Computers and Information Sciences
Cyber Security

Figure 1: Example of a "SHINI" heat map. The counts (and corresponding colors in the heat chart) represent the number of distinct connections from that country over approximately 60 seconds.

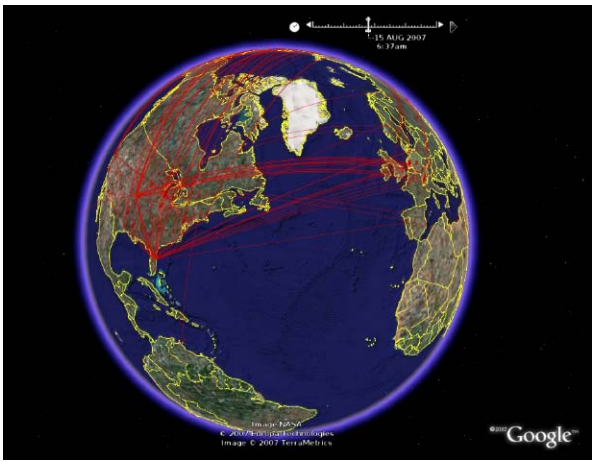

Figure 2: Example of a "SHINI" point map.

Geo-Temporal Visualization of Internet Activity

Student-developed programs help analysts detect trends.

Internet-connected computers are subject to attacks at all hours of the day and night from anywhere in the world. Intrusion detection analysts at Sandia, and their counterparts at other large organizations, need tools that allow them to visually display important information, such as when and where network connections originated, from their enormous security logs (typically measured in gigabytes of data). Such a tool would not only allow analysts to identify cyber attacks not readily apparent at first glance in the logs, but would also easily illustrate the origin of the attacks to a non-technical audience or customer. This is an example of geo-temporal visualization: displaying location and timing information together.

Intrusion detection analysts at Sandia tasked participants from Sandia's Center for Cyber Defenders student intern program to develop a computer program that uses geo-temporal visualization for security log data. Two students came up with an idea that works in conjunction with the popular application "Google Earth" that displays the activity in a variety of forms. This program is called "SHINI" (Sandia Heuristic Intelligent Network Imaging).

One way SHINI can visualize geo-temporal information is called a "heat map," similar to a weather map, where the color of a country is determined by the current number of connections from that country (Figure 1). The heat map can either display real-time log information or display a time-lapse visualization. Using time-lapse visualization, an analyst can view information from a period of days in a matter of minutes.

Another available visualization is a "point map." As shown in Figure 2, each network connection would be represented by a point on the map. When used in conjunction with the capability to link plotted points together, the results look similar to an airline route map. This capability can be extremely useful when logs from different sources are combined. As with heat maps, point maps can display both real-time and time-lapse information.

While the current SHINI program is constructed to accept network logs as input, these programs can be easily modified to accommodate virtually any data files that include time and location information. Thus, SHINI could be used in any number of situations where simple-to-use, real-time and time-lapse geo-temporal visualization can help analysts and investigators.

For more information:

Technical Contact:
Steven Hurd
925-294-1224
sahurd@sandia.gov

Science Matters Contact:
Alan Burns, Ph.D
505-844-9642
aburns@sandia.gov

Sandia National Laboratories

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND 2008-0486P

National Nuclear Security Administration

01/2008