Muhammad Danish

Albuquerque, NM | mdanish@unm.edu | (505) 219-6410 | mdanish.net

Education

University of New Mexico — Albuquerque, NM

- Ph.D. in Computer Science — Aug 2025 – May 2028
- M.S. in Computer Science — Aug 2025 – Jul 2026
- B.S. in Computer Science; Minor in Honors Interdisciplinary Liberal Arts — Aug 2021 – May 2025

Research & Publications

1. **Danish, M.**, et al. "**The Tragedy of Convenience: Cascading User-Data Leakage from SMS-Delivered URLs**." *ACM Conference on Computer and Communications Security (CCS)*, 2026.
   Led a large-scale study of 33M+ SMS messages and 322K URLs; built an end-to-end LLM-assisted pipeline to identify 170+ PII-exposing services; Performed token-entropy analysis, bounded enumeration, authentication testing, API and WebSocket analysis, and coordinated disclosure with remediations protecting 120M+ users.
2. Sobrados, E., **Danish, M.**, et al. "**Exposing Probe-Resistant VPNs via Protocol Coexistence**." *IEEE Symposium on Security and Privacy (SP)*, 2027.
   Developed an Internet-measurement pipeline that reverse-engineered commercial VPN applications and enumerated 72,887 servers; found that 83.4% were fingerprintable because probe-resistant protocols coexisted with detectable legacy or misconfigured protocols.
3. **Danish, M.**, et al. "**View-Based Monetization Fraud Across Content-Sharing Platforms**." (Submitted)
   Led a cross-platform study of view inflation across a diverse set of monetizable content-sharing services (e.g., Spotify, Dailymotion, Ameblo); 9 of 10 platforms counted more than 80% of attempted views and attacks on five platforms persisted & scaled using consumer-grade infrastructure;
4. **Danish, M.**, et al. "**A Cross-Attack Security and Privacy Evaluation of Model Compression**." (Submitted)
   Systematically evaluating how quantization, pruning, knowledge distillation, low-rank factorization, and hybrid compression affect model security and privacy across evasion, poisoning, and privacy attacks under varying compression levels, datasets, and architectures.
5. **Danish, M.**, et al. "**Robustness and Security of Embedded Edge AI for Space Systems**." (In Progress)
   Evaluating deployment and security of AI models across FPGA-based and GPU-based edge platforms across space-specific threats such as radiation-induced faults, adversarial fault injection, resource exhaustion, and model corruption under constrained operating conditions.

Experience

- **Research Assistant (PI and Reference: Afsah Anwar), University of New Mexico** — Dec 2023 – Present
  - Conducted large-scale AI, security & privacy research, resulting in multiple publications.
  - Built end-to-end pipelines and reverse-engineered AI/web/mobile systems to uncover vulnerabilities.
  - Characterized security & privacy issues in multiple systems (e.g., web, AI/ML) and proposed mitigation strategies.
- **Student Programming Analyst, University of New Mexico** — Oct 2022 – Aug 2025
  - Automated cross-department administrative workflows using Microsoft Power Platform, Power Automate, and Boomi.
  - Built regression-test suites and integrated them into Azure DevOps CI/CD pipelines, reducing testing time by ∼50%.
  - Delivered web applications and system integrations across multiple departments, supporting 20,000+ students.
- **Computer Science Teaching Assistant, University of New Mexico**
  - Led weekly programming, networking, and security labs for 40+ students.
  - Developed exercises, graded assignments and examinations, and provided individualized technical feedback.
  - Fostered a collaborative learning environment via group discussions, one-on-one sessions, and YouTube.
  - **Courses**: Introduction to Cybersecurity, Computer Networks, and Intro/Intermediate Programming

Skills

- **Languages:** Python (PyTorch and TensorFlow), Bash, PowerShell, Java, JavaScript, SQL, MATLAB
- **Technical:** adversarial ML, LLMs, agentic AI, model compression, web & API security, reverse engineering
- **Tools:** Linux/Windows, Playwright, Docker, NMap, Wireshark, Burp Suite, Kibana, Metasploit, Azure, Git

Awards, Media, and Volunteering

- **Awards:** CRA Outstanding Undergraduate Researcher (North America), NMEF Scholar (New Mexico), Bug Bounty
- **Media:** Research featured by Ars Technica, TechRadar Pro, Help Net Security, Azerbaijan CERT, and the UK NCSC CTO; invited guest on N2K CyberWire Research Saturday; profiled by CRA Computing Research News.
- **Peer Review:** AEC member at top conferences e.g., IEEE S&P (Award), ACM CCS, NDSS, PETS (Award)
- **Stanford Code in Place (Section Leader):** Mentored diverse students in Python and CS fundamentals.