ACM / EHC Tech Talk *sponsored by ACRC*
Sandia's Digital Assurance for High Consequence Systems (DAHCS)
The digital foundations and security consequences of modern integrated systems

When: Wednesday April 24th 2024, 5:00 – 6:00 PM
Where: Presenting in-person only in the CSSE Seminar Room (Shelby 3129)
Registration: To ensure sufficient seats, food, and beverages, registration is free but mandatory by 11:59 PM CDT on Monday April 22nd using the link: https://aub.ie/ACM-SNL

Abstract: The state-of-the-art in digital assurance falls far short of what's needed to enable decision makers (e.g., system designers, developers, hardware engineers) to make confident, evidence-based trade-offs that consider mission engineering requirements against current and future digital threats. Transformational solutions (technologies, modeling, analysis, theories, workflows, state space abstraction) are needed to enable provably secure systems and secure integration of untrusted products, intelligent threat mitigation, and informed engineering trade-offs, ensuring that existing and future high-consequence systems (HCS) meet functionality, reliability, and security requirements throughout their lifecycle (design, implementation, maintenance, and retirement).

Orders of magnitude improvement over today's ad hoc, slow, costly, specialized, expertise reliant solutions are needed through revolutionary new development, analysis, verification and validation (V&V), or test and evaluation (T&E) methods. Research challenges include (a) scalable behavioral analysis of HCS, (b) explicitly modeling, reasoning about, inferring constraints on, and bounding uncertainty, including threats, and (c) effectively tailoring and combining digital systems understanding, cyber assured and secure designs for integration into systems engineering workflows.

This talk will explore a framework for thinking about open questions in the technical foundations for understanding digital system behavior in the face of threats, using evidence, abstractions, modeling, and system composition to make reasonable claims about a system's digital assurance.

Short Bios:

Michelle (Shelley) Leger is a Distinguished Member of the Technical Staff at Sandia National Laboratories, where she's worked for approximately 20 years. Shelley received her BS and MEng in Electrical Engineering and Computer Science from MIT in 2004, researching automated code parallelization for multi-core architectures. Since graduating, Shelley has supported the National Security communities in reverse engineering and software systems vulnerability assessments, generally creating automated program analysis to support national security mission needs. Focus domains include firmware, malware, specialized architectures, and

compilers; techniques include symbolic execution, abstract interpretation, and manual scripting. Her work includes developing frameworks for evaluating syntactic and behavioral signatures. Over the past eight years, Shelley has worked with the Rapid Analysis of Mission Software Systems (RAMSeS) effort at Sandia, focusing on effectively integrating human analysts and automation in binary software analysis systems. Shelley has recently become the Technical Lead for Sandia's Digital Assurance for High Consequence Systems (DAHCS) Mission Campaign.

Will Zortman is the Digital Assurance for High Consequence Systems (DAHCS) Campaign Manager for Sandia National Laboratories' Laboratory Directed Research and Development Office. The DAHCS Mission Campaign is fundamental and developmental research focused on integrating digital assurance into the discipline of systems engineering so that systems engineers, program managers and risk acceptors can make engineering trade-offs between digital risk and other system risks.

He began his career as an Air Force Combat Weather Officer which included assignments leading a detachment at the Army's First Special Forces Group (Airborne) and a special operations weather team at the Air Force's 16th Special Operations Wing. Upon leaving the military Will led a security contracting activity providing tactical training to intelligence agencies.

Will moved into the semiconductor industry as a product change engineer at Lam Research Corporation where he was responsible for integrating design changes on etch and chemical mechanical planarization tools. He transitioned to diffusion engineer and later a defect analysis engineer at Intel Corporation where he pioneered AutoTracer, an automated defect response tool. Will left Intel to consult on the semiconductor industry for various hedge funds.

His career at Sandia began in integrated photonics designing state of the art photonics including devices for focal plane array communications, high performance computing interconnect and spread spectrum technologies. Will later transitioned to Sandia's Threat Intelligence Center where had leadership roles in supply chain security for the Air Force, the anti-tamper program and integrating cyber security into the nuclear deterrence mission. During that time, he authored guides for the acquisition of security devices.

Will volunteers as a Wilderness Emergency Medical Technician (W-EMT) on Albuquerque Mountain Rescue Council (AMRC).

A former adjunct professor at the University of New Mexico Department of Electrical Engineering, an author on more than 50 peer reviewed publications, Will has served on multiple IEEE committees and is the author of 14 patents that have been licensed to semiconductor manufacturers. He has a Bachelors in Atmospheric Science from the University of Arizona and a PhD with distinction in Electrical Engineering from the University of New Mexico with joint advisement from the Massachusetts Institute of Technology.