**Exploiting the Algorithm**

**Offensive and Adversarial AI Research at the Cybersecurity Frontier**

Srinivas Mukkamala PhD

Software runs the world—from healthcare to critical infrastructure, it’s the backbone of modern life, fueling productivity and innovation. But with every line of code, we expand the attack surface for malicious actors, creating vulnerabilities that threaten our digital foundation.

Enter AI: a double-edged sword in this battle. Unlike humans, AI systems learn without the constraints of norms or values, devising novel attacks—like model poisoning or evasion—that we’d never imagine. This isn’t just a technical challenge; it’s a paradigm shift. In our rush for data-driven AI and machine learning, we’ve overlooked a critical truth: we’re still the ones feeding these machines. What emerges—whether through mistake, ignorance, or malice—reflects what we enable.

As an industry, we’re obsessed with gathering more data, but we’ve neglected the processes to ensure it’s the right data, collected and used responsibly. Quality, trusted data is the lifeblood of AI systems, yet bad, distorted, or incomplete data can amplify false positives, erode trust, and open doors for attackers to exploit AI vulnerabilities. We’re not at a point where machines can match human nuance in detecting threats, which means the people behind the data—our analysts, our teams—must be protected and empowered.

Software runs the world but expands attack surfaces. AI’s unconstrained learning creates novel threats, amplified by flawed data. This keynote will explore how offensive and adversarial AI research can turn the tide. By harnessing AI to simulate attacks (like those validated by AEV) and exploit its own weaknesses, we can stay ahead of adversaries—whether they’re nation-states or lone actors.

**Biographies**

**Dr. Srinivas Mukkamala**

A strategic, innovative thinker, Dr. Srinivas Mukkamala is a global leader in AI-driven cybersecurity. He founded RiskSense (acquired by Ivanti, 2021), revolutionizing AI-driven risk-based solutions for 88 Fortune 100 firms.

Chief Scientist Mukkamala worked on the CACTUS project for the DoD, analyzing cyber threats and focusing on exploit analysis, which is relevant to Adversarial Exposure Validation (AEV) in validating attack scenarios. Scaled RiskSense and served as Ivanti’s CPO.

Currently, he advises New Mexico's governor on AI/security, sits on the boards of New Mexico Tech, Securin, and El Paso Electric. CACTUS’s emphasis on understanding attack feasibility prefigures AEV’s empirical validation approach, reinforcing Mukkamala’s influence on the field.

**Frantz M. Berthaud, MPH, FACHE**

Frantz M. Berthaud, MPH, FACHE is the Market Director of Oncology for the Hospitals of Providence. He has oversight of the system's operations and strategic vision for oncology. He has over 15 years of experience in the healthcare sector ranging from clinical research to management, education, operations, and strategy. Prior to Frantz joining THOP, he served in several leadership roles at the Dana-Farber Cancer Institute in Boston, MA. Mr. Berthaud is a former Chair of the American College of Healthcare Executives (ACHE) National Early Careerist Committee. Frantz is a member of Boston University School of Public Health's (BUSPH) Health Law Policy and Management Advisory Board and the Alumni Association Board of Directors for Boston College where he received his Bachelor of Arts in Biology and Philosophy. He holds a Master of Public Health from Boston University School of Public Health and was an adjunct faculty member at the school. Frantz is a fellow of the American College of Healthcare Executives.

**J.J. Childress**

J.J. Childress is a leader in economic development, tech policy, and technology enabled community transformation. He is currently a Director at Microsoft, leading the U.S. Philanthropies Western Team and spearheading the TechSpark Initiative in Texas. This transformative program is dedicated to nurturing talent and equipping communities for the opportunities of the 21st century.

J.J. has played a pivotal role in establishing innovation accelerators, broadband access, digital inclusion, computer science education and entrepreneurship programs across the United States and Mexico. As a proud El Paso native, UTEP graduate, serial entrepreneur and investor, J.J. has founded a range of successful businesses, earning him the Small Business Administration's Young Entrepreneur award in 2017.

**Chiagozie (Gozie) Nwabuebo**

Gozie Nwabueb is a senior executive and AI entrepreneur with over 20 years of experience leading strategy, innovation, business development, and social impact across the private and public sectors. He has advised and built trust-based relationships with C-suite leaders across industries including tech, media, finance, healthcare, and government.

Gozie is the Founder and CEO of InnovAI Global, a mission-driven company that builds AI-powered products and strategies to solve global challenges and help organizations grow. He previously led global growth and generative AI commercialization at Visa, where his initiatives helped expand financial inclusion for 20 million women and unlocked $15B in new market opportunities. Prior to that, he held leadership roles at Google, Comcast NBCUniversal, Accenture, and NASA—building social impact initiatives, scaling innovation platforms, and transforming organizations at scale.

A lifelong learner, Gozie holds degrees from Harvard University, NYU Stern, and is currently completing a Master’s in AI Engineering at Johns Hopkins University. He’s also a former USAID DIV Fellow and Clinton Global Initiative Fellow.

**Humberto Mendoza**

Humberto Mendoza currently serves as the Chief of the Cyber Experimentation & Analysis Division (CEAD) under the DEVCOM Analysis Center (DAC). In this role, Mr. Mendoza leads a team of over 80 certified ethical hackers and oversees the execution of cyber vulnerability and resilience analyses for Army Transformation and Readiness Technologies.

Mr. Mendoza earned a Bachelor’s Degree in Computer Science from the University of Texas-El Paso (UTEP) in May 2002 and completed a Master’s in Computer Science with a concentration in Software Engineering in May 2005. Prior to joining the Army as a civilian, Mr. Mendoza gained valuable industry experience, working as an Information Technology Specialist with Raytheon Corporation in Aurora, Colorado, and as a Software Developer for IBM Corporation in Austin, Texas.