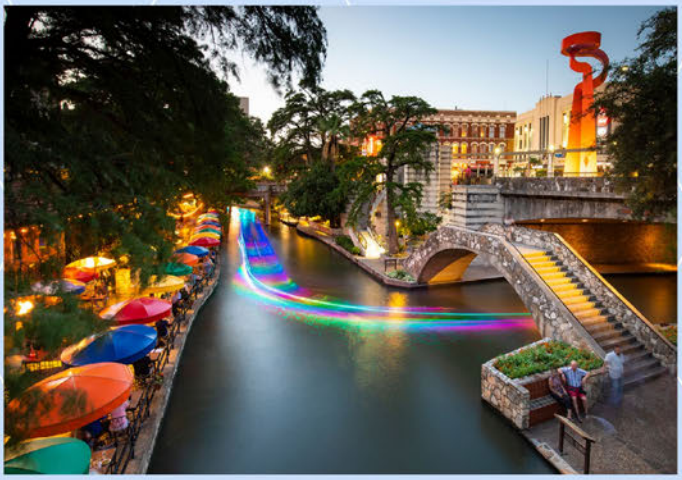
2025 ICCST

International Carnahan Conference on Security Technology

October 14-17 • San Antonio, Texas

2025 ICCST CONFERENCE BROCHURE



San Antonio, Texas is a world-renowned tourist destination, famous for its colonial Spanish missions and its Riverwalk. San Antonio is the largest cybersecurity hub in the U.S. outside of Washington D.C.

The conference will be held at the UT San Antonio San Pedro I building in downtown San Antonio, Texas. This facility houses both the College of AI, Cyber, and Computing and the National Security Collaboration Center.

PRINCIPAL SPONSORS

AESS

IEEE Advancing Technology for Humanity

LONE STAR SECTION

ICCST2025 WEB LINK

TABLE OF CONTENTS

Welcome Message from the Program Chair

On behalf of the organizing committee, it is my privilege to welcome you to the 57th IEEE ICCST in San Antonio, Texas. San Antonio is the largest cybersecurity hub in the U.S. outside of Washington D.C. and will be the home of the newly established Texas Cyber Command. San Antonio's cybersecurity ecosystem includes a diverse range of players, from major defense contractors to numerous locally head¬quartered firms. We are thrilled to have you join us for this prestigious event, where we will explore the latest technological developments and innovations in the field of advanced security technologies including physical, cyber, and electronic security research, development, systems engineering, testing, evaluation, case studies and new research lines to face current and future challenges.

Over the course of the three-day program, we will explore the latest security technology innovations through the lenses of 47 original research papers, tutorials, and presentations from authors and keynote speakers.

This year, we have curated a program that includes:

- Keynote Addresses: Academia and industry speakers with depth and breadth expertise in various security technologies ranging from biometrics, aviation security along with the use of quantum techniques and AI.
- Technical Sessions: Dive deep into original research to be presented by each of the authors.
- Networking Opportunities: Connect with fellow participants, industry representatives, and potential collaborators at the Young Professional, Women-in-Engineering, Exhibitor Reception.
- Exhibitors: Discover the latest products and solutions from the leading companies in the security technology sector.

In addition to the formal program, few destinations provide a sense of place like San Antonio. We encourage you to take full advantage of the downtown amenities located within walking distance from the conference facility located at the National Security Collaboration Center (NSCC) on the downtown campus of the University of Texas San Antonio. Please take a moment to review the Conference Brochure for detailed information about the schedule and speakers to make the most out of your 2025 ICCST experience.

Christoph E. Carnahan

2025 ICCST – Conference Chair

Welcome Message from the Technical Program Chair

Dear Friends,

As Chairman of the conference Technical Committee and of the Executive Committee of the IEEE International Carnahan Conference on Security Technology (IEEE ICCST), I welcome you to the University of Texas at San Antonio in the vibrant, historical and spectacular city of San Antonio, Texas, USA. This is the 57th IEEE ICCST, which is one of the most famous and longest running international conferences in the world. This conference proves to be truly international, representing Government, Academia and Industry, with 51 orally presented papers, along with 15 invited speakers who will give keynote addresses and deliver a series of tutorials on a range of contemporary topics in security technology. The spoken presentations are organized into a single thread of 11 sessions covering selected conference topics of wide general interest including biometrics, aviation security, threat detection, information security, cyber security and the application of quantum techniques and AI. We are also running a sponsor programme in which contributors will show exhibitions of their work and products, which we hope you will visit.

We offer a special welcome to the scientists, engineers and security practitioners who are attending the ICCST for the very first time. We would also take this opportunity to acknowledge the IEEE/AESS which has provided financial support for the conference, and to express our gratitude to all of those who have made this conference possible. This starts with you as honoured delegates, distinguished authors, invited speakers, our ICCST Executive Committee, the Technical Committee and finally, our ICCST 2025 Organising Committee, led by Chris Camargo, which includes Joan Labay-Marquez, Chyna Lane, Michelle Valero, John Huggins, Victor Murray, Werner Osorio, Abhilash Trehan, and Walt Downing. In addition to our technical program, we have suggested a social program for delegates and accompanying persons to explore the culture, sights and sounds of the exciting and dynamic city of San Antonio.

Again, I would like to express my sincere thanks to you all for taking the time to attend the conference this year. We involved in organising the event further hope that your time here will be enjoyable through participating in discussion, presenting your work and achievements, taking away of valued information, the making of lasting contacts and new friendships and, finally, departing with fond memories of San Antonio.

Gordon L. Thomas
Chair of Technical Committee
www.gordonlthomas.com

Welcome Message from the IEEE Lone Star Section Chair

On behalf of the IEEE Lone Star Section, I am pleased to welcome you to the 2025 IEEE International Carnahan Conference on Security Technology in San Antonio, Texas. The Lone Star Section is proud to be a co-sponsor of this conference and glad that you have come to participate. We hope that you find the conference interesting and informative, and that you also have a good time while you are in our city. There are many things to do and places to enjoy in and around San Antonio. If you need guidance or suggestions about local attractions, events, entertainment, dining, or other activities, just ask a member of the conference committee. They would be happy to help.

This year's conference is being held in the National Security Collaboration Center (NSCC) on the downtown campus of the University of Texas San Antonio. NSCC is a purpose-built facility that fosters public-private partnerships by facilitating events such as this conference. It is a great venue to convene government, industry, academia, and other stakeholders to present and discuss the latest scientific discoveries and technological developments in security technology to address the challenges posed by modern threats. The conference committee wishes to express our appreciation to UT San Antonio for making this venue available to us.

I would also like to thank the IEEE Aerospace and Electronic Systems Society (AESS) for allowing the Lone Star Section to be a financial co-sponsor of this conference. The Lone Star Section joint chapter of AESS appreciates the opportunity to raise funds in support of local activities that build engagement among the technical community. Hosting a technical conference is a challenging but invigorating experience. Our committee has worked hard to make this conference successful technically and financially. We learned a lot and have grown together as a team. I am very proud of them and thank them for their dedication and service.

Welcome Message from the Treasurer

Dear Attendees and Sponsors,

On behalf of the organizing committee, it is my sincere pleasure to welcome you to the 2025 IEEE International Carnahan Conference on Security Technology (ICCST), being held this year in the vibrant city of San Antonio, Texas.

As the Treasurer of this year's conference, I want to extend my heartfelt thanks to all of you who have registered and made the commitment to join us—whether you are presenting, attending sessions, supporting the event as a sponsor, or contributing in other important ways. Your participation is what makes the ICCST such a valuable gathering each year.

The ICCST continues to serve as a premier international forum for the exchange of ideas, research findings, and practical solutions in the field of security technology. We are proud to carry forward this tradition with a strong program featuring a diverse range of presentations, panel discussions, and keynote addresses from thought leaders and innovators across academia, industry, and government.

I hope that this year's conference not only enriches your understanding of the evolving security landscape, but also inspires meaningful dialogue, collaboration, and professional growth. Whether you are a first-time attendee or a returning participant, I encourage you to take full advantage of the learning opportunities, networking events, and technical sessions designed to foster exchange and advancement in our field.

To our sponsors, thank you for your generous support and commitment to the advancement of security technology. Your partnership plays a crucial role in the continued success of this conference.
Once again, welcome to the 2025 IEEE ICCST. I look forward to the insightful conversations and connections that will emerge from our time together in San Antonio.

Warm regards,

Werner Osorio
Treasurer, 2025 IEEE International Carnahan Conference on Security Technology

Welcome Message from the Tutorials Chair

Dear Attendees, Sponsors, and Distinguished Guests,

On behalf of the conference committee, we welcome you to the 57th International Carnahan Conference on Security Technology (ICCST 2025), held this year in Cyber City USA and located in the heart of downtown San Antonio, Texas.

As Tutorial Chair, I am especially excited about the rich and diverse lineup of tutorials we have prepared for you. These sessions are designed to provide in-depth exploration of emerging topics, practical applications, and cutting-edge research in the field of cybersecurity and technology. Our presenters include leading experts from academia, industry, and government who bring deep knowledge and real-world experience.

To our attendees, thank you for bringing your energy, expertise, and curiosity. Your participation is what makes this conference dynamic and forward-thinking. We encourage you to take full advantage of the learning and networking opportunities ICCST offers.

To our sponsors, your generous support is instrumental in making this conference a success. Your commitment to innovation and thought leadership in security technology helps ensure ICCST remains a premier venue for scholarly and professional exchange.

Finally, we hope you find some time to enjoy all that San Antonio has to offer—from its rich history and cultural heritage to its renowned hospitality and cuisine.

Thank you again for joining us. I look forward to an engaging, insightful, and productive conference with all of you.

Warm regards,
Joan Labay-Marquez J.D., M. Jur. B.A.

Welcome Message from the WIE-YP-Exhibits Chair

Welcome to the 57th Annual 2025 IEEE International Carnahan Conference on Security Technology. We are so excited to have you join us this year from October 14 to 17, 2025, at the University of Texas at San Antonio (UTSA) School of Data Science, right in the heart of San Antonio, Texas.

As the Chair of IEEE Women in Engineering (WIE), I am thrilled to help co-host a conference that highlights groundbreaking advancements in security technology but also shines a spotlight on the people who are driving those innovations forward.

Alongside Neil Rathod, our IEEE Young Professionals Chair (YP), we're proud to help shape a program that celebrates the contributions of early-career researchers, rising engineers, and women leaders in the field. This year the committee has put together dynamic sessions, mentorship opportunities, and networking events to help spark new ideas and open doors for collaboration across disciplines and industries.

We invite you to explore the exhibits area, which will take place during the WIE/YP reception. It showcases organizations and innovators from around the world presenting the latest in security technology—from next-gen surveillance and cybersecurity tools to AI-powered systems and more. It's a great opportunity to connect with people and projects that are shaping the future.

Whether you're here to present, learn, mentor, or make new connections, we're grateful you're part of this vibrant and growing community. We hope you leave inspired and energized to take your work to the next level.

We look forward to meeting you in San Antonio!

Chyna J. Lane

2025 ICCST Organizing Committee

General Chair
Christopher Camargo
Southwest Research Institute (SwRI)

Technical Program Chair
Gordon Thomas
ICCST

Technical Program Co-Chair
Soodamani Ramalingam
University of Hertfordshire, UK

Technical Program Co-Chair
Abhilash Trehan
SwRI

Treasurer
Werner Osorio
SwRI

Sponsors & Exhibitors Chair
Jose Navarro
SwRI

Professional Education & Tutorial Chair
Joan Labay-Marquez
University of the Incarnate Word

Local Arrangements Chair
Michelle Valero
SwRI

WIE/YP Coordinating Chair
Chyna Lane
SwRI

Publicity Chair
Jose Navarro
SwRI

Conference Manager
Michelle Valero
SwRI

PRINCIPAL SPONSORS

AESS

IEEE Advancing Technology for Humanity

LONE STAR SECTION

DIAMOND SPONSOR

SwRI®

SILVER SPONSOR

OSINT INDUSTRIES

BASIC SPONSOR

IRYS

AFFILIATED ORGANIZATIONS

IEEE Women in Engineering We

IEEE youngprofessionals

Tuesday, October 14	
8:00AM – 1:00PM	Carnahan Golf Cup
7:30AM – 8:15AM	Breakfast
8:15AM – 5:00PM	**Tutorials:** (with breaks and lunch)
	1. Gonzalo Parra – Responsible AI: Evaluating LLMs with TrustLLM in a Local Environment
	2. Yaser Jararweh & **Izzat Alsmadi** (TAMUSA) – LLMs and Generative AI (GenAI) for Cybersecurity Applications
	3. Kyle Owens – Leveraging Post Quantum Cryptography on Embedded Devices
	4. Donald Green (SwRI) & **Annie McIntyre** (Chief Security Officer of EverLine) – Unique security challenges in the Operational Technology (OT) world of Critical Infrastructure
	5. Brian Kelley & **Asrat Ara –** Cybersecurity of 5G & Emerging 6G System Security

Wednesday, October 15	
7:30AM – 8:15AM	Breakfast
8:15AM – 8:40AM	**ICCST 2025 Conference Inauguration Program**
8:15AM – 8:30AM	**Chris Camargo**
8:30AM – 8:40AM	**Gordon Thomas**
8:40AM – 10:40AM	Keynote Presentation 1 **Rick Blum**; Keynote Presentation 2 **Greg Touhill**
10:40AM – 11:00AM	Mid-morning break.
11:00 AM – 12:00 PM	Paper Session 1 (3)
12:00PM – 1:00PM	Lunch break and briefing: **Oscar Anaya**:
1:00PM – 3:00PM	Paper Session 2 (6)
3:00PM – 3:30 PM	Afternoon break
3:30PM –5:30PM	Paper Session 3 (6)
5:30PM -7:00PM	WIE/YP event. Lead: **Chyna Lane**

Thursday, October 16	
7:30AM – 8:15AM	Breakfast
8:15AM – 9:20AM	Keynote Presentation 3 **Kathleen Kramer**
9:20AM – 10:20AM	Paper Session 4 (3)
10:20AM – 10:40AM	Mid-morning break
10:40AM – 12:00PM	Paper Session 5 (4)
12:00PM – 1:00PM	Lunch break and briefing: **Zeb Bowden**
1:00PM – 3:00PM	Paper Session 6 (6)
3:00PM – 3:30PM	Afternoon break
3:30PM – 5:30PM	Paper Session 7 (6)

Friday, October 17	
7:30AM – 8:15AM	Breakfast
8:15AM – 9:20AM	Keynote Presentation 5 **Moises Diaz**
9:20AM – 10:20AM	Paper Session 8 (3)
10:20AM – 10:40AM	Mid-morning break
10:40AM – 12:00PM	Paper Session 9 (4)
12:00PM – 1:00PM	Lunch Break **Vic Murray: Cyber & AI Panel**
1:00PM – 3:00PM	Paper Session 10 (6)
3:00PM – 3:30PM	Afternoon break
3:30PM – 4:30PM	Paper Session 11 (3)
4:30PM – 5:30PM	**Valedictory Session; ICCST 2026: Moises Diaz**

2025 ICCST

TUTORIAL SESSIONS

LOCATION: The University of Texas at San Antonio (UTSA) School of Data Science

FORMAT: In-Person

DATE: October 14, 2025

Join the ICCST Tutorial Program, Enhance Your Knowledge and Skills with Cutting-Edge Cyber Tutorials!

REGISTER HERE: Seats are still available (Link)

CONTACT INFORMATION: Dr. Joan Labay-Marquez,University of Incarnate Word Tutorial Chair, *labaymar@uiwtx.edu*

HIGHLIGHTS: The Tutorial Topics include the following:

- Responsible AI
- Quantum computing on crypto graphic
- Physical security infrastructure
- Block Chain in trust transparency
- Biometrics
- Secure 5G

The conference will be held at the UT San Antonio San Pedro I building in downtown San Antonio, Texas. This facility houses both the College of AI, Cyber, and Computing and the National Security Collaboration Center.

Responsible AI: Evaluating LLMs with TrustLLM in a Local Environment

Abstract

This hands-on tutorial will introduce participants to TrustLLM, a comprehensive benchmark designed to assess the trustworthiness of large language models (LLMs) across multiple dimensions, including truthfulness, safety, fairness, robustness, privacy, and machine ethics. The session will guide attendees in setting up and deploying TrustLLM in a local environment, evaluating LLMs against these principles without relying on cloud-based infrastructure. By the end of the tutorial, participants will understand how to assess and improve LLM trustworthiness, ensuring responsible AI deployment in their own projects.

Outline

1. Introduction to Responsible AI and TrustLLM
2. Setting Up TrustLLM in a Local Environment
3. Evaluating LLMs with TrustLLM
4. Hands-On Exercises
5. Best Practices for Responsible AI
6. Q&A and Wrap-Up

Delivery Method

- Format: In-person workshop
- Instructional Style: Interactive, hands-on tutorial
- Resources: Step-by-step instructions provided (but no pre-configured cloud environment)
- Prerequisites: Participants should bring their own laptops with a compatible local environment for running TrustLLM
- Engagement: Live coding, guided exercises, and real-time discussions

Dr. Gonzalo De La Torre Parra

Dr. Gonzalo De La Torre Parra is an Assistant Professor at the University of the Incarnate Word (UIW) in the Department of Engineering, Computing, and Cybersecurity and the CEO of Safe AI LLC, where he leads research and development in secure, reliable, and ethical AI solutions. His expertise spans Large Language Models (LLMs), Agentic AI, AI-driven cybersecurity, and distributed AI architectures, with a growing focus on Quantum Artificial Intelligence (QAI) and its applications in cybersecurity and advanced computing.

Dr. Parra has an extensive research background in AI-driven cybersecurity, with publications in top-tier security conferences such as IEEE European Symposium on Security and Privacy (Euro S&P), IEEE Symposium on Security and Privacy (S&P), and the Network and Distributed System Security Symposium (NDSS).

LLMs and Generative AI (GenAI) for Cybersecurity Applications

Abstract

The tutorial aimed to provide a comprehensive review for the usage of the emerging technologies such as LLMs and GenAI for Cybersecurity applications. We are considering different domains and focusing on hardware design security, intrusion detection, software engineering, design verification, cyber threat intelligence, malware detection, and phishing detection.

Topics to be discussed:

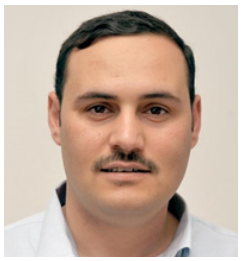
We are considering different domains and focusing on hardware design security, intrusion detection, software engineering, design verification, cyber threat intelligence, malware detection, and phishing detection.

Outline

1. Introduction to Generative AI and LLMs
2. Key Concepts and Architecture
3. Practical IT Applications
4. Challenges and Ethical Issues
5. Q&A

Izzat Alsmadi

Texas A&M, San Antonio. USA



Yaser Jararweh

University of Science and Technology: Jordan

Izzat Alsmadi is a Professor in the department of computing and cyber security at the Texas A&M, San Antonio. He has his master and PhD in Software Engineering from North Dakota State University in 2006 and 2008. He has more than 100 conference and journal publications. His research interests include: Cyber intelligence, Cyber security, Software security, software engineering, software testing, social networks and software defined networking. He is lead author, editor in several books including: Springer The NICE Cyber Security Framework Cyber Security Intelligence and Analytics, 2019, Practical Information Security: A Competency-Based Education Course, 2018, Information Fusion for Cyber-Security Analytics (Studies in Computational Intelligence), 2016. He is also a member of The National Initiative for Cybersecurity Education (NICE) group, which meets frequently to discuss enhancements on cyber security education at the national level.

Yaser Jararweh received the Ph.D. degree in computer engineering from The University of Arizona, in 2010. He is currently an Associate Professor of computer science with the Jordan University of Science and Technology. He has co-authored several technical papers in established journals and conferences in fields related to cloud computing, edge computing, SDN, and big data. He is a Steering Committee Member and the Co-Chair of CCSNA 2018 with INFOCOM. He is also chairing many IEEE events, such as ICSC, SNAMS, FMEC, and FLLM. He is also the Steering Committee Chair of the IBM Cloud Academy Conference. He served as a guest editor for many special issues in different established journals. He is also an Associate Editor of Cluster Computing Journal (Springer) and Information Processing and Management (Elsevier).

Mike O'Brien

Texas A&M,
San Antonio. USA

Mike O'Brien is a professor in the Department of History, Philosophy, and Geography and the Department of Health and Behavioral Sciences at Texas A&M University–San Antonio. He received his undergraduate degree from Rice University in 1972 and his PhD in anthropology from the University of Texas at Austin in 1977. He joined the University of Missouri in 1980 as an assistant professor of anthropology, becoming dean of the College of Arts and Science in 2006 after a national search. He moved to Texas A&M University–San Antonio in July 2016, serving as provost and academic vice president until December 2021.

O'Brien has authored or edited 26 books, eight of which have been translated into Spanish, German, Korean, Chinese, Hungarian, and Arabic. He has also written over 150 articles, which have appeared in journals such as Science, Philosophical Transactions of the Royal Society, Nature Communications, Journal of the Royal Society Interface, Behavioral and Brain Sciences, Journal of Human Evolution, and Journal of Theoretical Biology.

His work in AI began in 2015 as a result of his experience with serious social unrest at the University of Missouri stemming from the work of the Internet Research Agency, a well-known Russian troll factory in St. Petersburg. His research includes cybersecurity, deep fakes, LLMs, generative AI, and computational biology.

Leveraging Post Quantum Cryptography on Embedded Devices

Abstract

This workshop seeks to familiarize the participants with the basics of Post-Quantum Cryptography (PQC), especially on embedded platforms. It will consist of a brief introduction on the topic, followed by an interactive C/C++ programming session, and a demonstration of the PQC algorithms in an embedded environment. Ideally, participants will be more familiar with existing cryptographic libraries, embedded systems, and PQC following this exercise.

Outline

1. Existing embedded cryptography libraries
   - Do not roll your own crypto
   - MbedTLS, WolfSSL, OpenSSL
2. What is PQC?
   - Shor's, Grover's
   - What is asymmetric cryptography?
   - Lattice, ECC, Hash, Isogeny, elliptic curve, RSA
3. Integrating PQC into existing libraries
   - Modular cryptography/ swappable algorithms
   - Massive key sizes -> problems with some libraries
4. Download tutorial repo from git
5. Run submodule update to clone crypto library
6. Point STM32 IDE towards git repo/init project
7. Fill in skeleton code
8. Connect STM32 board via both USBs
9. Program Board
10. Monitor logs to verify functionality using UART

Delivery Method

1. Format: In-person workshop
2. Instructional Style: Interactive, hands-on tutorial
3. Resources Provided:
   - STM32 Nucleo board with wireless capability (*https://www.digikey.com/eproucts/detail/stmicroelectronics/NCLEO-WB55RG/13684823* for instance)
   - USB A/C -> Micro USB
   - USB A/C -> Serial wire
4. Prerequisites:
   - Laptop with 2 USB ports
   - STM32 Cube IDE installed
     – Other compilation plat forms will theoretically work, but I'm not supporting them for the sake of simplicity
   - Putty/other serial communication program to talk with board via UART
   - The ability to clone a Git repository

Kyle Owens

Southwest Research Institute

kyle.owens@swri.org

Kyle Owens is a computer engineer at Southwest Research Institute (SwRI). He has performed research across multiple disciplines, including cybersecurity, cryptography, reverse engineering, and software development. His background spans the commercial automotive and defense sectors, where he has contributed to secure software development, security assessments, and cybersecurity vulnerability research.

Unique Security Challenges in the Operational Technology (OT) World of Critical Infrastructure

Abstract

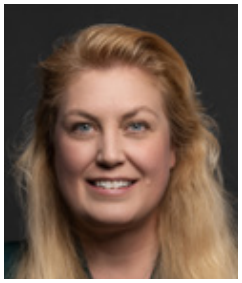
This tutorial tackles the identification of security, and approaches to mitigating those risks, within the challenging Operational Technology (OT) landscape. OT is everywhere, at diverse and complex sites across energy, logistics, transportation, and manufacturing. OT assets in this sector make up the US Critical Infrastructure, an attractive target by the adversary. Securing this environment requires a different way of thinking about data flow, physical protections, and human interaction with technology, to ensure that infrastructure remains safe and stable. In this tutorial, we will walk through those elements that make up the risk surface and delve into approaches to assessment and mitigation in a 24/7 operational architecture.

Outline

1. Defining the OT Environment
2. The Risk Equation, exploring Threat, Vulnerability, and Consequence
3. Nexus of Security, Safety, and Stability
4. Approaches to Mitigating OT Risk
5. Tabletop Exercises: Walking through Real Life Scenarios
6. Q&A, Discussion

Tutorial Presenter: Annie McIntyre,
annie.mcintyre@everlineus.com

Annie McIntyre is the Chief Security Officer at EverLine, an integrated technical services firm for critical infrastructure. Ms. McIntyre was previously the President and Chief Executive Officer of Ardua Strategies, Inc., acquired by EverLine in 2021, that provided solutions for the cyber and operational security issues of energy and infrastructure. Prior to founding Ardua, Ms. McIntyre was a Principal Member of Technical Staff and Program Manager at Sandia National Laboratories. Ms. McIntyre has worked extensively on federal defense, energy, and homeland security projects. She previously worked in information warfare and survivability, serving as IO Laboratory Chief and Information Warfare Lead for Future Combat Systems Assessments at the U.S. Army Research Laboratory.
She served as an author for the American Petroleum Institute's SCADA Security Standard (1164v2), serves on the Advisory Council at the North American Energy Standards Board, and has served as a Senior Fellow at the University of Minnesota's Technology Leadership Institute.



Annie McIntyre

Chief Security Officer, Everline

Donald Green

Southwest Research Institute

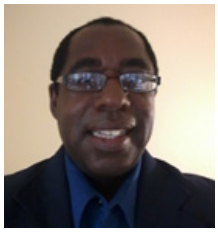
Tutorial Presenter: Don Green,
donald.green@swri.org

Don Green is a Lead Engineer at Southwest Research Institute (SwRI), an independent, nonprofit R&D firm. He leads projects to provide cybersecurity for clients as varied as commercial automobile manufacturers, public utilities, and the Defense Department. These projects range from traditional penetration testing to the design and implementation of secure update systems for embedded networks. Prior to joining SwRI, Mr. Green served as a civilian with the National Security Agency. He was chief of the SIGINT Forensics Center at NSA-Texas, and was an adjunct faculty member of the National Cryptologic School. He is a graduate of NSA's System and Networks Interdisciplinary Program and a Certified Information Systems Security Professional (CISSP).

Tutorial on the Cybersecurity of 5G and Emerging 6G System Security

Abstract

This tutorial presents an introductory overview of 5G cybersecurity and emerging 6G security. Coverage includes a summary of essential Network Functions (NFs) involved in 5G cybersecurity, an overview of the mutual authentication protocols between the 5G network and mobile devices, the protection of control plane traffic between the NFs and Transport Layer Security (TLS), the Security Edge Protection Proxy (SEPP), key separation in 5G, and an on overview of the security model associated with the 3GPP technical specification TS 33.501. We also present information on emerging 6G security research. The 6G cybersecurity tutorial includes 6G AI security, NIST Zero Trust, and 6G Physical Layer Security.



Dr. Brian Kelley

Department of ECE, COE, University of Texas at San Antonio
FutureG Applied Research, OUSD(R&E)

Israt Ara, Ph.D Candidate

Department of ECE, COE, University of Texas at San Antonio

Tutorial Outline, 9 am – 12 pm

1. Introduction to 5G Systems
2. 5G and Open-RAN
3. 5G Security
   a. 5G Network Access Security
   b. 5G Security Domains
   c. 5G Key Management
   d. NIST Security Standards
4. 5G Call Flow Examples
5. OSI Security Survey, Security Threats, and Defense Schemes
   a. Security at the Application Layer
   b. Transport Layer SEC
   c. Network Layer SEC
   d. Data Link Layer SEC
   e. Physical Layer SEC

Tutorial Outline, 1 pm – 4 pm

6. Introduction to 6G Systems
7. Future Trends in 6G Security
8. 6G Security Threats
   a. Emerging Areas of Security for Defending 6G Systems
   b. Survey of 6G Security
   c. Use of AI in 6G Security
   d. Application of AI and Physical Layer Security in 6G Systems

Tutorial Presenter: Dr. Brian Kelley, brian.kelley@utsda.edu

Dr. Brian Kelley is an Associate Professor of Electrical and Computer Engineering in advanced communication at the KLESSE College of Engineering, Department of Electrical & Computer Engineering, University of Texas at San Antonio (UTSA)1. His research interests include 5G-SA, 6G Systems, 6G-AI, Security, Augmented Reality wireless, 5G Telemedicine, and connected Autonomous Vehicles, Dr. Kelley's Spectrum Coexistence, Non-Terrestrial Networks, Massive MIMO MIMO, Software Management of Open Source 5G Systems, 6G Physical Layer Security for Private Air Interface, 5G Cybersecurity systems, and Open Radio Access Networks (O-RAN). He has over 80 refereed publications, holds 11 U.S. patents, and spent 10+ years in the Telecommunication industry with Motorola. In 2021, Dr. Kelley was named a Day One Technology Policy Accelerator Fellow in 5G Connected Autonomous Vehicles by the Day One Project. From 2021-2023, he was co-PI of the NSF REU in Artificial Intelligence Powered Robotics in 5G Networks. From 2020-2023, Dr. Kelley was the 5G Principal Investigator of two major programs: the 5G Core Capabilities & Security Program and the 5G Telemedicine Program, within the JBSA 5G Program Management Office of OUSD(R&E). He received his BSEE from Cornell University, graduating Tau Beta Pi and Eta Kappa Nu. He received his MSEE & Ph.D. in E.E. from the Georgia Institute of Technology, where he was an Office of Naval Research Fellow and a Georgia Tech Presidential Fellow. From 2023-present, Dr. Kelley has been a Principal Investigator in FutureG Applied Research with OUSD(R&E).

Tutorial Presenter: Israt.Ara, israt.ara@my.utsa.edu

Israt Ara received a B.Sc. degree in electrical, electronics, and communication engineering from the Military Institute of Science and Technology, Bangladesh 2018. She is currently a Ph.D. candidate with the University of Texas at San Antonio1, USA. She was a Network Operations Engineer with Ding, an Ireland-based company, until 2021. Her research interests include 5G and 6G communication security schemes, physical layer security, AI/Machine Learning (ML) in wireless communication, and open radio access networks.

2025 ICCST Tutorials • Moderator: Joan Labay-Marquez • Tuesday, Oct. 14		
Time	**Title/Room**	**Instructors**
9:00AM - 12:00PM	LLMs and Generative AI (GenAI) for Cybersecurity Applications Room – CR325	**Dr. Izzat Alsmadi** **Dr. Yaser Jararweh** **Dr. Mike O'Brian**
9:00AM - 12:00PM	Unique Security Challenges in the Operational Technology (OT) World of Critical Infrastructure Room – CR532	**Annie McIntyre** **Donald Green**
1:00PM - 4:00PM	Responsible AI: Evaluating LLMs with TrustLLM in a Local Environment Room – CR240	**Dr. Gonzalo De La Torre Parra**
1:00PM - 4:00PM	Leveraging Post Quantum Cryptography on Embedded Devices Room – CR450	**Kyle Owens**
All Day Session	Tutorial on the Cybersecurity of 5G and Emerging 6G System Security Room – Yotta Room	**Dr. Brian Kelley** **Israt Ara**

Wednesday, October 15th • Moderator: Gordon Thomas

Rick S. Blum

Author Biography: Rick S. Blum received a B.S. in Electrical Engineering from the Pennsylvania State University in 1984 and his M.S. and Ph.D in Electrical Engineering from the University of Pennsylvania in 1987 and 1991.

From 1984 to 1991 he was a member of technical staff at General Electric Aerospace in Valley Forge, Pennsylvania and he graduated from GE`s Advanced Course in Engineering. Since 1991, he has been with the Electrical and Computer Engineering Department at Lehigh University in Bethlehem, Pennsylvania where he is currently a Professor and holds the Robert W. Wieseman Endowed Professorship in Electrical Engineering. His research interests include machine learning and signal processing for security, smart grid, communications, sensor networking, radar, and sensor processing. He was on the editorial board for the Journal of Advances in Information Fusion of the International Society of Information Fusion. He was an associate editor for IEEE Transactions on Signal Processing and for IEEE Communications Letters. He has edited special issues for IEEE Transactions on Signal Processing, IEEE Journal of Selected Topics in Signal Processing and IEEE Journal on Selected Areas in Communications. He was a member of the SAM Technical Committee (TC) of the IEEE Signal Processing Society. He was a member of the Signal Processing for Communications TC of the IEEE Signal Processing Society and was a member of the Communications Theory TC of the IEEE Communication Society. He was on the awards Committee of the IEEE Communication Society.

Dr. Blum is a Fellow of the IEEE and served two terms as an IEEE Signal Processing Society Distinguished Lecturer. He is currently an IEEE AESS Distinguished Lecturer. He is an IEEE Third Millennium Medal winner, Eleanor and Joseph F. Libsch Research Award winner, a member of Eta Kappa Nu, a member of Sigma Xi, and holds several patents. He was awarded an ONR Young Investigator Award in 1997. His IEEE Fellow Citation ``for scientific contributions to detection, data fusion and signal processing with multiple sensors'' acknowledges contributions to the field of sensor networking.

Cyber Security of Sensor Systems for State Sequence Estimation: An AI Approach

Remarks Description: Due to possible devastating consequences, counteracting sensor data attacks is an extremely important topic, which has not seen sufficient study. This presentation presents the first methods that accurately identify/eliminate only the problematic attacked sensor data presented to a sequence estimation/regression algorithm under a powerful attack model. The approach does not assume a known form for the statistical model of the sensor data, allowing data-driven and machine learning sequence estimation/regression algorithms to be protected. A simple protection approach for attackers not endowed with knowledge of the details of our protection approach is first developed, followed by additional processing for attacks based on protection system knowledge. Experimental results show that the simple approach achieves performance indistinguishable from that for an approach which knows which sensors are attacked. For cases where the attacker has knowledge of the protection approach, experimental results indicate the additional processing can be configured so that the worst-case degradation under the additional processing and a large number of sensors attacked can be made significantly smaller than the worst-case degradation of the simple approach, and close to an approach which knows which sensors are attacked, with just a slight degradation under no attacks. Mathematical descriptions of the worst-case attacks are used to demonstrate the additional processing will provide similar advantages for cases for which we do not have numerical results. All the data-driven processing used in our approaches employs only unattacked training data.

Wednesday, October 15th • Moderator: Gordon Thomas

Gregory J. Touhill

Speaker Biography: Gregory J. Touhill is the director of the CERT Division of the Carnegie Mellon University (CMU) Software Engineering Institute (SEI), where he leads researchers who analyze security vulnerabilities and contributes to long-term improvements in cybersecurity. He served as the first CISO of the United States government and as deputy assistant secretary in the Department of Homeland Security's Office of Cybersecurity and Communications. He held executive leadership roles in industry including board directorship and advisor to three Fortune 100 companies, and as the president of a cybersecurity start-up.

Touhill is a 30-year U.S. Air Force combat veteran. He served as an operational commander and senior leader, advancing to the position of J6 and CIO of USTRANSCOM. He is the recipient of the Bronze Star medal, the Air Force Science and Engineering Achievement Award, and the Master Cyberspace Operations and Master Space Operations wings. He retired from the U.S. Air Force with the rank of brigadier general.

Touhill holds degrees from the Pennsylvania State University, the University of Southern California, and the Air War College. He maintains CISSP, CISM, and NACD.DC certifi-cations and is adjunct faculty at CMU.

Touhill has been recognized by Federal Computer Week and Security Magazine for his contributions to cybersecurity. He is a recipient of the Baldrige Foundation Leadership Award in Cybersecurity, the General Michael V. Hayden Lifetime Achievement Award, the ICS2 F. Lynn McNulty Tribute Award, and the Government Information Security Leadership Award. He is a co-author of Cybersecurity for Executives: A Practical Guide and Commercialization of Innovative Technologies.

Are You Ready for AI's Plan to Destroy Humanity?

Remarks Description: In this provocative, sometimes irreverent, and informative discussion, retired Brigadier General Greg Touhill, director of the CERT at Carnegie Mellon University's Software Engineering Institute, and former Chief Information Security Officer of the US government, will share observations on the current state of AI research and development; prescriptions to incorporate secure-by-design principles into AI products and services; lessons learned by the AI Security and Incident Response Team; and recommendations on how to engineer a safer and more secure future digital environment in the "Age of AI."

Wednesday, October 15th • Moderator: Gordon Thomas

Oscar Anaya

Biography: Oscar serves as the Chief Technology Officer of Irys Technologies, Inc., where he leads the development of adversarial testing environments and FPGA-accelerated threat models. A cybersecurity expert and former member of IBM X-Force Red, he specializes in ethical hacking, threat emulation, and vulnerability analysis. Oscar has extensive experience building and evaluating secure architectures for enterprise and mission-critical systems, with a particular focus on blockchain-informed security methods and red-team methodology.

Before the 'The': Pre-Conceptual AGI Detection Framework

Remarks Description: This presentation introduces a mathematical system for detecting AGI emergence by analyzing pre-conceptual cognitive structures—the foundational architecture of intelligence prior to behavioral expression. Attendees will gain insight into new substrate-level metrics and protocols with immediate applications for LLM evaluation, early AGI detection, and AI safety.

Thursday, October 16th • Moderator: Gordon Thomas

Kathleen A. Kramer, 2025 IEEE President & CEO

Kathleen A. Kramer is a Professor of Electrical Engineering at the University of San Diego in California. She worked to develop new engineering programs as a founding member of the faculty and eventually became the chair of electrical engineering, then serving as Director of Engineering (2004-2013), providing academic leadership for all of the university's engineering programs. Her teaching interests are in the areas of signal processing, mechatronics and robotics, and communication systems.

She has also been a member of technical staff at several companies, including ViaSat, Hewlett Packard, and Bell Communications Research. She is a Distinguished Lecturer for the IEEE Aerospace and Electronic Systems Society (AESS) and is a past vice president of the society. She is a Fellow of ABET, and a leader in the development of accreditation criteria for cyber security, mechatronics & robotics, and graduate programs.

Kathleen served on the IEEE Board of Directors as IEEE Secretary and chair of Governance and IEEE Region 6 (Western USA) Director. She was also chair of the 2023 IEEE Ad Hoc Committee on Innovating Funding Models.

She received the B.S. degree in electrical engineering magna cum laude with a second major in physics from Loyola Marymount University, and the M.S. and Ph.D. degrees in electrical engineering from the California Institute of Technology.

Evolving Cyber Systems in Avionics

Remarks Description: Avionics systems have evolved from a slow-changing field into complex, cyber-physical systems central to modern air and space transport. Their deployment involves multi-agent coordination in safety-critical environments. Autonomy depends on separation assurance and collision avoidance, while vision-based navigation tackles difficult implementation challenges. Traffic management for emerging platforms—especially UAS and low Earth orbit systems—faces integration and scalability hurdles. Artificial Intelligence offers promising solutions for autonomous functions, but certification demands remain a key barrier to adoption.

Thursday, October 16th • Moderator: Gordon Thomas

Zeb Bowden

Dr. Zeb Bowden oversees the Division of Technology Development and Deployment at the Virginia Tech Transportation Institute (VTTI), which is comprised of a talented team of technical experts that support the development and operations of VTTI's core technology. He holds a rank of Senior Research Scientist, with research areas of focus that include automotive cybersecurity, data management, and large-scale data ingestion for all naturalistic driving studies at VTTI. Dr. Bowden has served as PI or co-PI on over $10M in sponsored research. Prior to his current role, he served as VTTI's Systems Architect and Lead Application Developer, designing and supporting the IT systems responsible for collecting sensor/video data for naturalistic driving data collection, as well as developing client/server, database, and web-based applications to support the retrieval, transfer, ingestion, and analysis of data in global locations. In his time at VTTI, Dr. Bowden has designed and developed data pipelines for several large-scale projects, including the Second Strategic Highway Research Program and the FMCSA Data Repository.

Life(cycle) Lessons from Over-the-Air Updates

Remarks Description: This presentation investigates security and management implications of software updates, primarily in the automotive space, but with challenges and lessons learned that are applicable to many other environments. Recent changes in automotive technology, specifically software defined vehicles (SDVs) and the recent shift towards updating vehicles over-the-air (OTA), provide some especially interesting problems (and solutions). OTA can turn "please visit your dealer" into "done while you slept," but that isn't free magic. We will look at how OTA lifts completion and shrinks hazard dwell time, but also how validation costs swell as vehicles age and configurations proliferate (the curve is… decidedly not flat). You'll see why cadence matters—few big gulps vs. many small sips—and how to pick the right rhythm when safety risk is high, regulators are watching, and your time is finite.

Friday, October 17th • Moderator: Gordon Thomas

Moises Diaz

Author Biography: Moises Diaz received the M.Tech., M.Sc., and Ph.D. degrees in Engineering, and the M.Ed. degree in Secondary Education from the University of Las Palmas de Gran Canaria, Spain, in 2010, 2011, 2016, and 2013, respectively. He joined the Physics Department of the same university in May 2021, where he is currently an Associate Professor. He previously held Associate Professor positions at the Universidad del Atlántico Medio and the International University of La Rioja, Spain.

His current research interests include pattern recognition, document analysis, handwriting recognition, and biometrics. He serves as an Associate Editor for Pattern Recognition (Elsevier), is a regular reviewer for top-tier journals and leading international conferences, and has co-authored over 100 publications in international conferences and high-impact JCR journals, including 29 papers in Q1 journals.

Dr. Diaz has received Best Paper Awards at ICFHR 2014, ICDAR 2015, and ICCST 2023, as well as several research distinctions, such as the university's awards for highest scientific output and young investigator recognition. He was also a finalist in the European Biometric Research and Industry Award, and has been granted the IAPR Research Scholarship and a COST Trainee Grant. He has held visiting research positions at the University of Hertfordshire (UK), the Brno (Czech Republic), the Universities of Salerno, Bari, and Parma (Italy), the University of Fribourg (Switzerland), ISI Kolkata (India), and École Polytechnique Montréal (Canada).

Securing Biometric Systems: Detecting Bots in Handwriting

Remarks Description: Handwriting or handwritten signatures are commonly used to authenticate the identity of individuals in various digital systems. Prior to authentication, a security control related to the nature of the movement, i.e., whether it is real or synthetic, can help prevent large-scale frauds carried out by bots.

This keynote highlights a research cycle aimed at improving both the generation of bots and the robustness of their detection mechanisms.

The proposed cycle consists of four stages. First, we review a range of analytical and data-driven techniques for enhancing the realism of **S**ynthetic handwriting. Second, these realistic synthetic samples are used to **A**ttack biometric systems. Thirdly, an **E**valuation of the accepted/rejected samples is carried out. Fourth, the **D**etector of synthetic samples is improved to deal with synthetic handwriting that is wrongly accepted and real handwriting that is erroneously rejected.

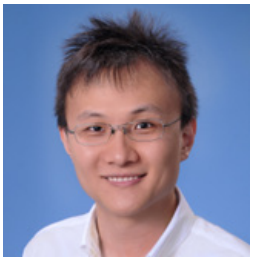
This cycle, known as the **SAED** cycle (**S**ynthetic, **A**ttack, **E**valuation, and **D**etection), will be illustrated using state-of-the-art technologies for bot detection based on handwriting. Throughout the keynote, special emphasis will be placed on the role of bot detection as a first-layer security control in digital devices such as tablets and smartphones.

Panel Leader: Victor Murray, CISSP

Biography: Mr. Murray is an assistant director at Southwest Research Institute and is a Certified Information Systems Security Professional (CISSP). He has over 20 years of experience leading the development and testing of embedded systems. He has performed penetration tests and risk assessments, developed secure systems, and performed cybersecurity related research. He has supported projects across multiple industries including critical infrastructure, commercial automotive, transportation, aerospace, and defense. Mr. Murray has led many projects including penetration testing, applying zero trust principles to embedded systems, and developing intrusion detection systems.

The Use of Artificial Intelligence in Cybersecurity

Remarks Description: Welcome to our panel discussion on the transformative role of artificial intelligence in cybersecurity. Today, we will explore how AI is both enhancing security measures and being utilized by cybercriminals, touching on the various challenges and ethical considerations that arise. Our panel will also discuss future trends and developments, examining how AI will shape the cybersecurity landscape moving forward. Join us as we delve into these critical issues and uncover insights to better protect our digital world.



Panel Member: Zechun Cao, Ph.D.

Biography: ZECHUN CAO received the Ph.D. degree in Computer Science from the University of Houston. He is currently an Assistant Professor in the Department of Computational, Engineering, and Mathematical Sciences at Texas A&M University–San Antonio. His research interests include computer security, graph-centric computing, and privacy-preserving algorithms. He has authored and coauthored publications in areas such as network and software security, cloud computing, and privacy-preserving natural language processing. His research has been supported by the National Science Foundation (NSF), the American Society for Engineering Education (ASEE), Google, and internal funding from Texas A&M University–San Antonio.

Panel Member: Jonathan Esquivel

Biography: Jonathan Esquivel is a senior research computer scientist for Southwest Research Institute in San Antonio, Texas. He has a background in cyber security, data science, and machine learning with advanced degrees in computer science and mathematics. During his time at the institute, Mr. Esquivel has influenced numerous applied machine learning technologies across a wide variety of areas including fugitive leak detection, traffic system monitoring, automotive cyber security, markerless motion capture, and general computer vision applications. During this time, he has been a key leader for algorithm development across several intrusion detection technologies in the automotive, Department of Transportation, and critical infrastructure industries.

Panel Member: Gonzalo De La Torre Parra, Ph.D.

Biography: Gonzalo De La Torre Parra is an accomplished assistant professor in the Department of Engineering, Computing, and Cybersecurity at the University of the Incarnate Word. He earned his Ph.D. in Cybersecurity from the University of Texas at San Antonio in 2021, where he also worked as a research fellow, leading several cyber security projects in collaboration with industry partners, including CPS Energy and CISCO. Gonzalo holds a Bachelor's degree in Electrical Engineering from Texas AM University-Kingsville, which he earned in 2009, and a Master's degree in Electrical Engineering from The University of Texas at San Antonio, which he obtained in 2015. His primary research interest lies in applying artificial intelligence techniques to tackle cyber security challenges in cloud computing, edge computing, and Internet of Things technologies. As a leading expert in his field, Gonzalo has contributed significantly to academia and industry, and he continues to mentor and inspire the next generation of cybersecurity professionals.

Panel Member: César A. Uribe, Ph.D.

Biography: César A. Uribe received his BSc. in Electronic Engineering from Universidad de Antioquia in 2010. He then received an MSc. in Systems and Control from Delft University of Technology in the Netherlands in 2013. In 2016, be received an MSc. in Applied Mathematics from the University of Illinois at Urbana-Champaign. He continued at the University of Illinois at Urbana-Champaign, and in 2018 received his Ph.D. in Electrical and Computer Engineering. Urbie was a Postdoctoral Associate in the Laboratory for Information and Decision Systems-LIDS at the Massachusetts Institute of Technology (MIT) and a visiting professor at the Moscow Institute of Physics and Technology. His research interests include distributed learning and optimization, decentralized control, algorithm analysis, and computational optimal transport. He joined Rice ECE Department as Louis Owen Assistant Professor in January 2021.

Panel Member: Steven Ullman, Ph.D.

Biography: Dr. Steven Ullman is an Assistant Professor in the Department of Information Systems and Cybersecurity at UT San Antonio in the College of AI, Cyber and Computing. Dr. Ullman's research is centered in AI and cybersecurity, where he focuses on developing AI-based methods for enhancing vulnerability detection, remediation, and management, particularly for open-source software and IT infrastructure. He has published his research in the Journal of Management Information Systems, AIS Transactions on Replication Research, ACM KDD AI4Cyber Workshop, and IEEE Intelligence and Security Informatics Conference. Dr. Ullman has presented his research through invited talks at the INFORMS Annual Meeting, the Open Data Science Conference (ODSC), and the Hawaii International Conference on System Sciences (HICSS). His research has also been funded by multiple grants from the NSF's cybersecurity programs, including the Secure and Trustworthy Cyberspace (SaTC) and Cybersecurity Innovation for Cyberinfrastructure (CICI) programs. He is a member of the IEEE, ACM, AIS, and INFORMS.

Paper Session 1 (3) • Insider Threat Detection • Moderator: Gordon Thomas • Wednesday, Oct. 15		
Time	**Title**	**Main Author**
11:00am - 11:20am	Explainable Bidirectional LSTM Autoencoder for Insider Threat Detection in Various Scenarios PID# 2025003491	**Abdul Abbasi** Systems Design, Engineering University of Waterloo, Canada
11:20am - 11:40am	Explicit Behavioral Embedding Method for Generating Explanations of Insider Threat Events – PID# 2025003490	**Abdul Abbasi** Systems Design, Engineering University of Waterloo, Canada
11:40am - 12:00pm	Technical Risk Indicators for the Critical Pathway to Insider Risk – PID# 2025003510	**Bill Claycomb** Software Engineering Institute Carnegie Mellon University United States

Paper Session 2 (6) • Threat Detection & Defense • Moderator: Lauren Reinerman Jones Wednesday, Oct. 15		
Time	**Title**	**Main Author**
1:00pm - 1:20pm	A Novel Approach for Host-based Security: SECUREHOST IDS – PID# 2025003319	**Ayad Barsoum** Professor of Computer Science, St. Mary's University, United States
1:20pm - 1:40pm	A Novel Vulnerability Prioritization Model for Workstation Endpoints with Context Intelligence – PID# 2025003295	**Logan Scott** School of Computer Information Sciences, University of the Cumberlands, United States
1:40pm - 2:00pm	Anomaly Detection Using Multivariate Gaussian Analysis on Communication Networks – PID# 2025003482	**Donald Van Rheeden** Defense and Intelligence Solutions, Southwest Research Institute, United States
2:00pm - 2:20pm	SwRI Briefing	
2:20pm - 2:40pm	Interpreting CNN in Cybersecurity: Process-Level Attribution via Benign-Replacement Occlusion – PID# 2025003337	**Gavin Holliday** Computer Science, Texas State University, United States
2:40pm - 3:00pm	Assessing Software Security Maturity via an AI-Augmented Risk-Based Framework – PID# 2025003489	**William Stout** Cyber Security Initiatives,Sandia National Laboratories, United States

Paper Session 3 (6) • AI & Machine Learning in Security – Part 1 • Moderator: Gordon Thomas Wednesday, Oct. 15		
Time	**Title**	**Main Author**
3:30pm - 3:50pm	AI-Powered Intrusion Detection with SHAP Explainability and Feedback Loop: A Modular Pipeline for Cyber Threat Classification – PID# 2025003322	**Raj Kumar Myakala** Data Analytics, CVS Health, United States
3:50pm - 4:10pm	Risk Profiling of CVE Vulnerabilities via Unsupervised Clustering – PID# 2025003478	**Arbaz Surti** Independent Researcher, United States
4:10pm - 4:30pm	Lightweight AI-Based Intrusion Detection Models for IoT Devices: A Comparative Review – PID# 2025003347	**Akalanka Mailewa** Information Systems and Cybersecurity, University of Texas San Antonio, United States
4:30pm - 4:50pm	A Risk-Conscious Cybersecurity Approach for Healthcare Using Zebra-Seeker Tuned Machine Learning Models – PID# 2025003508	**Damodhara Reddy Palavali** Software Engineer, Sbase Technologies, United States
4:50pm - 5:10pm	Adversarial Attacks on FinTech AI Models - Threats and Mitigation Techniques – PID# 2025003512	**Veeramani Sampathkumar** Senior Member, IEEE, United States
5:10pm - 5:30pm	Efficient Backdoor Defense for Federated Learning with Partial Model Inspection – PID# 2025003292	**Palden Lama** Computer Science, University of Texas at San Antonio, United States

Paper Session 4 (3) • Quantum Computing & Cryptography • Moderator: Fabio Garzia Thursday, Oct. 16		
Time	**Title**	**Main Author**
9:20am - 9:40am	OSINT Briefing	
9:40am - 10:00am	Quantum GAN Based Adversarial Attack Generation for Network Intrusion Detection System – PID# 2025003340	**Ishan Pathak** Department of Electrical Engineering and Computer Science, Texas A&M University Kingsville, United States
10:00am - 10:20am	Post Quantum Cryptography on Constrained Networks – PID# 2025003668	**Cameron Mott** Intelligent Systems Division, Southwest Research Institute, United States

Paper Session 5 (4) • AI &Machine Learning in Security – Part 2 • Moderator: Miguel Ángel Ferrer Thursday, Oct. 16		
Time	**Title**	**Main Author**
10:40am - 11:00am	VeriPhish: Bridging AI Explainability and Accuracy in Phishing Detection through XAI and LLMs – PID# 2025003487	**Priyanka Kumar** Computer Science, University of Texas Permian Basin, United States
11:00am - 11:20am	Redefining Cyber Resilience: AI-Driven Metrics for Enhanced Threat Intelligence Systems – PID# 2025003455	**Gahangir Hossain** Data Science, University of North Texas, United States
11:20am - 11:40am	AI-Driven Real-Time API Security: Explainable Threat Detection for Cloud Environments – PID# 2025003367	**Akshay Mittal** IT, PhD Scholar, University of the Cumberlands, United States
11:40am - 12:00pm	Robust Federated Learning via Stable Cosine Similarity – PID# 2025003518	**Panagiotis Markopoulos** Computer Engineering, University of Texas at San Antonio, United States

Paper Session 6 (6) • IoT and Network Security • Moderator: Virginia Espinosa • Thursday, Oct. 16		
Time	**Title**	**Main Author**
1:00pm - 1:20pm	Enhancing a Moving Target Defense Solution for IoT Agents with Task Distribution – PID# 2025003341	**Augusto Morales** Endpoint Security,Check Point Software Technologies Ltd, United States
1:20pm - 1:40pm	AI-Powered IoT Security: Multi-Dataset Evaluation of a Deep Learning Intrusion Detection Framework – PID# 2025003649	**Salahaldeen Duraibi** Electrical and Electronics Engineering, College of Engineering and Computer Science, Jazan University, Jazan, Saudi Arabia
1:40pm - 2:00pm	Adaptive Dual-Agent Authentication Framework: Balancing Security and User Experience in Digital Banking – PID# 2025003366	**Akshay Mittal** Department of Computer and Information Sciences, University of the Cumberlands, United States
2:00pm - 2:20pm	Securing Next-Generation IoT: An Integrated Security Framework with AI, Blockchain, and Edge Computing – PID# 2025003365	**Akshay Mittal** Department of Computer and Information Sciences, University of the Cumberlands, United States
2:20pm - 2:40pm	Cybersecurity in Smart Transit Infrastructure: A Meta-Review of Technical and Socio-Organizational Gaps – PID# 2025003457	**Gahangir Hossain** Data Science, University of North Texas, United States
2:40pm - 3:00pm	Autonomous UAS Object Avoidance and Path Detection Using Neuromorphic Computing – PID# 2025003448	**Brian Millikan** Defense & Intelligence Solutions Division, Southwest Research Institute, United States

Paper Session 7 (6) • Emerging Technologies • Moderator: : Harika Rama Tulasi Karatapu Thursday, Oct. 16		
Time	**Title**	**Main Author**
3:30pm - 3:50pm	Co-reference Pattern-aware Intelligent Text Watermarking Scheme for Forensic Identification via DL – PID# 2025003475	**Akhil Vaitla Janardhan** Independent Researcher, United States
3:50pm - 4:10pm	Spiking Neural Networks for RF Signal Classification and Unified Timing Estimation on Loihi 2 – PID# 2025003452	**Howard Yanxon** Tactical Aerospace Department, Southwest Research Institute, United States
4:10pm - 4:30pm	The Role of Psychoeducation for Stress Reduction in Security Management - the Case Study of the Pompeii Archaeological Park – PID# 2025003375	**Fabio Garzia** DICMA, SAPIENZA - University of Rome, Italy
4:30pm - 4:50pm	A New Hybrid Steganographic Technique for MP3 file – PID# 2025003376	**Fabio Garzia** DICMA, SAPIENZA - University of Rome, Italy
4:50pm - 5:10pm	AI-Driven Digital Twin Framework for Security Threat Simulation and Compliance Optimization – PID# 2025003372	**Vivek Venkatesan** Independent Researcher, United States
5:10pm - 5:30pm	Exposing and Mitigating Adversarial AI Threats in IoT or 5G Intrusion Detection Systems Using Random Forest and Feature Reduction – PID# 2025002514	**Harika Rama Tulasi Karatapu** Network Specialist, Customer Engineer, Google LLC, United States

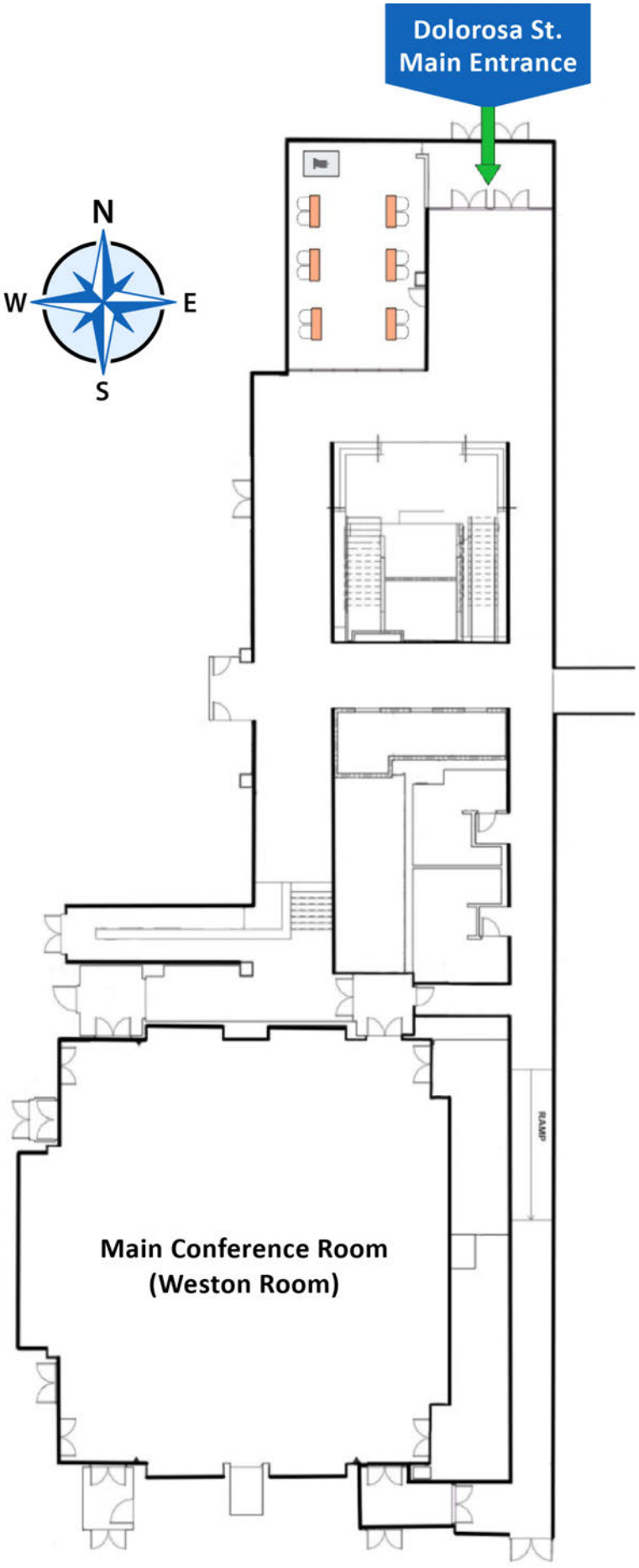
Paper Session 8 (3) • Biometric/Behavior-based Security – Part 1 • Moderator: Abhilash Trehan Friday, Oct. 17		
Time	**Title**	**Main Author**
9:20am - 9:40am	The role of velocity in online signature verification: security concerns – PID# 2025003278	**Cristian Rodriguez** Instituto Universitario para el Desarrollo Tecnologico y la Innovacion en Comunicaciones, Universidad de Las Palmas de Gran Canaria, Spain
9:40am - 10:00am	Machine Learning for Digital Signatures – PID# 2025003336	**Juan Couder** Department of Electrical Engineering and Computer Science, Embry-Riddle Aeronautical University, United States
10:00am - 10:20am	Is one view enough? - Biomatter threat identification in 3D CT scans – PID# 2025003494	**Ivan Koptev** Department of Engineering Science and Biomedical Engineering, The University of Auckland, New Zealand

Paper Session 9 (4) • Biometric/Behavior-based Security – Part 2 • Moderator: Abhilash Trehan Friday, Oct. 17		
Time	**Title**	**Main Author**
10:40am - 11:00am	Knowledge, mental models, and trust regarding AI for baggage screening – PID# 2025003412	**Giulio Staufer** School of Applied Psychology, University of Applied Sciences Northwestern Switzerland (FHNW), Switzerland
11:00am - 11:20am	A New Fairness Evaluation Metric of Biometric Systems Based on the Theil Inequality – PID# 2025003598	**Kaira Neily Sanon** University of Normandy, France
11:20am - 11:40am	Explainable AI(XAI) for Touch-Stroke Biometrics: Insights from SHAP – PID# 2025003353	**Soodamani Ramalingam** School of Physics, Engineering and Computer Science, University of Hertfordshire, United Kingdom
11:40am - 12:00pm	Studying the Generalized Coordinates and Torques in On-line Signature Verification – PID# 2025003272	**Moises Diaz** Physics Department, Universidad de Las Palmas de Gran Canaria, Spain

Paper Session 10 (6) • Applied Technologies – Part 1 • Moderator: Vishal Gudhka • Friday, Oct. 17		
Time	**Title**	**Main Author**
1:00pm - 1:20pm	Hard-Earned Lessons in Access Control at Scale: Enforcing Identity and Policy Across Trust Boundaries with Reverse Proxies and mTLS – PID# 2025003268	**Sanjay Singh** Engineering, LinkedIn Corporation, United States
1:20pm - 1:40pm	Zero Trust and Cyber Risk Modelling for Intelligent School Transportation Systems (ISTS) – PID# 2025003454	**Gahangir Hossain** Data Science, University of North Texas, United States
1:40pm - 2:00pm	Feature Analysis of All Email Components for Phishing Detection – PID# 2025003360	**Tsafack Armand Florent** Téïcée company,France
2:00pm - 2:20pm	The Public Chatter Bureau - A Framework for Cyber Threat Early Detection and Triage – PID# 2025003459	**Dippu Kumar Singh** Application Services, Fujitsu North America Inc., United States
2:20pm - 2:40pm	The Evolution of Secure Access Service Edge in the Digital Landscape: Comprehensive Literature Review – PID# 2025003622	**Vishal Gudhka** Senior Network Architect, Versa Networks, United States
2:40pm - 3:00pm	Logic Locking for Protecting Sensitive Microelectronics: Perspective and Analysis – PID# 2025003348	**Jonathan Cruz** Systems Security Research, Sandia National Laboratories, United States

Paper Session 11 (3) • Applied Technologies – Part 2 • Moderator: Vishal Gudhka • Friday, Oct. 17		
Time	**Title**	**Main Author**
3:30pm - 3:50pm	A Strategic Position on Multi-Agent AI Systems for Secure and Scalable Retail Fraud Detection – PID# 2025003468	**Ananya Ghosh Chowdhury** Independent Researcher, United States
3:50pm - 4:10pm	FedScam-NBD: Federated Learning for Network Behavior-Driven Telecommunication Scam Detection – PID# 2025003282	**Tahir Ekin** Information Systems and Analytics, Texas State University, United States
4:10pm - 4:30pm	Exploring the Integration of Edge AI into 5G Networks: Implications for Efficiency, Security, and Privacy – PID# 2025003493	**Mehek Hasnat** Computer Science, Rowan University (Glassboro), United States

UTSA SCHOOL OF DATA SCIENCE SITE MAP



2025 ICCST Executive Committee

Adrian Schwaninger, Switzerland	Martin Hromada, Slovakia
Michael Coole, Australia	Brian G. Rich, Canada
Miguel Angel Ferrer, Spain	Daniel A. Pritchard, USA
Milos Klima, Czech Republic	Fabio Garzia, Italy
Harika Karatapu, USA	Francisco Vargas, Colombia
Shufei He, Netherlands	Gordon L. Thomas, UK, (Chair)
Soodamani Ramalingam, UK	Han Lin, USA
Virginia Espinosa-Duró, Spain	Jack Glover, USA
William R. Claycomb, USA	Yen Hsyang Chu, Taiwan, ROC