NIST National Institute of Standards and Technology U.S. Department of Commerce

DNS Security:

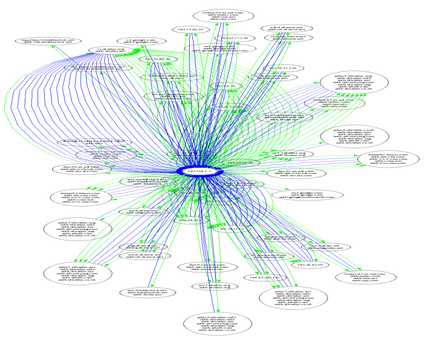
A Trusted Naming Infrastructure for the Internet

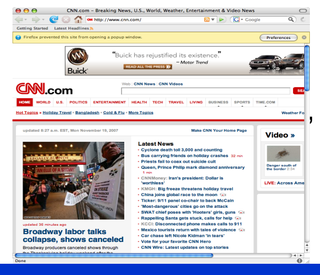
http://www-x.antd.nist.gov/dnssec/

INFORMATION TECHNOLOGY LABORATORY

DNS – User's Interface to Internet

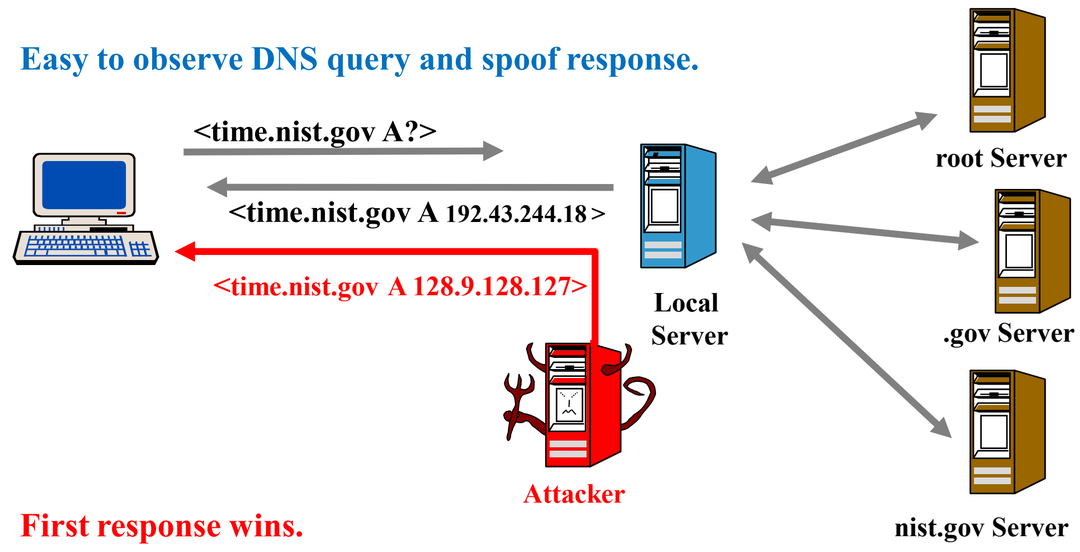
- **Importance of DNS Names**
  - URIs part of our language now
    - dougm@nist.gov, www.nist.gov., ibm.com
- **Complexity of DNS-System**
  - ~50-100 queries to load a news/ecommerce web page.
  - Dynamic DNS resolution
    - CDNs, load redirections.





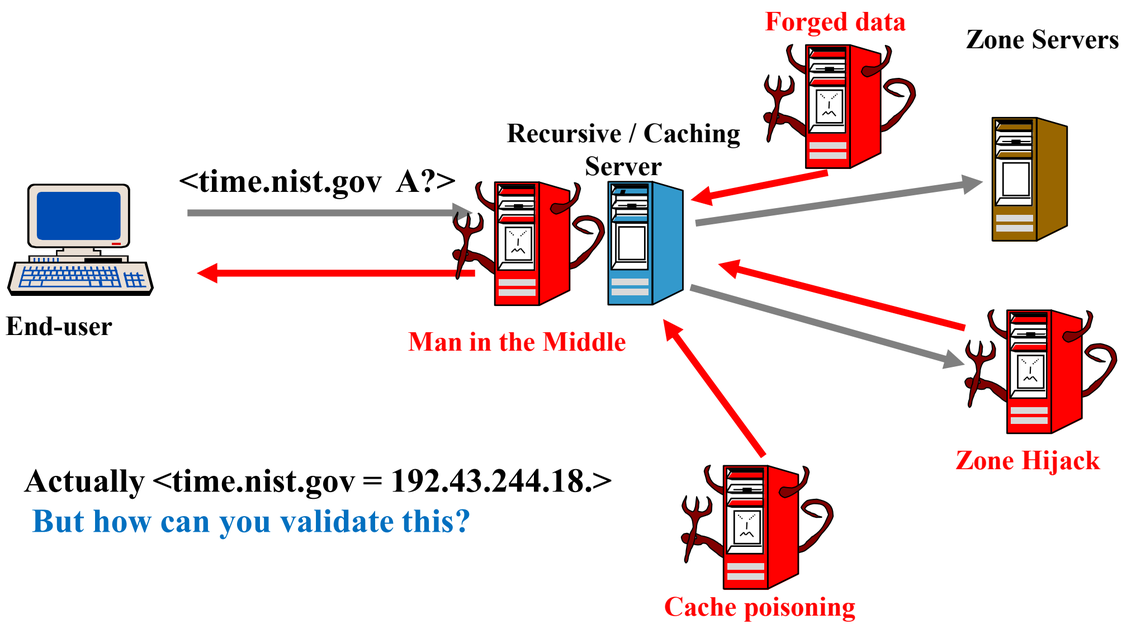
DNS Interactions to load www.cnn.com

A Simple DNS Attack



First response wins.
Second response is silently dropped.

Other Forms of DNS Attacks



Actually <time.nist.gov = 192.43.244.18.>
But how can you validate this?

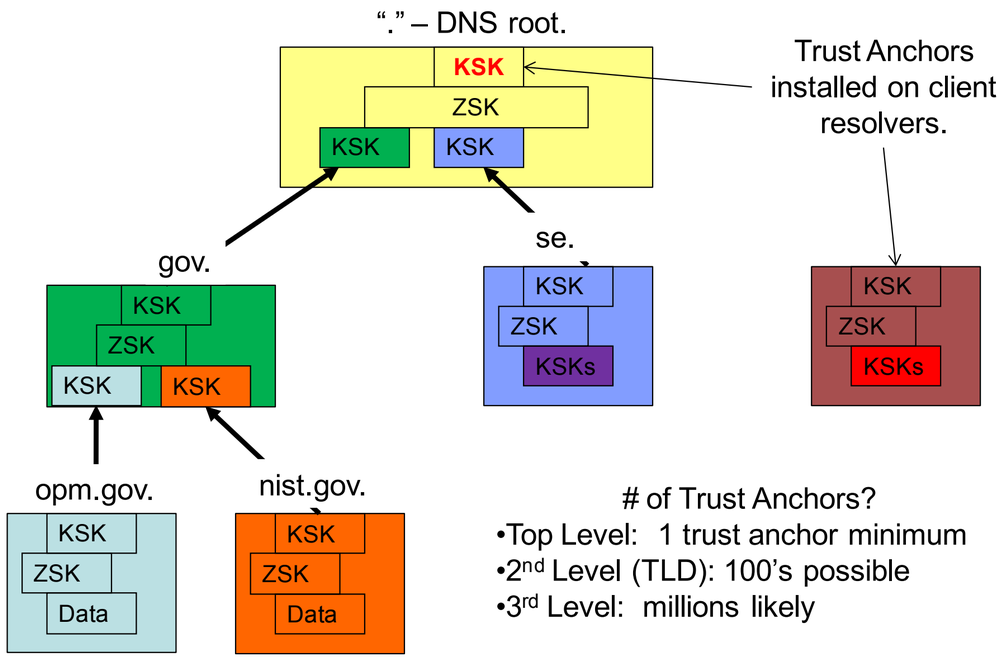
DNS Security Extensions (DNSSEC)

- **DNSSEC Standards:**
  - Open, consensus, international IETF standard extensions to **add** basic security mechanisms and trust models to the DNS.
  - Adds digital signatures to DNS data.
    - Source authentication and Data integrity
  - Incremental deployment model on current DNS infrastructure.
  - Enables establishment verifiable "chain of trust" between parent and child zones.

IETF

- **RFC 4033 -** DNS Security Introduction and Requirements
- **RFC 4034 -** Resource Records for the DNS Security Extensions
- **RFC 403 -** Protocol Modifications for the DNS Security Extensions
- **RFC 5011 -** DNS Key Rollover
- **RFC 5155 -** DNSSEC Hashed Authenticated Denial of Existence

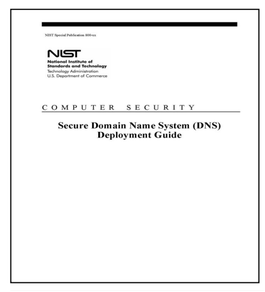
DNSSEC Chain of Trust

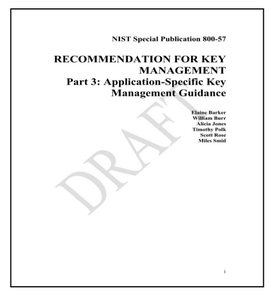


# of Trust Anchors?
- Top Level: 1 trust anchor minimum
- 2nd Level (TLD): 100's possible
- 3rd Level: millions likely

DNSSEC Deployment Guidance

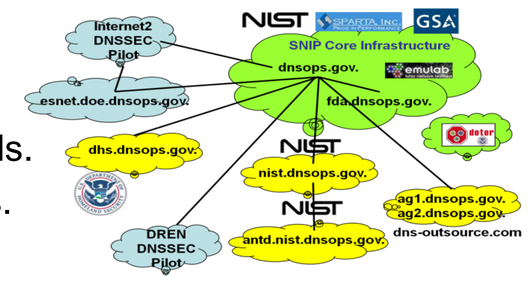
- **Secure DNS Deployment Guide**
  - NIST Special Publication 800-81
  - Deals with DNS Security, not just DNSSEC
  - Technical deployment guidance for enterprise DNS administrators and security officers.
  - Provides both information for robust configuration of traditional DNS services and deployment / operational guidance for DNSSEC.
  - Provides cookbook configuration examples for commonly used DNS servers.
- **DNSSEC Key Management Guides**
  - NIST Special Publication 800-57 Parts 1,2,3
  - Key / Algorithm parameters for DNSSEC
  - Puts DNSSEC in context of general USG requirements for key management and use.



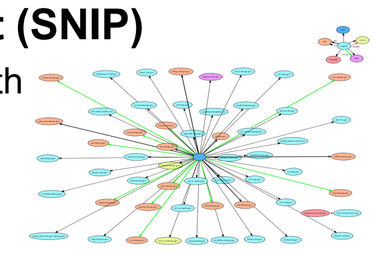


DNSSEC Tools, Tests & Testbeds

- **Open Source Test Tools**
  - NIST Zone Integrity Tester
  - Load generation and perf tools.
  - Performance analysis reports.



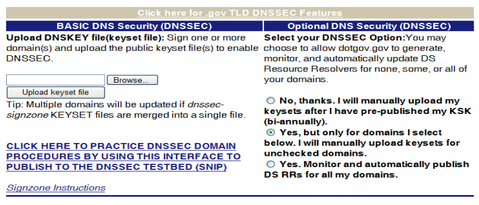
- **Secure Naming Infrastructure Pilot (SNIP)**
  - USG / Industry testbed to experiment with DNSSEC technologies.
  - Practice new zone administration processes.
  - Pilot USG .gov TLD key management processes.



Starting From the Top: .gov & root

- **Deployment at the .gov gTLD.**
  - Feb 2009 - First global TLD to operationally deploy DNSSEC!
    - NSEC3 signed, 2048bit keys, trust anchor @ itar.iana.org.
  - Dotgov.gov registry is up & operational
    - accepting secure delegations from secondary's.
    - POC authentication and notification functions.
    - Manual and automated key rollover functions.
    - Monitoring and diagnostics for USG signed zones.
    - Prepared to accept other .gov secure delegations (states, etc).
    - Registry interface integrated with SNIP
- **Deployment at the global DNS root.**
  - NIST & NTIA developing technical plans to sign the root.
  - Global root signed in 2010.

dotgov.gov



NIST NTIA