DNSSEC: Securing the DNS

ICANN Office of the Chief Technology Officer

David Conrad
OCTO-006v3
24 July 2020

TABLE OF CONTENTS

This document is part of the OCTO document series. Please see the OCTO publication page for a list of documents in the series. If you have questions or suggestions on any of these documents, please send them to octo@icann.org.

This revision contains updates from many people who read OCTO-006v2. ICANN greatly appreciates the reviews sent to us.

Introduction

Domain Name System Security Extensions (DNSSEC) help secure the way information moves around the Internet.

The Domain Name System (*DNS*) is used by everyone who connects to the Internet and nearly all devices on the Internet every day. Using an automated process known as a *lookup* or *resolution*, one of the many functions of the DNS is to map easy-to-remember names (e.g., example.com) to the unique numbers known as *Internet Protocol* (IP) *addresses* (e.g., 192.0.2.189 or 2001:DB8:107A:61F7). These IP addresses are then used by devices to identify and communicate with each other. In this way, the DNS is often compared to a telephone directory or a contact list, translating names into numbers.

What is DNSSEC?

When the DNS was created in the early 1980s, security was not a focus of the design. Due to a design decision that made sense at the time, in rare cases it was possible for attackers to provide their own answers to domain name lookups instead of what the owner of the domain (the registrant) intended. For example, instead of going to the website you requested in your browser, an attacker might compromise DNS messages to redirect you a website that looks like the web site you wanted to go to, but which is instead controlled by the attacker. In the 1990s, the DNS technical community came up with the definitive solution to this problem, known as the DNS Security Extensions or *DNSSEC*.

How does DNSSEC work?

A registrant is the person or organization who controls the information associated with a domain name, that is, the name-to-address mapping and other data. DNSSEC allows registrants to digitally sign the information they put into the DNS; this allows clients (for instance, your web browser) to verify that the DNS answers they receive in response to lookup requests have not been modified since they were signed.

In 2010, ICANN enabled the top-most level of the DNS, known as the root, to be DNSSEC-signed, thereby greatly facilitating global DNSSEC deployment. However, even a decade later, deployment of DNSSEC continues to lag.

What are the benefits of deploying DNSSEC?

- **DNSSEC Protects the Internet**: Since the DNS is essential to the operation of the Internet, protecting the data provided by the DNS is critical. By analogy, the DNS can be seen as road signs on the Internet, allowing communication to be directed to the correct content or service. As with road signs on actual roads, if attackers change where those signs point, it could result in misrouted traffic, perhaps redirecting to a bad part of town.

- **DNSSEC Protects End Users**: DNSSEC can provide assurance that the domain name data received by end users is the same data the registrant intended the end user to receive. DNSSEC helps ensure that when an end user or device is trying to obtain the content or service pointed to by a domain name, the site they are communicating with is the site the registrant intended.

- **DNSSEC Protects Companies, Organizations, and Governments**: DNSSEC reduces the likelihood that end users wishing to make use of their services or view their content will be misdirected to a site where they could possibly be defrauded by an attacker. Internet service providers (ISPs) can add value to the service they provide to their customers by enabling DNSSEC validation on their resolvers. Organizations that sign their domain names with DNSSEC reduce the risk of the people looking for them on the Internet being misdirected.

- **DNSSEC Fosters Innovation**: DNSSEC provides a way of verifying and protecting DNS data, thereby allowing that data to be trusted. This in turn allows the leveraging of the global DNS to create a secure name/value database (e.g., you submit a name and the DNS returns values associated with that name) that is globally distributed and publicly accessible by anyone on the Internet. As a result, this secure database can create opportunities for innovation and enable new technologies, services, and facilities. For example, one such technology, DNS-based Authentication of Named Entities (DANE), creates a new way to secure connections across the Internet. DANE leverages DNSSEC-protected data in the DNS and addresses some of the vulnerabilities in the current way secure connections on the Internet are made. This makes Internet commerce and communications more secure.

How do I put DNSSEC into action?

Broadly speaking, the DNS has two sides: publishing, which is performed by registrants or their agents, and lookup (also known as resolution), which is typically done by network operators such as Internet service providers. To benefit from DNSSEC, both sides must use it.

- **Registrants:** The people responsible for publishing DNS information must ensure their DNS data are DNSSEC-signed. Historically, this process tended to be complicated and error-prone. However, today most modern DNS software packages and registration systems have tools that automate DNSSEC-signing of the data registrants wish to publish. As a result, registrants or their agents merely need to enable DNSSEC-signing in their DNS servers (or at their registrars) and provide their registrar with a bit of information, known as the *delegation signer record*, to help establish trust in the information they just signed.

- **Network Operators:** On the lookup side, it is even easier: network operators only need to enable DNSSEC validation on the resolvers that handle DNS lookups for users. Resolver software increasingly enables DNSSEC validation by default.

- **Internet End Users:** End users typically do not need to do anything other than encourage their network operators to enable DNSSEC validation and signing of the domain names they use.

What are the costs associated with DNSSEC?

The DNS servers on both the publishing and lookup sides need to support DNSSEC, so it may be necessary for organizations to update their DNS software packages (a best practice, whether or not DNSSEC is deployed).

- On the publishing side, it may also be necessary for registrants or their agents to modify their processes to allow the "delegation signer" records to be sent to their registrar. The cost of such modifications may be considerable; however, this would be a one-time change and cost.

- On the lookup side, assuming the DNS server software is reasonably modern, the costs should be negligible as all that may be required would be a one-time configuration change to enable DNSSEC validation.

What happens if I don't deploy DNSSEC?

- **Users Could Be Vulnerable to Attacks:** If an organization chooses not to deploy or enable DNSSEC, its users are susceptible to a particular type of attack known as "cache poisoning". When an end user does a lookup, attackers could transparently insert answers to DNS questions, potentially redirecting communication attempts to devices controlled by the attackers. The attackers could then mimic websites or other services, steal usernames and passwords, etc. The incorrect answers would also be kept in the the server doing the lookup for some period of time, thus causing the redirection to continue until the answers expire or are removed. While these kinds of attacks are rare, given that DNSSEC exists to address these attacks and has been available for some time, organizations that are victimized by this exploitation may need to have difficult discussions with their users as to why they did not deploy DNSSEC. As other forms of attack are prevented, it is likely attackers will take advantage of sites that have not deployed DNSSEC as implementing attacks via the DNS becomes more common.

- **Innovation Could Be Slowed:** Failure to deploy DNSSEC hampers innovation and slows the deployment of new technologies that use the DNS as a globally trusted database. Some of those technologies promise to provide better ways to trust connections for Internet services, such as email or the web.

Although the vulnerabilities DNSSEC addresses have existed since the DNS was created, there have yet to be many high-profile attacks that leverage those vulnerabilities. Because of this, some may believe the costs of deploying DNSSEC outweigh the benefits DNSSEC provides. Still, it is worth noting that the costs and risks of implementing DNSSEC have greatly decreased. In fact, the benefits of DNSSEC increase as more networks deploy it.

Another way of looking at the question of deploying DNSSEC: "If it is worth the effort to put data into the DNS, isn't it worth the effort to ensure that data isn't tampered with?"

Some history of DNSSEC

In 1983, Paul Mockapetris of the Information Sciences Institute at the University of Southern California published a series of documents that introduced the concept of the domain name system. In its original form in the 1980s, the DNS did not have any built-in security, confidentiality, or authentication; there was no mechanism to assure that an answer received was legitimate and actually corresponded to the question asked.

Around 1990, Steve Bellovin of AT&T Bell Laboratories authored a paper that described how attackers could leverage a particular design decision in the DNS to break into systems. In his paper, Bellovin recommended using cryptographic authentication to better protect the DNS. Following the publication of Bellovin's paper, a formal process started to make his proposal an Internet Engineering Task Force (IETF) protocol standard called "DNS Security Enhancements" (*DNSSEC)*.

DNS software that implemented DNSSEC was initially developed in the late 1990s, with some early deployments of DNSSEC starting around 2000, including by the popular .SE ccTLD (the country code of Sweden). Those early deployments, however, revealed numerous technical challenges to operating DNSSEC at scale in production, which led to the IETF continuing to work on improving the protocol over the next eight years.

Nothing major happened in terms of deployment until 2008, when a security researcher named Dan Kaminsky discovered a serious design shortcoming in the DNS protocol itself that allowed attackers to launch cache poisoning attacks against the lookup side of the DNS. This finding prompted renewed attempts by the DNS technical community at getting more DNSSEC deployment, and in particular, at getting the root of the DNS signed.

In July 2010, the root zone was signed for the first time by ICANN, providing a global trust anchor for all DNSSEC validation. In October 2018, the root zone's key signing key was successfully updated for the first time, representing a significant milestone for DNSSEC.

A series of international DNS hijacking campaigns in 2018 and 2019 led to the first-ever Emergency Directive by the United States Cybersecurity and Infrastructure Security Agency (US-CERT), and prompted ICANN to renew its call for all DNS stakeholders to fully deploy DNSSEC.

ICANN's role in DNSSEC

ICANN, as part of its mission to promote a more stable, secure, and resilient DNS ecosystem, has long been a leading proponent of DNSSEC deployment. ICANN's formal operating agreements with both Registries and Registrars require that DNSSEC be supported. ICANN org regularly engages with DNS stakeholders around the globe to help them understand the importance of DNSSEC, and to train engineers in how to deploy and operate DNSSEC in their networks. In addition to awareness and capacity development, technologists at ICANN work with the IETF community on DNSSEC enhancements.

From the operational side, ICANN continues to play a critical role. ICANN is responsible for generating, storing, and periodically updating the root key signing key, a cryptographic key

trusted by all validating resolvers on the Internet, which is used in the process to sign the root of the global DNS.

For more information

There are many resources and technical groups involved in DNSSEC and its deployment. A small sampling:

- DNSSEC and all other DNS protocol-related efforts are discussed within the IETF, in particular in the DNS Operations (DNSOP) Working Group.
- DNSSEC workshops are held three times a year at ICANN Public Meetings. These workshops, organized by the Internet Society, provide operational insights, advice, and analyses about DNSSEC deployment. An associated website sponsored by the Internet Society provides an archive of those meetings.
- For more information, ICANN provides a general description of DNSSEC and why it is important.