Purpose of project and the creative, leading edge R&D effort

The purpose of this project is to improve cyberdefenses against social engineering attacks. We believe that for attackers to craft personalized phishing (spear phishing) attacks, web-based reseaSAND2012-8242P
research via our web sites -- will likely occur to identify appropriate targets. In this project, we work to visualize and analyze visit patterns to our web pages.

This research leverages Sandia's robust research environment with several researchers from three disparate organizations. Furthermore, we are making contacts and sharing information with other lab-directed research and development projects, as well as leveraging tools created for customer-sponsored work.

Noteworthy scientific and technical accomplishments over the life of the project

We have developed tools to collect and store the data necessary for our analysis, some demo-quality visualizations that provide new ways for analysts to look at the web server logs, and some early statistical analytics for deriving additional data on visitors based on their server traffic.

What do key R&D accomplishments mean to the general S&T community and the national security mission areas?

Successful attacks against Sandia jeopardize our intellectual property and the integrity of our computing infrastructures. As spear phishing has shown itself quite effective at introducing malicious software past conventional cybersecurity systems, we are working to innovate new defenses against these tactics.