DNSSEC: Securing the DNS

ICANN Office of the Chief Technology Officer

David Conrad
OCTO-006
27 February 2020
## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>WHAT IS DNSSEC?</td>
<td>3</td>
</tr>
<tr>
<td>HOW DOES DNSSEC WORK?</td>
<td>3</td>
</tr>
<tr>
<td>WHAT ARE THE BENEFITS OF DEPLOYING DNSSEC?</td>
<td>3</td>
</tr>
<tr>
<td>HOW DO I PUT DNSSEC INTO ACTION?</td>
<td>4</td>
</tr>
<tr>
<td>WHAT ARE THE COSTS ASSOCIATED WITH DNSSEC?</td>
<td>4</td>
</tr>
<tr>
<td>WHAT HAPPENS IF I DON’T DEPLOY DNSSEC?</td>
<td>5</td>
</tr>
<tr>
<td>FOR MORE INFORMATION</td>
<td>5</td>
</tr>
</tbody>
</table>

This document is part of the OCTO document series. Please see [https://www.icann.org/resources/pages/octo-publications-2019-05-24-en](https://www.icann.org/resources/pages/octo-publications-2019-05-24-en) 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.
Domain Name System Security Extensions 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, the DNS maps 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) that are 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. In particular, it was possible for attackers, in rare cases, 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 to another website. 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?

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 tampered with.

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, significant implementation 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 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 to 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’re 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. In this way, since it is the responsibility of network operators like ISPs to turn on the DNS resolver feature to validate DNSSEC signatures, enabling DNSSEC may also be an added value that network operators provide to their customers.

- **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 a value) 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, **DANE** (DNS-based Authentication of Named Entities), 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**: Registrants, who are 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 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 to their registrar a bit of information, known as their **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.

- **INTERNET END USERS**: End users typically do not need to do anything other than encourage their network operators to enable DNSSEC.

### What are the costs associated with DNSSEC?

The DNS servers in 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, regardless if DNSSEC is deployed).

- On the publishing side, it may also be necessary for publishers to modify their processes to send the delegation signer records 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.

What happens if I don’t deploy DNSSEC?

** USERS COULD BE VULNERABLE TO ATTACKS:** If an organization chooses not to deploy or enable DNSSEC, their users are susceptible to attacks. 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. 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 address have existed since the DNS was created, there has 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 keep increasing as more networks have deployed 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?”

For More information

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

- DNSSEC and all other DNS protocol-related efforts are discussed within the Internet Engineering Task Force (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 [https://www.dnssec-deployment.org/](https://www.dnssec-deployment.org/), sponsored by the Internet Society, provides an archive of those meetings.
- For a bit more information, ICANN provides a general description of DNSSEC and why it is important at [https://go.icann.org/2Mt08bY](https://go.icann.org/2Mt08bY).