Visual Analytics for Cyber Intelligence Sharing

Abstract

Large repositories of cyber intelligence sources have been built with many terabytes of information. A common use scenario of such information sources is to consume it in an automatic fashion by computers. However, before automation can be built, analysts must examine and understand what is contained in such cyber intelligence sources and make decisions on how they may be used automatically. In addition to knowing the origins of the data along with description of the data format, an essential part of this analysis is to gain a sense of the data contained in the intelligence source, e.g. attack types and distributions, attack sources and distributions, temporal characteristics of the data, and details of information sources (how much descriptive information is provided).

Providing a visual overview of such characteristics of data is an effective way to approach such large data sets. This proposed research is to identify a set of visualization tools that can be used by an analyst to gain a quick sense of the data and decide how to use the data in security operations. Specific design goals include (1) Identify a set of common questions when analyzing cyber intelligence sources that can be effectively answered through visualization. (2) Identify visualizations that are intuitive to understand and easy to use, and (3) Tools must work well with large volumes of data and platforms such data may reside.