Exceptional service in the national interest

Sandia National Laboratories
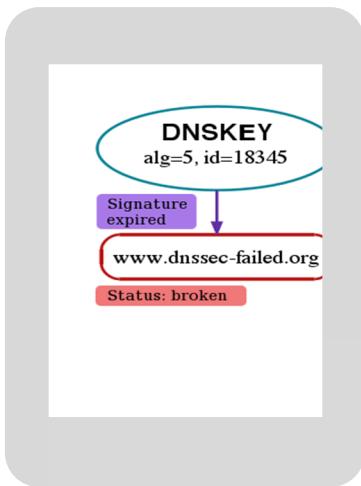
DNSViz

Casey Deccio
Sandia National Laboratories

Executive Summary

DNSViz is a Web-based tool that analyzes a domain name and presents its analysis in a visual interface to the user. Its primary contribution is a graphical representation of the authentication chain that is the crux of the Domain Name System Security Extensions (DNSSEC). It serves as a resource for visual understanding, troubleshooting, and maintenance of names for which DNSSEC has been deployed. In addition to real-time analysis, the tool periodically analyzes nearly 100,000 names on a daily basis, making a deployment history available to users. It has been used as a resource by registrars, registries, Internet Service Providers (ISPs), DNS architects, and others involved in the adoption of DNSSEC deployment.

I. *Describe the problem that was the impetus for this work.* This technology addresses difficulties in deploying, troubleshooting, and maintaining the Domain Name System Security Extensions (DNSSEC).

    a. *Why is this problem important?* DNSSEC will protect Internet users (including private and public sectors alike) from various attacks. Despite a great deal of government and community investment in developing and promoting DNSSEC, the extensions are very difficult to configure, deploy, and maintain.

    b. *Who is affected by this problem?* This problem affects public and private Internet service providers, the online retail sector, government agencies, and home users.

II. *Describe the technology that you are researching.* DNSViz is a Web-based diagnostic tool for troubleshooting and debugging problems with DNSSEC deployment. It is backed by a comprehensive scanning system that is constantly monitoring the Internet's DNS.

    a. *How does your research address the problem?* DNSViz provides a resource to users, such as network administrators, for troubleshooting and debugging their DNSSEC deployments.

    b. *How does your approach differ from products currently on the market or other research?* DNSViz was the first Web-based tool that demonstrated a comprehensive DNSSEC view of a domain name, addressing the most common operation issues with DNSSEC deployment and displaying the entire authentication chain. It is the only tool that provides a comprehensive DNS analysis in a concise, graphical representation.

    c. *Is this a standalone technology or is it a suite of solutions?* This is a standalone technology.

III. *Assess the research's technical readiness level.*
- a. *Has the technology been thoroughly tested?* Yes
    - i. *If so, in an operational or research setting?* Operational
- b. *Is the technology currently being used?* Yes
    - i. *If so, in an operational or research setting? By an internal or external organization?* Operational, by network administrators around the world
    - ii. *If not, when might it be ready for use, and how much funding over what timeframe would be needed if additional funds are required?* N/A
- c. *What infrastructure must be in place to deploy the proposed technology?* One or more servers are necessary to respond to Web requests and to perform periodic monitoring, each with accessibility to query Internet DNS servers over IPv4 and IPv6. A small cluster of servers provides a database housing the current and historical DNS data. Servers in a geographically distributed environment would be ideal.
- d. *What is the on-going overhead involved with operating and maintaining the technology?* Typical maintenance to the servers hosting the system is necessary. This includes software updates to core Operating System (OS) components and supporting software, hardware replacement, etc. Additionally, as development continues, features will be added and bugs fixed over time. Future development might also require additional architectural changes, e.g., if a different database system is deemed to be more suitable.
    - i. *Will operators be required to learn new skill sets?* Most system administration would be understood by typical system operators. However, there would need to be some understanding of the database being utilized.
    - ii. *Beyond operators, are there other support requirements?* No
    - iii. *Are these assessments based on operational experience with the technology, or are they estimates/expectations?* At the moment, DNSViz has only been deployed at a single location with a minimal architectural install, so the requirements for general application are estimate.

Continue your text here in Section 2, giving you a different page 2 header

IV.   *Has anyone expressed interest in transitioning this research to practice?* Yes
    a. *If so, who and when? What is the current status?*   Comcast is interested in hosting some of the DNSViz software. Discussions are ongoing.

V.   *Intellectual Property (IP) Interests*
    a. *What is the funding history, and implications for government or private use?* DNSViz was initially funded by operational overhead to assist in DNSSEC deployment at Sandia. It is currently in the process of being licensed as open-source software, so parts of it can be used by others.
    b. *What are your organization's IP interests relative to this technology?* Our primary interest is benefitting the community by supporting efforts to deploy DNSSEC and ultimately secure the Internet for end users. The plan is to make portions of the code available for additional users and uses while continuing to support a public site for DNSSEC monitoring and analysis.
    c. *Are there other collaborators?*   Not currently, though there have been discussions with outside entities of future collaboration.
        i. *If so, who are they?* (future) Comcast, CAIDA, ESnet
    d. *Who owns the IP?* Department of Energy (Sandia is in the process of asserting copyright)
        i. *Does anyone else have a claim to the IP?* No
    e. *Are there any patents or patents pending for this technology?* No
        i. *Does this approach require licensing any foundational IP?* No
    f. *Are there processes in place for transitioning IP for commercialization?*   No
    g. *Are there any IP issues that would restrain open sourcing the technology?* No. The process of open sourcing the technology is underway.