Conferenceship Narrative Statement

Zhaohui Wang
University of Kansas

My work in information security is driven by a simple goal: to solve problems that matter in everyday life. As smart devices are part of our daily lives, cross-app threats, privacy leaks, and low-level vulnerabilities aren't just technical puzzles, they affect people's safety and trust.

My research has focused on making smart-home platforms safer and more trustworthy. I developed a framework called *InteractionShield*, which leverages event relations to detect and resolve rule conflicts that could otherwise lead to unsafe behaviors. Alongside the framework, I built a GUI that integrates real-world environmental factors, helping users better understand risks in practical contexts. I'm excited that this work, *InteractionShield: Harnessing Event Relations for Interaction Threat Detection and Resolution in Smart Homes* has been accepted to *ACSAC 2025*, and I plan to attend the conference to present it. I'm grateful for the opportunity to share this work and exchange ideas on improving the security of smart-home platforms.

Before this project, I worked on two other research efforts in smart home security. I investigated the security challenges of IoT apps. Due to the rapid growth of SmartApps and the retirement of older ones, the existing datasets had become outdated, leaving the research community in need of a new, large-scale and carefully curated benchmarking dataset. To address this gap, I created *SmartAppZoo*, a large-scale repository of SmartApps, which was published at *IoTDI 2023*. Next, I developed *PrivacyGuard*, a framework that explored a new type of privacy threat arising from cross-app chains built among multiple seemingly benign IoT apps. By formalizing cross-app chaining, inferring device profiles, and quantifying both direct and implicit risks, supported by a visualization tool to aid user decision-making, I uncovered previously hidden cross-app privacy leakage threats. This work was published at *PETS 2025*.

These projects highlight my dedication to research that is careful and useful in practice. I aim to move beyond theory and deliver tools that others can directly use. For example, I design GUIs that allow researchers and developers to perform complex threat detection with minimal effort. I also follow open-science principles, releasing artifacts, datasets, source code, and documentation so that others can reproduce results, build upon them, and deploy the tools in real-world settings. Beyond IoT, I have also explored broader areas of systems security, including Rowhammer-based memory attacks and kernel exploitation. Each project has deepened my technical expertise and reinforced my motivation to continue pursuing this line of work.

Attending *ACSAC* is more than a paper presentation for me. It's a chance to meet leading researchers, listen, learn, and grow. I'm eager for conversations that challenge my assumptions, feedback that sharpens my methods, and collaborations that increase the impact of my work. Sharing my research with this audience is both a Ph.D. milestone and a personal point of pride. However, I have already exhausted my eligibility for the university's travel fund by attending *PETS 2025* in Washington, D.C., in July 2025. Due to the limited research funds available from my advisor, I am unable to receive sufficient support for additional travel. Therefore, external travel grant support is essential for me to participate in this conference.

Looking ahead, I want to build a career in security research, whether in academia or an industry lab, so I can keep publishing useful work and help secure real-world systems. A Conferenceship would let me fully attend *ACSAC 2025*, and I'm excited to bring back the insights, connections, and inspiration that will shape my next steps as both a researcher and a member of this community.