Multiple PhD Student Positions in Systems and Security — CactiLab, Khoury College of Computer Sciences, Northeastern University

The CyberspACe securiTy and forensIcs lab (CactiLab) at Northeastern University is seeking PhD students with a strong interest in systems and security, particularly in ML/LLM systems, software and hardware security, and machine learning security, to join in Fall 2026. Students from disciplines such as Computer Science, Computer Engineering, Electrical Engineering, Software Engineering, or other related fields are encouraged to apply. Northeastern University (NEU) is a private research university in Boston, Massachusetts, USA. NEU's computer science research is highly ranked at 12th in the country and 17th in the world by CSRankings, with its computer security research ranked among the top 6 in the country and top 8 in the world.

Prof. Ziming Zhao, an Associate Professor at the Khoury College of Computer Sciences, leads the CactiLab. CactiLab's research outcomes have appeared in IEEE S&P, USENIX Security, ACM CCS, NDSS, ACM MobiSys, ACM/IEEE DAC, IEEE RTAS, ACM TISSEC/TOPS, IEEE TDSC, IEEE TIFS, etc. Additionally, their research has received best/distinguished paper awards from several prestigious conferences, including USENIX Security 2019, ACM AsiaCCS 2022, ACM CODASPY 2014, and ITU Kaleidoscope 2016. Their research also received the Test-of-Time paper award at ACM SACMAT 2024. CactiLab's research has been supported by the U.S. National Science Foundation (NSF), the U.S. Department of Defense, the U.S. Air Force Office of Scientific Research, the U.S. National Centers of Academic Excellence in Cybersecurity (part of the National Security Agency), and two Amazon Research Awards. Ziming is a recipient of an NSF CAREER award and an NSF CRII award. Ziming is also an associate chair at IEEE S&P 2026.

PhD students at the Khoury College of Computer Sciences receive a stipend of $51,000 for a 12-month appointment. Self-motivated students with strong programming/hacking skills and a solid background in any of the following research areas are an excellent fit for the CactiLab:

- Operating systems and hypervisors, e.g., Linux kernel, KVM
- Computer architecture, e.g., ARM Cortex-A/M, RISC-V, GPU, TPU
- Systems for machine learning and large language models (LLM systems)
- System and hardware security, e.g., Linux kernel security, side-channel defenses, hardware fault injection (glitching)
- Confidential computing and trusted execution, e.g., ARM CCA, TrustZone
- Program analysis and compilers, e.g., LLVM
- Machine learning and deep learning security

Please feel free to send your application package (CV, transcript, papers, open source projects, or/and anything else you feel may increase your chances) to Ziming at z.zhao@northeastern.edu.