Title: Expert Insights into Advanced Persistent Threats: Analysis, Attribution, and Challenges

Authors: Aakanksha Saha, *Technische Universität Wien;* James Mattei, *Tufts University;* Jorge Blasco, *Universidad Politécnica de Madrid;* Lorenzo Cavallaro, *University College London;* Daniel Votipka, *Tufts University;* Martina Lindorfer, *Technische Universität Wien*

Venue: 34th USENIX Security Symposium, August 13–15, 2025

Paper Link: https://www.usenix.org/conference/usenixsecurity25/presentation/saha

Abstract: Advanced Persistent Threats (APTs) are sophisticated and targeted threats that demand significant effort from analysts for detection and attribution. Researchers have developed various techniques to support these efforts. However, security practitioners' perceptions and challenges in analyzing APT-level threats are not yet well understood. To address this gap, we conducted semi-structured interviews with 15 security practitioners across diverse roles and expertise. From the interview responses, we identify a three-layer approach to APT attribution, each having its own goals and challenges. We find that practitioners typically prioritize understanding the adversary's tactics, techniques, procedures (TTPs), and motivations over identifying the specific entity behind an attack. We also find challenges in existing tools and processes mostly stemming from their inability to handle diverse and complex data and issues with both internal and external collaboration. Based on these findings, we provide four recommendations for improving attribution approaches and discuss how these improvements can address the identified challenges.