RAVE : The Retrospective Analysis and Visualization Engine

Phil Groce
CERT Network Situational Awareness Group

John Prevost
CERT Network Situational Awareness Group

Abstract

As tools for collecting flow data and other network metric information improve, we must more often consider how to present that data to end users for analysis. Existing approaches tightly couple generation of analytical products with the presentation of those products. Unfortunately, this tight coupling forces tradeoffs between analytical power and interface usability.

The Retrospective Analysis and Visualization Environment (RAVE) provides data analysis and visualization capabilities independent of user interface. Applications may interact with RAVE analyses directly: using RAVE as a software library acting on local data, or remotely: communicating with a central server over the network. In both configurations, RAVE caches intermediate and final analytical products for use by multiple applications.

In this paper, we present RAVE as an analysis service provider. We discuss problems we encountered implementing RAVE and a web-based network monitoring interface that uses it. Finally, we identify places where RAVE can be improved and expanded, and ideas for possible enhancements that require further evaluation.