Sandia cyber project looks to help IT professionals with complex DNS vulnerabilities

January 11 2012

Sandia computer scientist Casey Deccio developed a software tool called DNSViz to help network administrators with Domain Name System (DNS) vulnerabilities. DNSViz provides a visual analysis of the DNSSEC authentication chain for a domain name and its resolution path in the DNS namespace. Credit: Dino Vournas

Sandia National Laboratories computer scientist Casey Deccio has developed a visualization tool known as DNSViz to help network administrators within the federal government and global IT community better understand Domain Name System Security (DNSSEC) and to help them troubleshoot problems.

DNSSEC is a security feature mandated to all federal information systems by the White House's Office of Management and Budget

(OMB). The mandate, issued in 2008, requires that "the top level .gov domain will be DNSSEC-signed, and processes to enable secure delegated sub-domains will be developed."

The entity that serves to translate the hostname of a Uniform Resource Locator (URL) into an Internet Protocol (IP) address is known as the Domain Name System (DNS). A DNS "lookup" is a prerequisite for doing almost anything on the Internet, including Web browsing, emailing or videoconferencing.

Although the mandate made perfect sense, said Deccio, there soon emerged a problem when .gov organizations actually began deploying DNSSEC.

"DNSSEC is hard to configure correctly and has to undergo regular maintenance," he said. "It adds a great deal of complexity to IT systems, and if configured improperly or deployed onto servers that aren't fully compatible, it keeps users from accessing .gov sites. They just get error responses."

The still-new DNSSEC security feature is designed to allow user applications like Web browsers to ensure that the IP addresses they have received from the DNS have not been "spoofed" by anyone with ill intent. As such, Internet-connected systems within the government can verify that the responses are authoritative and have not been altered. Still, the hiccups with implementing DNSSEC convinced Deccio that there was a need for a tool like DNSViz.

DNSViz – helping the IT professional "see" the problems

DNS, said Deccio, is inherently insecure. Without DNSSEC, tampering

by third-party attackers could go undetected, thus redirecting online communications to unwanted destinations. This represents a particularly troublesome problem for .gov addresses owned by government organizations guarding national security information and other vital data.

Deccio believes DNSSEC is of little use if network administrators don't know how to configure or use it.

He describes DNSViz as a "tool for visualizing the status of a DNS zone." It provides a visual analysis of the DNSSEC authentication chain for a domain name and its resolution path in the DNS namespace, made available via a Web browser to any Internet user (http://dnsviz.net/). It visually highlights and describes configuration errors detected by the tool to assist administrators in identifying and fixing DNSSEC-related configuration problems.

DNSViz brings together all the components that work together for DNSSEC to function properly into a single graphical representation. The resulting visualization is a collection of configuration data and relationships that are otherwise difficult to assemble, assess and understand.

To help network administrators in their DNSSEC deployment, Sandia's DNSViz tool functions in two primary ways: It actively analyzes a domain name by performing pertinent DNS lookups, and it makes the analysis available via the Web interface. The active analysis occurs periodically to build a history of DNSSEC deployment over time and provide a historical reference for DNS administrators.

Currently, the Web interface is the primary source for viewers to observe data, though Deccio intends to expand DNSViz functionality to allow access via other means. For example, alert mechanisms might be used to inform affected parties, and application programming interfaces

(API) can be designed to allow administrators to programmatically access the information instead of manually browsing the DNSViz website.

Deccio has the tool running in the background on Sandia/California's servers, monitoring a list of some 100,000 DNS names. It performs an analysis a couple of times each day and offers a situational awareness of what the DNS configuration for each name looks like from top to bottom.

Though the functionality provided by DNSViz could potentially be included in a marketable software product that's sold by a for-profit company, Deccio says he envisions it as an open-source tool available to anyone who needs it. With further funding, he hopes to expand the tool so that it can analyze DNS health and security on a continuous basis, essentially creating a full-blown monitoring system that is scalable, versatile and more informational.

Provided by Sandia National Laboratories