Riverside: Dynamic Visualization of Network Traffic for Situation Awareness in Computer Security

Authors: Kaitlyn DeValk, Niklas Elmqvist

Summary:

Monitoring security in a computer network requires understanding both real-time network traffic as well as the evolving structure of the network itself. While visualization is increasingly being used for this purpose, current network security tools rely mostly on static network topology and fail to account for user needs. To better understand this problem domain, we interviewed 24 network and security analysts to gain insight on their practices, needs, and current tooling. Based on their qualitative feedback, we designed and built Riverside, a computer security tool visualizing dynamic network traffic across time. By enabling an analyst to navigate traffic in time, summarize intervals, and highlight specific events to prevent change blindness, Riverside gives network and security professionals increased situation awareness of their network.

ACM Author Affiliations: Kaitlyn DeValk: University of Maryland; Niklas Elmqvist: University of Maryland, College Park