Major findings

- 38% of federal .gov domains have been signed with DNSSEC as of mid-September 2010
- 36% of federal .gov domains are fully authenticated with DNSSEC
- 2% of federal .gov domains signed with DNSSEC are incorrectly configured and provide DNSSEC answers that fail on authentication
- 2,941 .gov domains were successfully identified and tested – the largest set of .gov domains we are aware of being studied outside of the Federal government
- The majority of domains in the .gov namespace are run by state and local agencies rather than federal departments and agencies.

Background

What is DNSSEC and why is it important? DNSSEC is meant to prevent DNS based exploits and redirections like DNS cache poisoning attacks by allowing domain names and corresponding IP addresses to be verified using digital signatures and public-key encryption. This system is envisioned to reach from the very root of the DNS all the way out to individual hostnames, allowing Internet users to verify the authenticity of DNS responses from their ISPs or enterprise resolving nameservers. Rollout of DNSSEC became a major initiative in 2008, with the discovery of a major flaw in the current DNS system that allow attackers with sufficient resources to exploit resolving nameservers. This flaw is commonly referred to as the “Kaminsky Bug” after its discoverer, Dan Kaminsky.

On August 22, 2008, the White House Office of Management and Budget (OMB) mandated DNSSEC deployment for all US Federal agencies’ domain names by December 2009 (http://www.dotgov.gov/OMBDNSSECMemo.pdf). Since that time the .gov zone and the DNS root itself have been signed. Many agencies have successfully deployed DNSSEC-signed domains. This allows for properly configured .gov domain names to be fully authenticated end-to-end from the trust anchor at the DNS root itself out to their own space.

It has been widely reported that the OMB target wasn’t met (e.g. http://it.slashdot.org/article.pl?sid=10/01/22/1540205 http://www.networkworld.com/news/2010/012010-dns-security-deadline-missed.html). So the question nine months later is how close are we now? Since the US government does not release information on the full makeup of the .gov zone, it is hard to determine what domains to test, much less do some of the sophisticated queries and interpretation necessary to qualify a domain as authenticated. There is a government website that reports on DNSSEC implementation on a portion of .gov...
domains ([http://www.dnsops.gov/USAdotGOV-status.html](http://www.dnsops.gov/USAdotGOV-status.html)) but this resource only covered 868 .gov domains at the time this study was done. To get a fuller picture, other resources must be consulted and independent tests run.

**Methodology**

We enumerated a large set of the .gov domain zone based on known agency names and abbreviations, observed domains in DNS traffic, search results, and other sources. We found and confirmed 2,941 domain names in the .gov namespace. Based on prior reporting on the size of the .gov zone, and our findings of registered, but non-deployed, domain names, we believe we have tested a majority of the active domains in the space that contains approximately 5,000 domains overall (both active and inactive).

We then ran the entire set of domains through a series of tests using the DNS-OARC Open DNSSEC Validating Resolvers ([https://www.dns-oarc.net/oarc/services/odvr](https://www.dns-oarc.net/oarc/services/odvr)), a definitive resource for checking DNSSEC resolution for any domain name or DNS record. The tests included a series of “digs” for the domains using those resources that returned the statuses of their DNSSEC deployment, and tabulated the results.

**Findings**

When analyzing the test results, it was important to break out Federal domains from Native American, state and local government agency, and other non-Federal agency domain names. Only U.S. Federal agencies were directed to have their .gov domains signed this year. It is also interesting to note that several domains appeared to not meet the currently published eligibility requirements for .gov domain registration, perhaps because those domains were registered prior to the current standards taking effect. The eligibility requirements may be found at the dotgov.gov website ([http://www.dotgov.gov/help_qualify.aspx](http://www.dotgov.gov/help_qualify.aspx)).
In our sample set, 1,185 domains are registered to Federal agencies and potentially fall under OMB’s directive. Within that set, over a third return fully authenticated DNSSEC results under multiple lookup scenarios. These domains are ready for DNSSEC to take hold across the Internet as a standard, offering fully signed, valid responses.
Two percent of federal domains have been signed using DNSSEC but are failing authentication with a hard (SERVFAIL) result using at least one major DNS resolver implementation. This failure means that those domains would be blocked for many Internet users around the world under full DNSSEC implementation. Interestingly there were many domains that had even more basic configuration issues like non-existence in the .gov zone file, possibly due to expired registration or lack of payment. Other errors included several domains’ authoritative nameservers either not being configured to support them, or simply refusing to answer any DNS queries at all. Domains with these issues are not resolvable at all, regardless of their DNSSEC signing status.

Overall, about 15% of all the domains in .gov we studied were fully signed and authenticated, with just 11 domains outside of Federal jurisdiction being signed for DNSSEC. Vermont and Idaho deserve kudos for successfully signing several of their
states' domain names on their own accord. Virginia.gov is also a good example of a fully DNSSEC authenticated domain name.

**Take-Aways**
DNSSEC deployment in .gov is underway, making progress, but behind schedule. Much has been made about the difficulties of implementing an entirely different DNS standard that is highly complex and new to most administrators. The adoption and error rates for .gov deployment bear that out so far. Yet despite the difficulties, there are many success stories: highly sensitive domains for the FBI, the Federal Reserve, DHHS, and the DEA, along with hundreds more, are being fully signed and authenticated.

It appears that once a particular agency implements their DNSSEC plan, many or most domains controlled by that organization get signed. Agencies like the Treasury Department and the Department of Defense, that run many of the most sensitive, and as-yet unsigned, large blocks of .gov domains, could be encouraged and/or assisted in implementing DNSSEC for their overall departments and various sub-agencies. Perhaps some best practices or other cross training from other agencies would be helpful.

DNSSEC implementation and maintenance are not easy, and are difficult to test and monitor during this initial transition period. Instructions and implementation programs exist, but are limited and still being refined. Testing tools are even more limited, and having more definitive, easy-to-use testing tools and services would be helpful in preventing some of the failure issues we saw. Lessons that are being learned in the Federal .gov space will be useful for all to learn as we look to the signing of .com and .net next year.

IID will continue to report on adoption rates at the domain level of .gov and other TLD zones regularly to help the industry understand how the DNSSEC rollout is progressing.