Tuesday, May 6, 2025
1:10 pm – 1:30 pm
RAVID (Randomized Automated Virtual Infrastructure Defense) - An end-to-end Automated, Stealth, Moving Target Defense Architecture

Harris Nussbaum
Tyto Athene, LLC

Abstract:
RAVID addresses the pressing challenge of outdated, static cybersecurity infrastructures that expose organizations to predictable and exploitable threats. Traditional models rely on fixed endpoints and constant network configurations, making it easier for adversaries to detect, target, and breach critical systems. Inspired by historical shifts in military strategy—from stationary defenses to agile, stealth-enabled operations—RAVID redefines cyber defense by emphasizing mobility and dynamic obfuscation across the entire digital landscape.

At its core, RAVID implements a multi-layered Adaptive Moving Target Defense (AMTD) strategy that continuously reorients network pathways, infrastructure, and applications. This approach leverages stealth networking techniques—such as rotating network routes, decoupling control and data planes, and eliminating static IP addresses—to transform the network from a vulnerable threat plane into an active shield. Additionally, orchestrated API-driven failover mechanisms ensure that endpoints and virtualized storage are not fixed targets but are dynamically repositioned to preempt adversarial attacks.

By integrating cost-effective commercial and open-source tools, RAVID not only extends the lifespan of legacy systems but also creates a resilient, self-healing infrastructure. This proactive defense model drastically reduces the attack surface and minimizes the window of opportunity for cyber threats. In doing so, RAVID sets a new standard for cybersecurity—one where continuous adaptation and stealth are central to maintaining a robust defense in the face of an ever-evolving threat landscape.