Department of Computer Science and Engineering
University of Notre Dame

Visual Exploration and Analysis on Host, Users and Applications in Enterprise Networks

Qi Liao, Dirk VanBruggen, Andrew Blaich and Aaron Striegel

Problem: This work is motivated by a relatively innocuous question: *how well do we know our network*? Although there exists a wide spectrum of security analysis and network visualization toolkits, the tools tend to focus on *where* and how much communication is occurring, not *whom*, *what* and *why* are the communications occurring. With the increasing trend towards distributed systems and the ever changing behavior of users, the *context* of the communications with regards to security and enterprise management rather than packet/flow *content* becomes more important than ever. The dynamic relationships between a rich array of network components such as services, users, applications and data make monitoring and understanding a large enterprise network extremely challenging. As a result, troubleshooting and security analysis devolve into the equivalent of a digital spelunking expedition, frequently overwhelming the network administrator and resulting in considerable lost enterprise productivity or increased security risk.

Solution: We argue that for enterprise networks, knowing end-to-end connections is too coarse to be useful and network addresses and port numbers become less useful identifiers for visualizing network activities. We believe that the inclusion of relatively simple context (users, applications, and data) in addition to host locations coupled with advanced data analysis techniques can shed significant light on the question of *what is really going on in my network*?

To that end, we created *ENAVis* (Enterprise Network Activities Visualization), a graphical tool that brings the notion of local context (*whom*, *what*, *why*) to dramatically improve how administrators view the network. The key innovation of *ENAVis* is to leverage local context to allow the administrator to quickly assess relationships among the hosts, users, and applications using the network. The powerful, yet intuitive interface of *ENAVis* enables administrators to seamlessly browse, assess, debug, and analyze the timelines of activities within the network on the order of seconds, whereas existing tools require hours if such tasks are even possible.

In this poster, we will highlight our ongoing work with *ENAVis* including:

- New *analytical module* that performs intelligent graph analysis and visual mining on the time evolution of the network changes in terms of hosts, users, and applications to provide in-depth knowledge and insight that fill the gap between network monitoring and high level decision making.
- Exploration of various *similarity* measurements of the *HUA* (Hosts, Users, Applications) network connectivity graphs that involve high-dimensional visualization techniques, graph theory, inter-graph and intra-graph clustering and various data mining techniques.
- Exploration of the impact of *files* on visualization, i.e. the *HUAF* control (Hosts, Users, Applications, and Files).

Website: Full demonstration movie of tool walkthrough available at http://netscale.cse.nd.edu/Lockdown