Veena Krish

veena.t.krish@gmail.com │ linkedin.com/in/veenakrish │ vkrish1.github.io

I'm a Computer Science PhD candidate at Stony Brook University. Since obtaining my BSE/MSE in Bioengineering, working as a data scientist at a technical consultancy, and co-founding a medical device start-up, I've had a growing interest in the security implications of emerging technologies that leverage machine learning. I am professionally interested in developing safe and responsible AI technologies. My work spans security, formal verification, reinforcement learning, and cyber-physical systems.

ACADEMICS AND RESEARCH

PhD Candidate in Computer Science, Stony Brook University   Stony Brook | Aug 2019 - anticipated Dec 2024
- *Advised by:* Prof. Amir Rahmati, Ethos Security and Privacy lab
- *Graduate Coursework:* GPA 3.91/4.00: Network Security; Computer Security; Machine Learning; Computer Vision; Cyber-Physical Systems; Visualization
- *TA Experience*: Fundamentals of Software Development; Offensive Security
- *Current Research Areas:*
    - Understanding the scope of adversarial threats against algorithms used for decision-making in medical cyber-physical systems
    - Investigating the vulnerability of biometric authentication systems to spoofing attacks synthesized using generative ML and RL frameworks. Target applications include health wearable devices.
    - Evaluating the robustness of neural network controllers trained under reinforcement learning paradigms
- *Leadership and Awards:*
    - Recipient of 2024-2025 Dr. W. Burghardt Turner Fellowship from Stony Brook's Center for Inclusive Education
    - Recipient of 2023-2024 John Marburger III Fellowship for Science, Engineering & Mathematics (one PhD student awarded from all STEM disciplines at Stony Brook per year)
    - President of the Women PhDs affinity group
    - 2021 TA training ambassador for the College of Engineering and Applied Science

BSE/MSE in Bioengineering, University of Pennsylvania   Philadelphia, PA | May 2016
- Graduated *cum laude* and awarded a Littlejohn Fellowship for undergraduate research in the Litt Translational Neuroengineering Lab
- Submatriculated into the Master's program in Bioengineering, where I transitioned my senior undergrad design project into a startup through an accelerator program within the Penn Center for Innovation
- Spent a semester abroad at the National University of Singapore

PROFESSIONAL EXPERIENCE

Software Engineering Intern, Snowflake   Bellevue,WA | Summer 2024
- Summer internship in the Produce Security team, helping build tools to augment software security scans (AppSec for third-party applications submitted to the public marketplace)

Medical Device Security Intern, Harbor Labs   Pikesville, MD | Summer 2023
- Summer internship comprising threat assessments and penetration testing of medical devices (e.g. infusion pumps, insulin delivery systems) in advance of FDA filing
- Experience with STRIDEs and testing system designs including network protocols, bluetooth communication

R&D Research Intern, General Motors   Warren, MI (remote) | Summer 2022
- Summer internship within the Perception, Planning and Decision Systems group, focused on improving the performance of vision models for use in autonomous driving
- Designed and implemented a method for adversarially training a large self-supervised segmentation model

Summer Research Intern, Air Force Research Laboratory   Wright-Patterson AFB, OH (remote) | Summer 2021
- Summer intern within the Safe Autonomy group on the Autonomy Capability Team (Sensor Directorate), where I studied the robustness of neural network controllers designed for a series of reinforcement learning benchmarks

Data Scientist Consultant, Tessella Inc   Needham, MA | 2016 - 2019

Data scientist for healthcare-focused analytics consulting services firm; selected project history:

- Implemented bayesian statistical models for a large pharmaceutical company to quantify the "Go/No-Go" decision used to continue or terminate a clinical trial (WPF, C#, .NET)
- Developed a LIMS application to track biomarkers for a biotech company (full-stack: Postgres, Java API, Aurelia JS, AWS-hosted)
- Conducted exploratory data science and visualization projects across industries (major chemical and energy companies)

Co-Founder, Shock Analytics LLC   2016-2019

- Startup focused on detecting early sepsis via noninvasive measurement of systemic vascular resistance
- Idea accepted into the DevelUPmed startup accelerator at the University of Pennsylvania
- Designed a machine learning system on time-series pulse waveforms; built the initial prototype and developed software for data collection

PUBLICATIONS/PATENTS

- **Krish V,** Paoletti N, Kazemi M, Smolka S, Rahmati A. *Biosignal Authentication Considered Harmful Today*. USENIX Security 2024
- Chang P, **Krish V**, Rahmati A. *Security Analysis of RL-Based Artificial Pancreas Systems*. Cybersecurity in Healthcare (HealthSec) workshop at ACM CCS 2024
- Bak S, Bogomolov S, Hekal A, **Krish V**, Mata A, Rahmati A. *Zero-One Attack: Degrading Closed-Loop Neural Network Control Systems using State-Time Perturbations*. ICCPS 2024
- **Krish V,** Mata A, Hobbs K, Bak S, Rahmati A. *Provable Observation Noise Robustness for Neural Network Control Systems*. Cambridge Research Directions: Cyber-Physical Systems 2023
- **Krish V**, Paoletti N, Smolka SA, Rahmati, A. *Synthesizing Pareto-Optimal Stealthy and Effective Signal-Injection Attacks on ICDs*. IEEE Access. 2022
- Vaishnavi P, **Krish V**, Ahmed F, Eykholt K, Rahmati A. *On the Feasibility of Compressing Certifiably Robust Neural Networks*. Trustworthy and Socially Responsible Machine Learning workshop at NeurIPS 2022
- Azarion AA, Wu J, Davis KA, Pearce A, **Krish V**, Wagenaar J, Chen W, Zheng Y, Wang H, Lucas TH, Litt B, Gee JC. *An open-source automated platform for three-dimensional visualization of subdural electrodes using CT-MRI coregistration*. Epilepsia 2014
- Patent WO2017173284A1 2016: *Methods, Systems, and Computer Readable Media for Measuring Systemic Vascular Resistance*

PERSONAL

- US Citizen, Native English speaker
- Graduated with high school diploma from Hopkins School in New Haven, Connecticut
- Interests: Piano and guitar, Fencing (high school), DIY SmartThings, Mentorship for girls/women in tech (Girls Who Code, Grace Hopper Conference)