittsburgh, PA, USA, November 11-14, 2025.

S&P25 *"It's almost like Frankenstein": Investigating the Complexities of Scientific Collaboration and Privilege Management within Research Computing Infrastructures*. Souradip Nath, Ananta Sojeni, Adam Doupé, Tiffany Bao, **Carlos E. Rubio-Medrano**, and Gail-Joon Ahn. In Proceedings of the IEEE Symposium on Security and Privacy (IEEE S&P 2025). San Francisco, CA, USA, May 12-15, 2025.

USENIX24 *SoK: Security of Programmable Logic Controllers*. Efrén López Morales, **Carlos E. Rubio-Medrano**, Álvaro Cárdenas, and Ali Abbasi. In Proceedings of the 33rd Usenix Security Symposium (USENIX 2024), Philadelphia, PA, USA, August 14-16, 2024.

ICSOFT-24 *Asserting Frame Properties*. Yoonsik Cheon, Bozhen Liu, and **Carlos E. Rubio-Medrano**. In Proceedings of the 19th International Conference on Software Technologies (ICSOFT), SciTePress, Pages 145-152, Dijon, France, July 2024.

SACMAT24-1 *Pairing Human and Artificial Intelligence: Enforcing Access Control Policies with LLMs and Formal Specifications*. **Carlos E. Rubio-Medrano**, Akash Kotak, Wenlu Wang, and Karsten Sohr. In Proceedings of the 29th ACM Symposium on Access Control Models and Technologies (SACMAT'24), San Antonio, Texas, USA May 15-17, 2024.

SACMAT23 *SpaceMediator: Leveraging Authorization Policies to Prevent Spatial and Privacy Attacks in Mobile Augmented Reality*. Luis Claramunt, **Carlos E. Rubio-Medrano**, Jaejong Baek, and Gail-Joon Ahn. In Proceedings of the 28th ACM Symposium on Access Control Models and Technologies (SACMAT'23), Trento, Italy, June 7-9, 2023.

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, CA, 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, TX, 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 and Work In Progress Papers

AIRET-25 *Beyond the Chatbox: An Exploratory Case Study of Autonomous Computer-Use Agents*. Malak Mahdy and **Carlos E. Rubio-Medrano**. In Proceedings of the First International Workshop on Agentic Intelligence: Risks, Ethics, and Trust (AIRET), co-located with the International Conference on Computational Intelligence in Cybersecurity, Trust, Privacy, and Security in Intelligent Systems and Applications, and Cognitive Machine Intelligence (IEEE CIC/ TPS/ CogMI 2025), Pittsburgh, PA, November 11-14, 2025.

HAIPS-25 *"I Apologize For Not Understanding Your Policy": Exploring the Specification and Evaluation of Security Authorization Policies by AI-Based Virtual Assistants*. Jennifer Mondragon, Gael Cruz, Dvijesh Shastri and **Carlos E. Rubio-Medrano**. In Proceedings of the ACM Workshop on Human-Centered AI Privacy and Security (HAIPS 2025), in conjunction with the ACM Conference on Computer and Communications Security (ACM CCS 2025), Taipei, Taiwan, October 7, 2025.

SaT-CPS-25 *PendingMutent: An Authorization Framework for Preventing PendingIntent Attacks in Android-based Mobile Cyber-Physical Systems*. Pradeepkumar D S, **Carlos E. Rubio-Medrano**, Jaejong Baek and Geetha S. In Proceedings of the ACM Workshop on Secure and Trustworthy Cyber-Physical Systems (SaT-CPS 2025), organized in conjunction with the 15th ACM Conference on Data and Application Security and Privacy (CODASPY 2025). Pittsburgh, PA, June 4-6, 2025.

USEC-25 *Vision: The Price Should Be Right: Exploring User Perspectives on Data Sharing Negotiations*. Jacob Hopkins, **Carlos E. Rubio-Medrano**, and Cori Faklaris. In Proceedings of the Symposium on Usable Security and Privacy (USEC) 2025, co-organized with the Network and Distributed System Security (NDSS) Symposium 2025. San Diego, CA, USA, February 26, 2025.

BIGDATA-24 *Fly-ABAC: Attribute Based Access Control for the Navigation of Unmanned Aerial Vehicles*. Wynter Japp, Victoria Lee, Sai Avinash Vagicherla, and **Carlos E. Rubio-Medrano**. In Proceedings of the Symposium for Undergraduate Research in Data Science, Systems, and Security (REU Symposium 2024) collocated at the IEEE BigData 2024 Conference, Washington, DC, USA, December 15, 2024.

RICSS-24 *By the Numbers: Towards Standard Evaluation Metrics for Programmable Logic Controllers' Defenses*. Efrén López Morales, Jacob Hopkins, Alvaro A. Cardenas, Ali Abbasi, and **Carlos E. Rubio-Medrano**. In Proceedings of the 2024 Workshop on Re-design Industrial Control Systems with Security (RICSS'24), Salt Lake City, UT, USA, October 14-18, 2024.
Best Presentation Award.

CPSIoTSec-24 *ICSNet: A Hybrid-Interaction Honeynet for Industrial Control Systems*. Luis Salazar, Efrén López Morales, Juan Lozano, **Carlos E. Rubio-Medrano**, and Alvaro Cardenas In Proceedings of the 6th Workshop on CPS and IoT Security (CPSIoTSec 2024), co-located with the ACM Conference on Computer and Communications Security (CCS 2024), Salt Lake City, UT, October 14-18, 2024.
Best Paper Award.

SACMAT24-2 *SecureCheck: User-Centric and Geolocation-Aware Access Mediation Contracts for Sharing Private Data*. Jacob Hopkins and **Carlos E. Rubio-Medrano**. In Proceedings of the 29th ACM Symposium on Access Control Models and Technologies (SACMAT'24), San Antonio, Texas, USA May 15-17, 2024.

MOBIHOC-23 *No-Fly-Zone: Regulating Drone Fly-Overs Via Government and User-Controlled Authorization Zones*. Abdullah Kamal, Jeremy Vidaurri, and **Carlos E. Rubio-Medrano**. In Proceedings Twenty-fourth International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing (MobiHoc '23), Washington, DC, USA October 23-26, 2023.

MOBIHOC-23-P *Poster: No Fly-Zone: Drone Policies for Ensuring Safe Operations in Restricted Areas.* Arturo Gonzalez, Amani Davidson, and **Carlos E. Rubio-Medrano**. In Proceedings of the Twenty-fourth International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing (MobiHoc '23). Washington, DC, USA October 23-26, 2023.

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 and Magazine Papers

Access25 *POF+MADER: Trajectory Planner in Dynamic Environments With Improved Collision Avoidance*. Syed Izzat Ullah, Jose Baca, Pablo Rangel, Tianxing Chu and **Carlos E. Rubio-Medrano**. In IEEE Access, vol. 13, pp. 215533-215549, December 2025,

CACAIE-24 *Aeroelastic force prediction via temporal fusion transformers*. Miguel Cid Montoya, Ashutosh Mishra, Sumit Verma, Omar A. Mures, and **Carlos E. Rubio-Medrano**. Computer-Aided Civil and Infrastructure Engineering (CACAIE), Volume 39, Issue 24, December 2024.
Journal Cover Selection.

JWEIA24 *On the Cybersecurity of Smart Structures under Wind*. Miguel Cid Montoya, **Carlos E. Rubio-Medrano**, Ahsan Kareem. Journal of Wind Engineering & Industrial Aerodynamics, January 2024.

JSTAEORS24 *Ultra-fusion: optimal fuzzy fusion in land-cover segmentation using multiple panchromatic*. Hadi Mahdipour, Alireza Sharifi, Mehdi Sookhak, and **Carlos E. Rubio-Medrano**. IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, satellite images, Pages 1-12, 2024.

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

SACMAT24-3 *Circles of Trust: A Voice-Based Authorization Scheme for Securing IoT Smart Homes*. Jennifer Mondragon, Gael Cruz, Dvijesh Shastri, and **Carlos E. Rubio-Medrano**. In Proceedings of the 29th ACM Symposium on Access Control Models and Technologies (SACMAT'24), San Antonio, Texas, USA May 15-17, 2024.

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.

Conference and Student Abstract Papers

AAAI26 *Towards Capable and Secure Autonomous Computer-Use Agents*. Malak Mahdy and **Carlos E. Rubio-Medrano**. In Proceedings of the 40th Annual AAAI Conference on Artificial Intelligence, Singapore, January 20-27, 2026.

ICWE23 *A First Look at Cybersecurity of Structures Under Wind*. Miguel Cid Montoya, **Carlos E. Rubio-Medrano**, and Ahsan Kareem. In Proceedings of the 16th International Conference on Wind Engineering (16ICWE), Florence, Italy, August 27-31, 2023.

TEACHING EXPERIENCE

- *COSC 6376: Network Security*,
  Texas A&M University - Corpus Christi, Spring 2024, Spring 2025
- *COSC 4310: Digital Forensics*,
  Texas A&M University - Corpus Christi, Spring 2022, Spring 2024
- *COSC 6370: Advanced Software Engineering*,
  Texas A&M University - Corpus Christi, Spring 2022, Fall 2022, Spring 2023, Spring 2025, Fall 2025, Spring 2026

- *COSC 6379: Advanced Information Assurance*,
  Texas A&M University - Corpus Christi, Fall 2021, Fall 2026
- *COSC 6374: Computer Forensics*,
  Texas A&M University - Corpus Christi, Spring 2021, Spring 2023, Fall 2024, Fall 2025
- *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 (Graduated)

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

Doctoral Students (Active)

- Jacob Hopkins.
  Texas A&M University - Corpus Christi. SAGE Scholarship Recipient.
  Research Topics: Cybersecurity, Privacy Enhancing Tools.
  Expected Graduation: December 2026
- Jennifer Mondragon (Female, Hispanics).
  Texas A&M University - Corpus Christi.
  Research Topics: Cybersecurity, Smart Homes, Voice Assistants.
  Expected Graduation: December 2027
- Souradip Nath.
  Arizona State University.
  Co-advised with Dr. Gail-Joon Ahn.
  Research Topics: Cybersecurity, Access Control, Resource-Sharing Cyberinfrastructures.
  Expected Graduation: December 2027
- Lewis Heuermann.
  Texas A&M University - Corpus Christi.
  Research Topics: Cybersecurity, Access Control, Zero-Trust.
  Expected Graduation: December 2030

Masters Students (Graduated)

- Ashutosh Mishra.
  MS Computer Science Completed. Texas A&M University - Corpus Christi. May 2024
  Co-advised with Dr. Miguel Cid Montoya.
  Research Topics: Machine Learning, Modeling of Civil Structures.
- Akash Kotak.
  MS Computer Science Completed. Texas A&M University - Corpus Christi. May 2024
  Research Topics: Cybersecurity, Formal Specifications, AI Chatbots.
  Current Position: Founder. TinkerTechLogix, Mumbai, India.

- Laila Romero (Female, Hispanics).
  SecureNN: Defeating Adversarial Attacks with Moving Target Defense and Genetic Algorithms
  MS Thesis Completed. Texas A&M University - Corpus Christi. May 2023
  Current Position: Machine Learning Scientist. Northrop - Grumman Inc.

- 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
  Current Position: Assistant Professor. New Mexico State University.

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

Undergraduate Students

- 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.

STUDENT ACHIEVEMENTS

- Efrén López Morales.

  -Dagstuhl Seminar: Guardians of the Galaxy: Protecting Space Systems from Cyber Threats.
  Schloss Dagstuhl, Germany Spring 2025

  -Rising Star in CPS.
  Cyber Physical Systems Virtual Organization /National Science Foundation. Spring 2025

  -Outstanding Graduate Scholar.
  Computing Alliance of Hispanic Serving Institutions. Fall 2024

  -Second Place. 3 Minute Thesis (3MI) Competition.
  Texas A&M University - Corpus Christi. Spring 2024

-First Place. 3 Minute Thesis (3MI) Competition.
Texas A&M University - Corpus Christi. Spring 2022

-First Place. Graduate Poster Competition.
Great Minds in STEM National Conference. Spring 2021

- Jennifer Mondragon.
-Second Place. Short Oral Research Competition.
MSGSO Student Research Symposium. Texas A&M University - Corpus Christi. Fall 2023

- Jacob Hopkins.
-First Place. Science and Technology Research Presentation.
TAMUS Doctoral Pathways Symposium. Spring 2023

PROFESSIONAL SERVICE

Invited Talks

- *Artificial Intelligence for Secure Computer Programming*
U.S. Embassy in Tunisia, October 2024
- *Towards Effectively Teaching and Practicing Cybersecurity-By-Design Approaches for Future Transportation Systems*
AI and Emerging Technologies for Integrated Transportation Cybersecurity Workshop, co-located with the ASCE International Conference in Transportation & Development June 2024
- *Get That Drone Away From my Head: Restricting Drone Flyovers for Sensitive Physical Locations*
Society for Industrial and Applied Mathematics at Texas State University, April 2024
- *Pairing Human and Artificial Intelligence: Enforcing Security Policies with LLMs and Formal Specifications*
NSF Workshop: Understanding Cyber Victimization Risks in Job Searching in the Hybrid World, April 2024
- *Artificial Intelligence for Secure Computer Programming*
Texas A&M University - Corpus Christi President's Circle Lunch and Learn, February 2024
- *Writing a Successful CISE-MSI Proposal*
NSF Southwest CISE Research Expansion Aspiring Investigators Conference, December 2023
- *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, October 2022
- *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

Outreach Events

- *Stop, Hack, Go! - Cybersecurity and AI Workshop*
  Kaffie Middle School, Corpus Christi, TX — April 2025, October 2025
- *Science Spectacular - Drone Showcase*
  Mireles Elementary School, Ella Barnes Elementary School, Corpus Christi, TX — March 2025

Student Competitions

- *IslanderHack Hackathon*
  Texas A&M University - Corpus Christi, — November 2025
- *Stop, Hack, Go! - Cybersecurity and AI Workshop*
  Texas A&M University - Corpus Christi, — October 2025
- *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, 2023-2024
- Graduate Curricula Studies Committee,
  Department of Computer Sciences, Texas A&M University - Corpus Christi, 2022-2023, 2023-2024
- 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
- IT Manager Search Committee,
  College of Engineering and Computer Science, Texas A&M University - Corpus Christi, 2022-2023
- Digital Learning & Instructional Technology (DLIT) Committee,
  Texas A&M University - Corpus Christi, 2023

Research Article Reviewer

- ACM Symposium on Information, Computer and Communications Security (ASIACCS), 2014, 2017, 2024
- Annual Computer Security Applications Conference (ACSAC), 2025
- IEEE Transactions on Dependable and Secure Computing (TDSC), 2019, 2024
- ACM Conference on Data and Application Security and Privacy (CODASPY), 2014-2019, 2025

- 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, 2025
- European Symposium on Research in Computer Security (ESORICS), 2018

Conference Organizing Committee

- ACM Symposium on Access Control Models and Technologies (SACMAT), 2025
- 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

- *Google-CAHSI Cybersecurity Fellow Award* November 2024
  Presented by Computing Alliance of Hispanic Serving Institutions (CAHSI) alongside with Google Inc.
- *Best Paper Award. ICSNet: A Hybrid-Interaction Honeynet for Industrial Control Systems* October 2024
  Presented by the 6th Workshop on CPS and IoT Security (CPSIoTSec 2024), co-located with the ACM Conference on Computer and Communications Security (CCS 2024).
- *Best Presentation Award. By the Numbers: Towards Standard Evaluation Metrics for Programmable Logic Controllers' Defenses* October 2024
  Presented by the 2024 Workshop on Re-design Industrial Control Systems with Security (RICSS'24), co-located with the ACM Conference on Computer and Communications Security (CCS 2024).
- *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, Unrestricted) October 2022