

Friday, September 19, 2008 | Modified: Tuesday, September 23, 2008

Sandia lab tool puts Internet traffic on the map

East Bay Business Times - by [Michael Fitzhugh](#) Staff reporter

Interns at the [Sandia National Laboratories Livermore](#) lab have come up with a way to transform text-based computer security logs, which can run to thousands of lines, into something a little easier on the eyes: Google Earth maps.

The Sandia Heuristic Intelligent Network Imaging tool, SHINI for short, allows computer scientists to visualize connections between computers drawn as lines between points or color-coded “heat maps” on [Google Inc.](#)’s free digital globe software.

“We have lots of tools to show us what we’re looking to find. But there’s always a gap between what analytical tools can show and what reality is. Sometimes you need to look at things from a whole different perspective,” said computer scientist Steve Hurd, who helps mentor the interns behind SHINI: Scott Crawford and Andrew Schran.

The tool was inspired by a summer meeting in which Sandia network security manager Ed Talbot found his audience’s attention drifting from his talk to the “shiny” visuals he had brought to illustrate his talk, said Sandia spokesman Mike Janes. That led Talbot to consider how he could tell his department’s story more effectively, Janes said.

Sandia’s network intrusion analysts monitor the lab’s computer networks for unauthorized connections, hacking and attacks. SHINI has already helped them pick out unusual network connections for further investigation, Hurd said.



From left, Steve Hurd, Randy McClelland-Bane and intern Scott Crawford at Sandia.

“A lot of what SHINI is doing is giving you someplace to look that you might not have otherwise looked,” he said. Visual patterns created by the computer log data as it is drawn on the map can create both the usual patterns and the breaks from those patterns, indicating something worth digging deeper into, he said.

SHINI can also be very flexible in terms of the types of data it does and does not display, Hurd said.

“Say you’re having trouble with e-mail traffic. We’re planning to allow for the examination of particular kinds of traffic, helping analysts perceive things they might not perceive,” he said.

Mike Chaput, CEO of Berkeley’s [Endsight Inc.](#), said big multi-site companies could benefit from such a tool to spot problems, such as bandwidth issues, and make strategic decisions about whether to buy additional bandwidth and, if so, where.

“Something like this could help them better understand their data flows and recognize when patterns are broken, alerting them to potential viruses, and hackers too,” Chaput said.

The lab is already examining the potential for releasing an open-source version of SHINI, for use by both computer scientists and people in other fields that could benefit from visualizing data with geographic components in real time.

“If you think about the data we’re feeding into Google Earth ... it’s not that different than tracking flu, where you have data about where a person is, when they came in (to see the doctor) and what (strain) they had,” Hurd said. Sandia is already involved in some high-end analytical tracking of such things, as part of its research on bioterrorism, though it uses different tools.

SHINI could also be used to look at events such as the recent string of Oakland restaurant robberies, using the address, date and time, Hurd said. “Time gives you that third dimension.” That may just be the piece someone needs to solve a problem, he said.

mfitzhugh@bizjournals.com | 925-598-1425

All contents of this site © American City Business Journals Inc. All rights reserved.