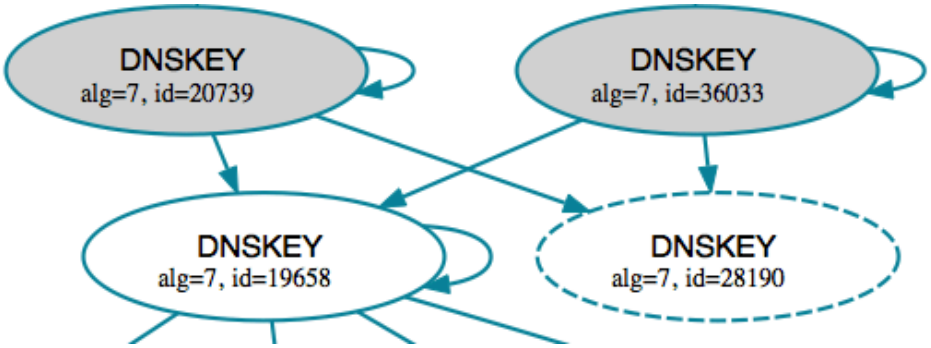
SAND2012-5547P

Exceptional service in the national interest

Sandia National Laboratories



DNSViz – Simplifying Internet Security Troubleshooting

Casey Deccio

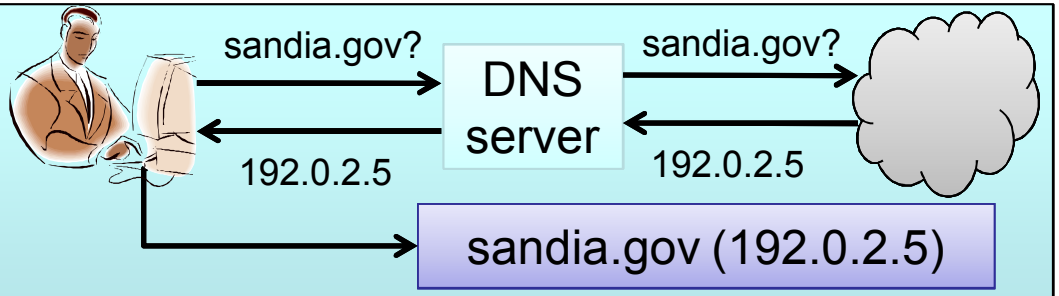
ctdecci@sandia.gov

U.S. DEPARTMENT OF ENERGY | NNSA

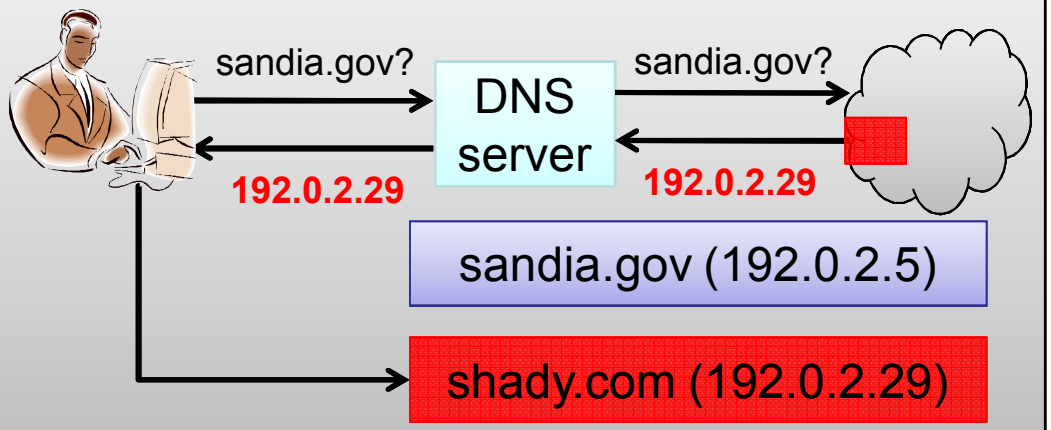
Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

DNS – Roles and Threats

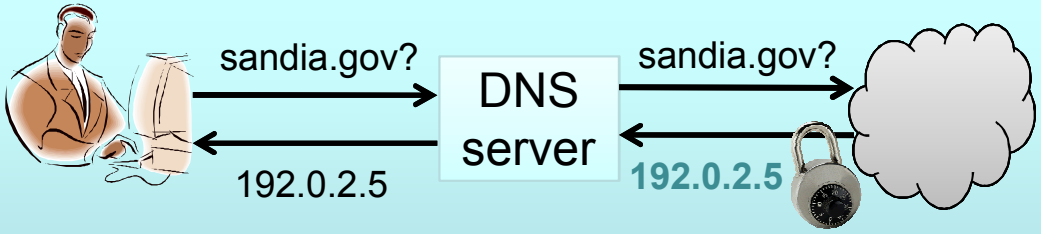
The Domain Name System (**DNS**) **translates** domain names to IP addresses.



With DNS **cache poisoning** a computer is directed to a malicious server.



DNS security (**DNSSEC**) allows DNS servers to cryptographically **authenticate** DNS responses and detect forged responses.



DNSSEC Challenges

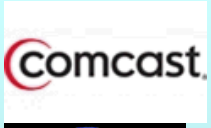
Sandia National Laboratories

DNSSEC validation outcomes:

- **Insecure** – no security available (plain old DNS)
- Secure – signed and validated
- Bogus – validation fails (tampering… or misconfiguration)

Problem: Configuring and maintaining DNSSEC is **hard.** All failures to date are attributed to **misconfiguration**, rather than cache poisoning.

Example:



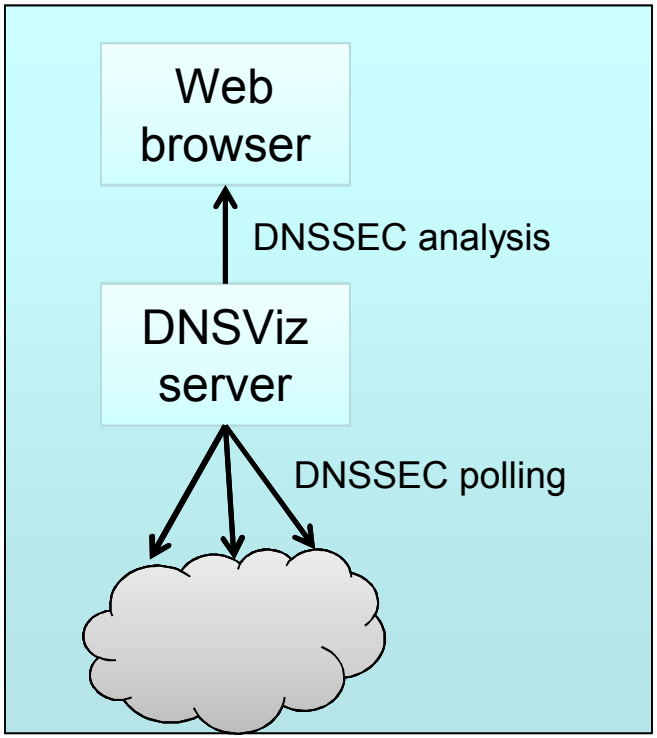
Jan 10, 2012 – Comcast enables validation for 17M residential customers.

Jan 18, 2012 – nasa.gov DNSSEC configuration breaks (NASA's fault). nasa.gov becomes unavailable for all Comcast customers. Comcast disables validation of nasa.gov for hours.

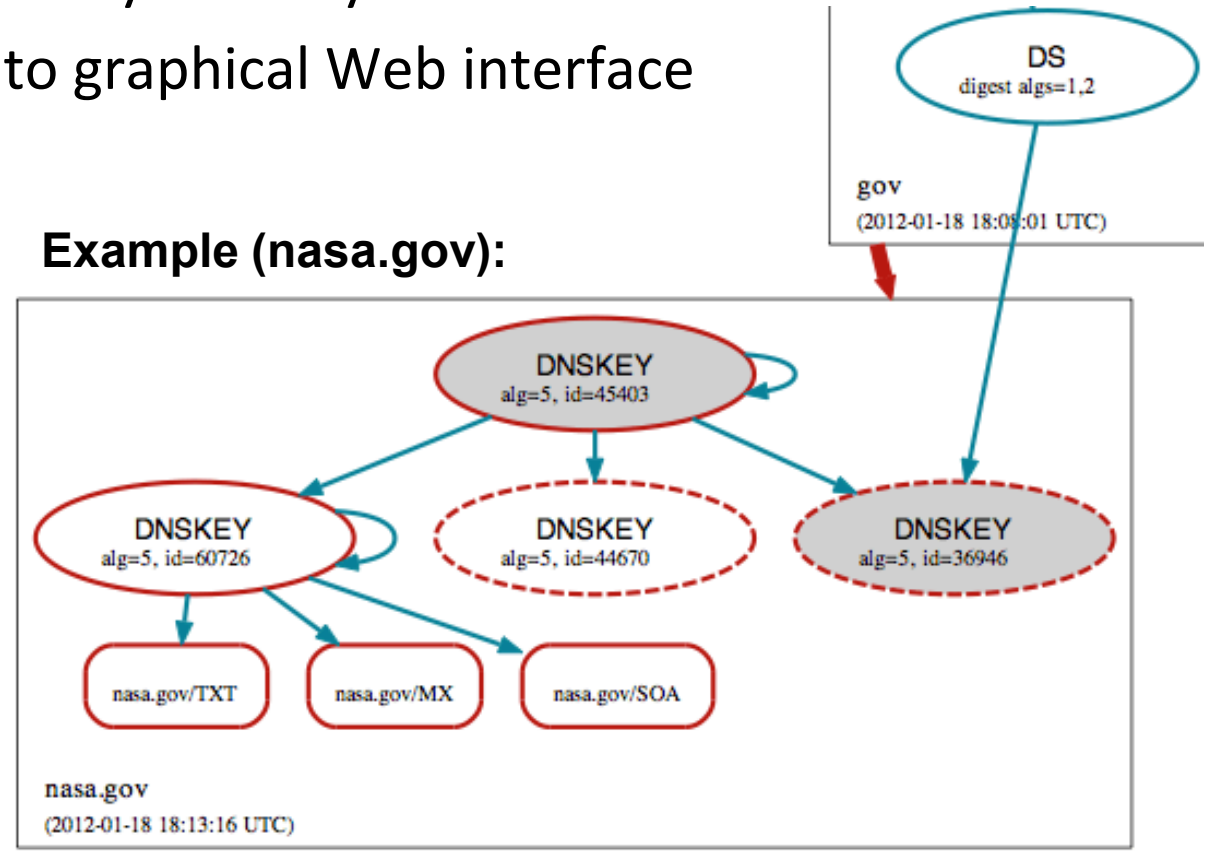
Problem: Troubleshooting DNSSEC problems is **hard.** DNS data and security are spread across **multiple servers.**

DNSViz – Visualizing DNSSEC

- Designed for comprehensive analysis to facilitate deployment, understanding, and troubleshooting
- Polls all servers necessary to analyze a DNS domain
- Consolidates data into graphical Web interface



Example (nasa.gov):



DNSViz – Impact

- Facilitated DNSSEC understanding and troubleshooting.
  - Visualization helps developers and administrators understand and analyze DNSSEC.
  - Comcast uses DNSViz as first resource when troubleshooting DNS issues.
  - DHS FNS is looking to partner with Sandia to leverage DNSViz functionality.
- Historical analysis for improved DNSSEC deployment.
  - Behavioral trends have been analyzed and presented at international forums.
- DNSSEC depth and experience.
  - Sandia has been a technical resource to the US Government for independent legislation review, e.g., SOPA.