Prateek Sahu
+1-737-207-2578
prateeks@utexas.edu

To
Hiring Committee

I am a doctoral candidate at University of Texas at Austin advised by Dr. Mohit Tiwari. My work centers on designing efficient, scalable systems security solutions that span the hardware-software stack, with the goal of translating deep technical insights into practical, deployable defenses.

As part of my doctoral thesis, I have investigated microarchitectural side-channel attacks and detection mechanisms, as well as cross-layer approaches that leverage system-wide signals to detect sophisticated software layer threats such as ransomware. This cross-stack perspective is motivated by the recognition that modern attacks rarely occur in isolation; instead, they emerge from subtle interactions across components. I have published in leading architecture venues such as MICRO and ASPLOS, and have ongoing work under submission to top security conferences.

Rapid integration of AI agents and language models into everyday life introduces a new class of security challenges. I am excited to bring my systems and hardware security expertise to emerging threats in AI applications and at-scale user platforms. Recently, I have examined vulnerabilities in modern AI inference pipelines, focusing on how system- and hardware-level weaknesses can amplify algorithmic attacks such as membership inference and prompt injection. The current industry trends around AI integration is particualrly interesting avenues for me as it addresses advanced threats of growing concern to industry while allowing me to extend my prior work on runtime ransomware and side-channel detection into the AI security domain.

Thank you for your time and consideration. I would welcome the opportunity to discuss how my background and research vision align with your team's goals.

Prateek Sahu

Research Outputs: https://prateeksahu.github.io/publications.html