DNSSEC：保护 DNS 的安全

ICANN 首席技术官办公室

戴维 • 康纳德 (David Conrad)
OCTO-006v3
2020 年 7 月 24 日

ICANN

目录

本文档是首席技术官办公室 (OCTO) 文档系列的一部分。请参阅 OCTO 文档页面，以了解该系列的文档列表。关于这些文档，如果您有任何问题或建议，请将您的反馈发送至 octo@icann.org。

这个修订版本包含的更新内容均来自众多 OCTO-006v2 读者的反馈。对于大家给予的评论，ICANN 在此致以深深的谢意！

简介

域名系统安全扩展 (Domain Name System Security Extensions, DNSSEC) 有助于确保信息在互联网上以安全的方式传输。

每天，每位连接互联网的人员，以及互联网上几乎所有的设备，都会用到域名系统 (*DNS*)。在 DNS 提供的多项功能中，有一项称之为“*查询*”或“*解析*”的自动化进程，它可以将易于记忆的名称（例如，example.com）映射为称作是*互联网协议* (IP) *地址*的唯一数字（例如，192.0.2.189 或 2001:DB8:107A:61F7）。设备可随后使用这些 IP 地址来相互识别和通信。根据这种将名称转换为数字的方式，人们常常把 DNS 比作是“电话号码簿”或“通讯录”。

什么是 DNSSEC？

DNS 创建于 20 世纪 80 年代初期，在当时，安全性并不是网络设计的重点考虑因素。由于当时的设计决策有其合理性，因此就域名查询而言，除了域名所有者（注册人）打算应答之外，攻击者几乎不可能提供他们自己的应答。举例来说，与侵入您在浏览器中请求的网站不同，攻击者可能会破坏 DNS 消息，从而让您重定向到一个貌似于您要访问的网站，实则却是攻击者操控的网站。20 世纪 90 年代，DNS 技术社群针对这个问题提出最终解决方案，即 *DNSSEC*。

DNSSEC 如何运作？

“注册人”是指有权控制域名相关信息（即，名称转换为地址的映射以及其他数据）的个人或组织。DNSSEC 准许注册人对他们存放在 DNS 中的信息进行数字签名，这样一来，客户端（例如，您的 Web 浏览器）就能够验证它们收到的 DNS 查询请求的应答结果与签名时的内容相比是否发生了修改。

2010 年，ICANN 针对 DNS 的顶层（即“根”）实施 DNSSEC 签名，从而极大地推动了 DNSSEC 在全球范围内的部署。然而，即使在十年后的今天，DNSSEC 的部署仍然滞后。

部署 DNSSEC 有哪些优点？

- **DNSSEC 可以保护互联网**：由于 DNS 对于互联网的正常运营至关重要，因此，保护 DNS 提供的数据，自然是重中之重。打个比方，我们可以将 DNS 看作是互联网上的路标，为来来往往的通信指明获取正确内容或服务的方向。跟实际道路上的路标一样，如果攻击者更改了这些路标的指向，那就可能会导致交通路线错误，甚至会驶往城市的不安全地带。

- **DNSSEC 可以保护最终用户**：DNSSEC 可以保证，最终用户收到的域名数据与注册人打算让最终用户接收的数据相同。DNSSEC 有助于确保，最终用户或设备尝试通过访问域名而获取的内容或服务，正是源自于注册人希望用户访问的站点。

- **DNSSEC 可以保护公司、组织和政府机构**：对于希望使用有关公司、组织和政府机构的服务或查看其内容的最终用户，DNSSEC 可降低他们被定向到错误网站的可能性，从而减少被攻击者欺诈的危险。通过在其解析器上启用 DNSSEC 验证，互联网服务提供商 (ISP) 可以向客户提供增值服务。如果组织采用 DNSSEC 技术来签署其域名，则可以降低用户在互联网上搜索该组织信息时遭遇误导的风险。

- **DNSSEC 可以促进创新**：DNSSEC 提供了一种验证和保护 DNS 数据的方法，从而使这些数据成为可信数据。相继地，这也促进了全球 DNS 的应用，进而创建了一个安全的域名/值数据库（例如，您提交一个域名，DNS 就会返回与该域名关联的值），该数据库在全球范围内分布，且面向互联网上的所有公众开放。作为结果，这个安全的数据库可以提供多种创新机会，并且支持新的技术、服务和设施。例如，一项名为“基于 DNS 的名称实体验证”(DNS-based Authentication of Named Entities, DANE) 的技术，开创了确保互联网安全连接的新方法。DANE 利用 DNS 中受 DNSSEC 保护的数据，解决了当前互联网安全连接方法中存在的一些漏洞。这让通过互联网开展的商务和通信活动变得更加安全。

如何实施 DNSSEC？

从广义上来讲，DNS 涉及两个方面：发布，由注册人或其代理执行；以及查询（又称为“解析”），通常由网络运营商（例如，互联网服务提供商）来完成。要从 DNSSEC 中获益，这两方面都必须使用 DNSSEC。

- **注册人**：负责发布 DNS 信息的人员必须要确保其 DNS 数据经过 DNSSEC 签名。从以往的经验来看，这个过程比较复杂，并且容易出错。然而，如今的大部分现代 DNS 软件包和注册系统都配备了相关工具，能够自动对注册人希望发布的数据进行 DNSSEC 签名。这样一来，注册人或其代理只需在其 DNS 服务器（或在其注册服务机构）启用 DNSSEC 签名，并向他们的注册服务机构提供一些信息（称为“*授权签名者记录*”），即可有助于在他们刚刚签名的信息中建立信任。

- **网络运营商**：查询环节的 DNSSEC 实施工作较为简单：网络运营商只需在为用户处理 DNS 查询的解析器上启用 DNSSEC 验证即可。越来越多的解析器软件现在都默认启用 DNSSEC 验证。

- **互联网最终用户**：最终用户除了鼓励他们的网络运营商对他们使用的域名进行 DNSSEC 验证和签名之外，通常不需要做任何事情。

实施 DNSSEC 需要花费哪些成本？

由于发布环节和查询环节的 DNS 服务器都需要支持 DNSSEC，因此，相关组织有必要更新其 DNS 软件包（无论是否部署 DNSSEC ，这都是最佳做法）。

- 对于发布环节，注册人或其代理还有必要修改其流程，以允许将“授权签名者”记录发送给其注册服务机构。执行此类修改的成本较高，不过，只需投入一次成本进行修改即可。

- 对于查询环节，如果 DNS 服务器软件版本较新，那么所需成本应当可以忽略不计，因为可能只需执行一次配置更改，即可启用 DNSSEC 验证。

如果没有部署 DNSSEC，会发生什么情况？

- **用户容易遭到攻击：**如果组织选择不部署或不启用 DNSSEC，他们的用户则容易遭到一种称作“缓存投毒”(cache poisoning) 的特定类型的攻击。最终用户执行查询时，攻击者可能会在 DNS 问题中“悄无声息”地插入应答，从而潜在地将用户的通信意图重定向到攻击者控制的设备中。然后，攻击者会模仿网站或其他服务，窃取用户名和密码等信息。此外，这个不正确的应答信息也会在一段时间内保存在用来查询的服务器上，从而导致这种重定向错误持续发生，直至该应答信息过期或被删除为止。尽管发生这类攻击的情况很少，然而鉴于 DNSSEC 专门用来识破这类攻击，而且 DNSSEC 也已推行了一段时间，因此遭受这种恶意利用的组织可能会因为没有部署 DNSSEC，而不得不面临与用户艰难讨论、尴尬交涉的局面。随着其他的攻击形式不断遭到阻止，攻击者有可能会将攻击目标转向那些尚未部署 DNSSEC 的站点，毕竟，通过 DNS 发起的攻击正变得越来越普遍。

- **创新速度可能减缓：**缺少 DNSSEC 的部署会阻碍创新的步伐，而且对于那些将 DNS 用作全球可信任数据库的新技术而言，也会因此而减缓其部署速度。其中不乏这样的一些技术：承诺可提供更好的方法来信任互联网连接服务（例如，电子邮件或 Web）。

自 DNS 创建以来，它的各种漏洞就一直不断，尽管 DNSSEC 在解决漏洞，然而这些利用漏洞实施的攻击却并没有引起人们的高度关注。因此有些人可能认为，部署 DNSSEC 的成本会超过 DNSSEC 带来的好处。但是值得注意的是，实施 DNSSEC 的成本和风险都已显著下降。事实上，随着越来越多的网络部署 DNSSEC，实施 DNSSEC 的好处会不断增加。

换个角度看待“部署 DNSSEC”的问题：“如果值得花费精力将数据放入 DNS，那么确保这些数据不被篡改怎会不值得？”

关于 DNSSEC 的一些历史背景

1983 年，南加州大学信息科学研究所的保罗 • 莫卡派乔斯 (Paul Mockapetris) 发表了一系列介绍域名系统概念的文档。在 20 世纪 80 年代的 DNS 原型中，它不具备任何内置的安全性、保密性或验证机制；也没有任何机制来确保收到的应答是合法且真正对应于所提出的查询请求。

大约在 1990 年，美国贝尔实验室 (AT&T Bell Laboratories) 的史蒂夫 • 贝洛文 (Steve Bellovin) 撰写了一篇论文，其中介绍了攻击者怎样利用 DNS 中的特定设计决策来入侵系统。贝洛文在论文中建议，使用加密验证机制可以更好地保护 DNS。在贝洛文的论文发表后，经过正式的流程，他的提议成为了 Internet 工程任务组 (Internet Engineering Task Force, IETF) 的一项标准，即“DNS 安全扩展” (*DNSSEC*)。

实现 DNSSEC 技术的 DNS 软件最初于 20 世纪 90 年代末开发成功，关于 DNSSEC 的一些早期部署始于 2000 年左右，其中包括为常见的 .SE ccTLD（瑞典的国家/地区代码）部署这项技术。

然而，这些早期部署揭示了在大规模生产中运营 DNSSEC 会面临着许多技术挑战，这迫使 IETF 在随后的八年不断改进这项协议。

在段期间，部署方面一直没有取得重大进展，直到 2008 年，一位名叫丹 • 卡明斯基 (Dan Kaminsky) 的安全研究员发现了 DNS 协议本身存在的一个严重设计缺陷，该缺陷能让攻击者对 DNS 的查询机制发起缓存投毒攻击。这项发现促使 DNS 技术社群重新尝试部署更多的 DNSSEC，特别是对 DNS 的根区进行签名。

2010 年 7 月，ICANN 首次对根区进行了签名，并为所有 DNSSEC 验证提供了一个全球信任锚。2018 年 10 月，根区的密钥签名密钥首次获得成功更新，这代表着 DNSSEC 的一个重要里程碑。

2018 年和 2019 年发生的一系列国际 DNS 劫持事件，导致美国网络安全和基础设施安全局 (US-CERT) 首次发布紧急指令，敦促 ICANN 再次呼吁所有 DNS 利益相关方全面部署 DNSSEC。

ICANN 在 DNSSEC 中发挥的作用

促进更加稳定、安全且具有弹性的 DNS 生态系统，是 ICANN 肩负的一项使命，长期以来，ICANN 一直是部署 DNSSEC 的主要倡导者。在 ICANN 与注册管理机构和注册服务机构签署的正式运营协议中，要求这些机构支持 DNSSEC。ICANN 组织定期与全球的 DNS 利益相关方开展合作，帮助他们了解 DNSSEC 的重要性，并就如何在网络中部署和运营 DNSSEC，向工程师提供培训。除了提高认知和培养能力之外，ICANN 的技术专家还与 IETF 社群合作，共同对 DNSSEC 技术实施改进。

在运营方面，ICANN 继续发挥关键作用。ICANN 负责生成、存储和定期更新根密钥签名密钥，这是一种受互联网上所有验证解析器信任的加密密钥，可用于对全球 DNS 的根区进行签名。

关于更多信息

大量的资源和技术工作组都在投身于 DNSSEC 及其部署工作。例如：

- 在 IETF 中，尤其是在 DNS 运营 (DNSOP) 工作组中，要讨论 DNSSEC 和所有其他 DNS 协议相关的工作。
- 在每年的 ICANN 公共会议期间，要举办三次 DNSSEC 工作坊。这些工作坊由国际互联网协会负责组织，提供关于 DNSSEC 部署的见解、建议及分析。由国际互联网协会赞助的相关网站提供这些会议的存档。
- 有关更多的信息以及为何实施 DNSSEC 如此重要的原因，请参阅 ICANN 提供的关于 DNSSEC 的一般性介绍。