I am currently a Ph.D. candidate in Computer Science at the University of South Florida, and my research focuses on cybersecurity, privacy, and AI security. My interest in information security began with studying vulnerabilities in shared computing environments, where I investigated how seemingly harmless system information could be used to infer sensitive data. This experience led me to a question that continues to motivate my research: even when sensitive content is protected, what information can an attacker still learn from the surrounding system or communication behavior?

Much of my current research explores this question through network traffic analysis and privacy. I study website fingerprinting, where an adversary attempts to identify a user's online activity from encrypted network traffic without decrypting its content. My work examines both attacks and defenses, including how machine learning can improve traffic analysis and how privacy defenses can remain effective against adaptive attackers. I have also studied Wi-Fi fingerprinting for device localization and tracking in public environments. More recently, I have begun investigating privacy leakage from LLMs and AI agents, particularly whether encrypted traffic patterns can reveal characteristics of user prompts, identify models or agents, or expose interaction behaviors. Through these projects, my primary interests have developed around network security, privacy, traffic analysis, adversarial machine learning, and emerging AI security problems.

After completing my Ph.D., I plan to pursue a research-oriented career in cybersecurity and AI security, either in academia or an industrial research lab. I hope to continue investigating security and privacy problems that emerge as networked and AI systems become more capable and widely deployed. My long-term goal is to develop security research that not only identifies new threats but also leads to practical defenses that can improve the privacy and security of real-world systems.

Attending ACSAC 2026 would give me a valuable opportunity to communicate with researchers and practitioners from different areas of cybersecurity and learn from their experiences and perspectives. I look forward to discussing research ideas, learning about new security challenges and approaches, and receiving insights from researchers outside my immediate area. These interactions would help me broaden my understanding of cybersecurity and discover new research directions, particularly as I approach the completion of my Ph.D. I am especially interested in learning about recent work in network security, privacy, side channels, and AI security, as well as building connections with researchers who share similar interests. In addition, our paper, “Exploiting Wi-Fi Fingerprints for Practical Device Localization and Tracking in Public Environments,” has been accepted to ACSAC 2026. Presenting this work will give me the opportunity to share our findings with the community, receive constructive feedback, and discuss how our research can be improved and extended in future work.

The Student Conferenceship would make it more feasible for me to participate fully in ACSAC by helping with conference and travel expenses that are difficult for me to cover as a graduate student. I understand that the purpose of the Conferenceship is to enable students who might otherwise have difficulty attending, rather than simply recognize research merit. I will pursue available support from other sources and would use Conferenceship funding only for expenses that cannot be covered elsewhere. Receiving this support would allow me to take full advantage of ACSAC as both an author and a student researcher. I hope to contribute my own work to the conference while learning from the broader cybersecurity community and building connections that will support my continued development as a security researcher.