Network Access Log Visualization and Sonfication

Benjamin deButts

As the worldwide web gets larger and larger, the variety and number of network incidents swells alongside it. Security analysts need to be able to detect, analyze, and respond to incidents faster than ever. However, access logs are both extensive and exhaustive in detail. Visualization, a field that bases itself around making clunky, hard-to-decipher data manageable and understandable, is an obvious method of aiding the detection/response process. By visually displaying access logs on an interactive timeline, analysts will be able orient themselves in a notification stream more quickly and efficiently than with other text-based tools. Additionally, by mapping distinct notification sounds to anomalous incidents, analysts will be able to monitor live network streams without constant visual attention. Upon the recognition of an "incident" tone, they will be able to interact with the timeline, spotting the incident and visually reviewing history to unearth more.