Abstract for Philip Brown

The growing adoption of zero-trust architectures brings the principle of complete mediation to the forefront of well-designed, secure systems. Despite the potential for zero-trust to improve the security and resilience of systems from cyberattack, practical adoption of these architectures is hindered by lack of sufficiently trustworthy origin authentication within untrusted networks such as the Internet. Notably, problems with authentication exist due to stolen credentials and mobile clients used by remote workers that are easier for threats to compromise than traditional workstations hiding behind boundary firewalls. The result is that access control for the protection of critical assets increasingly depends not just on user authentication but also on context-sensitive techniques, e.g., behavior and location, to monitor and isolate such threats.

In this talk, we introduce path-aware risk scores for access control (PARSAC), a novel context-sensitive technique to enrich access requests with risk scoring of the path taken by those requests between the authenticated user and the resources they access. These path-aware risk scores enable another layer of security for traditional access control systems that addresses the need for fine-grained monitoring and enforcement within a zero-trust architecture. We define rules for general functions that can be used to determine risk and instantiate a specific approach to calculate path risk scores. We have evaluated our approach with realistic network graphs and discovered that PARSAC finds more paths with lower risk when compared with traditional routing algorithms that select the shortest path.