巴塞罗那 — 人人都学 DNSSEC：初学者指南
中欧夏季时间 2018 年 10 月 21 日星期日下午 15:15 至 16:45
ICANN63 | 西班牙巴塞罗那

韦斯 • 哈达克
(WES HARDAKER)：

… 如果你使用它并将它启用，它将能够保护整个互联网世界的安全。我们将通过一个故事来进行介绍。我们将首先从域名系统安全扩展 (DNSSEC) 的起源说起，这事发生在很久很久以前，大概是公元前 5000 年吧。在互联网出现之前，DNSSEC 就已经存在了。

我们先来介绍乌格维娜 (Ugwina)。她住在科罗拉多大峡谷的这边。可能有人不熟悉科罗拉多大峡谷，那是位于美国中部的一处自然风景名胜。

这位是奥格 (Og)。他住在科罗拉多大峡谷另一边的一个洞穴里。他们两个相隔很远，不能经常见面说话。我曾经穿越过大峡谷，大概要花两到三天时间才能从这一边走到那一边。

在某次难得的见面过程中，他们注意到了奥格家的火堆产生的烟雾。于是他们很快便开始经常通过用户数据包协议 (UDP) 使用烟雾信号来聊天。直到后天有一天，喜欢捣蛋的穴居人卡明斯基 (Kaminsky) 搬到了奥格家隔壁，他也开始发出烟雾信号。我想向那些十年前左右还没有进入本行业的人介绍一下，卡明斯基是真正发现域名系统 (DNS) 的一个严重漏洞的人。

现在，乌格维娜就感觉很困扰了。她不知道应该相信哪个烟雾信号。距离是如此的远，又无法使用望远镜观察烟雾信号是谁发出的，她应该读取哪一个信号呢？

于是乌格维娜走进了大峡谷之中，希望能够找到解决这个问题的办法。乌格维娜和奥格请教了村里聪明的长者。穴居人迪菲 (Diffie) 认为他想到了一个好主意。我向不了解情况的人说明一下，迪菲是公开密钥加密机制的发明者之一，这是当今大多数互联网加密技术的基础。

说做就做，穴居人迪菲马上跳起来并跑到了奥格的洞穴中。他在洞穴的最里面找到了一堆颜色奇怪的沙子，奥格之前从来没有注意到自己的洞穴里原来有这些东西。他跳着冲了出来，向火堆里撒了一些这种神奇的沙子，于是烟雾信号变成了奇妙的蓝色。

现在，乌格维娜和奥格又可以开心地聊天了，因为他们知道只有奥格拥有神奇的蓝色沙子，所以再没有谁能够干扰他们的对话。

刚才我通过幼稚的图表形式对 DNSSEC 进行了一些介绍。现在，我们回头来看看 DNS，它的运行机制和这些烟雾信号有点类似。

DNS 具有树状结构，有些人喜欢这样叫它，当然我们也可以称之为层级结构。这个结构的最上面是根。下面一层是各种顶级域名 (TLD)，包括国家和地区顶级域 (ccTLDs)、通用顶级域 (gTLD) 以及新的顶级域名 (TLD)。然后，再下面一层是实际执行各种操作的注册点。

大家看，底部的中间就是 bigbank.com。我们稍后会提到它几次。根将 com 信息授权给 com 服务器，而 com 服务器将 bigbank 授权给他们的服务器。

作为解析器，当它试着回应你的请求时，例如你问 www.bigbank.com 位于哪里，它实际上并不了解整个树结构。它得从顶部开始查询。

但是它知道根区在哪里，并且能够遍历整个 DNS 层级结构以便找到它。

就像我刚才提到的，层级结构中的每个层级都会指向下一个解析器。所以解析器只能沿着链路往下查找，直至最终获得问题的答案。

解析器会缓存所有这些信息以备日后使用。所以，在实际掌握这些信息后，它可以更快速地回答你的问题，因为它可以在自己可能的期限内长期缓存这些信息。

然而 DNS 存在一个问题。它在设计之初没有整合任何形式的安全性。就像烟雾信号没有整合安全性一样，DNS 也是如此。它天真地认为一切都是准确无误的。域名是很容易被模仿的，而缓存机制是能够长期记住信息的。因此，如果在缓存中找到了错误答案，那它也会长期记住这个错误答案。

这些幼稚的图表还不够说明情况，我们得再演一场滑稽短剧。这个戏真的很搞笑。有人之前看到这个滑稽短剧么？

有几个人看过。好的。其他人可以好好欣赏一下。之前看过的人只能将就一下，再看一遍了。

好的。有谁愿意来当演员吗，请站出来。

好的，我们有几个演员了。我们有一位普通用户，用户乔 (Joe)。请举手。他将在这场戏中扮演用户，他今天要办理一些银行业务。我们有一位根代表，他将充当 DNS 树的根。我们有一位互联网服务提供商 (ISP)，他了解根的位置。我们有 .com，我们还有 bigbank.com。

你可能要站在那边，弗雷德。我现在要将舞台交给他们，请他们开始表演。开始。

男性发言人（姓名不详）： [当] 灯亮起的时候，喂，喂。

韦斯 • 哈达克： 噢，好了。好的，都正常了。这边，帝姆。拉斯要问几个问题。

帝姆 (TIM)： 哇哦！我有这么多钱。我得去把它们存起来。我要去 www.bigbank.com 把我的钱存起来。

男性发言人（姓名不详）： 我不知道它在哪里，不过我可以帮你问问。我从根开始问。你好，你知道 www.bigbank.com 在哪里吗？

弗雷德 • 贝克 (FRED BAKER)： 哇哦。我不知道。不过我帮你想到了一个好主意！你可以问问 .com，他可能知道。他在 1.1.1。

帝姆： 好极了。我去问问他。

韦斯 • 哈达克： [听不清]。好的。抱歉。

帝姆： 有人建议我来问你，你知道 www.bigbank.com 在哪里吗？

男性发言人（姓名不详）： 这个问题问得非常好。我是 .com。我的位置是 1.1.1。谢谢你访问我。我可以告诉你 bigbank 在哪里。在这里。Bigbank 在 2.2.2。你想去那边？

帝姆： 谢谢。我得知道 www.bigbank.com 在哪里。

拉斯 • 芒迪 (RUSS MUNDY)： 谢谢你提出这个问题，ISP 先生。事实上，我可以告诉你 www.bigbank.com 的准确位置。它在 2.2.2.3。

帝姆： 谢谢。Bigbank.com 在 2.2.2.3。太好了！我现在可以去那边存我的钱了！谢谢你，Bigbank！

弗雷德 • 贝克： 我不知道。他应该谢谢你。

韦斯 • 哈达克： 好的。谢谢大家的表演。请在旁边休息一下，我等下还要麻烦大家继续演。

男性发言人（姓名不详）： 你们可不要旷工哦！

韦斯 • 哈达克： 这确实是他们的日常工作。乌格维娜与奥格的聊天就和刚才我们看到的情形差不多，他们分别相当于解析器和服务器。他们通过烟雾信号沟通。这个方法最初是没有问题的，当时没有其他人的干扰。

接下来，我们继续看表演，看看会遇到一些什么问题。请大家继续表演。

帝姆： 哇哦！我现在有一百万，我得把这笔钱存起来。我得去 www.bigbank.com，所以我要先问我的 ISP，“www.bigbank.com 在哪里？”

男性发言人（姓名不详）： 我不知道，不过我可以帮你问问。你好。你知道 www.bigbank.com 在哪里吗？

弗雷德 • 贝克： 我是根，我其实并不知道这么多信息。不过你可以问问 .com。他可能知道。他在 1.1.1.1。

帝姆： 好的。谢谢。你好，.com。你知道 www.bigbank.com 在哪里吗？

男性发言人（姓名不详）： 欢迎你。我是 .com。我可以告诉你 bigbank.com 在哪里。Bigbank.com 在 2.2.2。

男性发言人（姓名不详）： .2。

男性发言人（姓名不详）： .2。

男性发言人（姓名不详）： IPv3？

帝姆： 谢谢。你好，

男性发言人（姓名不详）： 你好。

帝姆： 你好。你知道 www.bigbank.com 在哪里吗？

男性发言人（姓名不详）： 我当然知道，它在 6.6.6.6。

帝姆： 好极了。谢谢。[听不清]

男性发言人（姓名不详）： 好的。www.bigbank.com 在 6.6.6.6。

男性发言人（姓名不详）： 哦，天啊。谢谢！我去存钱喽！

男性发言人（姓名不详）： 谢谢。

韦斯 • 哈达克： 好的。再次感谢。真正的问题在于，我们如何摆脱这个隐藏在银行背后的邪恶先生，从这种可怕的会话中跳出来？

解析器乌格维娜感觉很困惑。这就是大家刚才看到的情况。出现了两种信号。她不知道应该相信哪一个。实际上，在 DNS 中，我们通常会相信首先返回的那个，或者说至少在出现 DNSSEC 之前是如此。

再来看这些图表，如果两个不同的服务器给你提供了两种不同的回答，你得到了两种不同的关于 bigbank.com 位置的回答，这时你就不知道该相信哪一个了。在以上图表中，一个是蓝色，一个是红色。你得自己猜哪一个是正确的。

但是，DNSSEC 能够切实地为 DNS 带来安全性，它使用数字签名来实现这个目的。从本质上说，它可以帮你确认两件事情：那些信息没有被篡改，以及信息源自正确的位置。所以无论存储在多少个位置，无论被缓存过多少次，那些信息都不会被篡改，而且你能知道它来自哪里。

密钥和签名本身也都存储在 DNS 中。由于 DNS 拥有一个查找系统，我们可以轻松查找密钥以及签名，就像其他数据一样，只要有一个可以开始的位置，我们就可以找到它。

概括而言，DNSSEC 的概念就是让解析器不仅知道根服务器在哪里，还知道根服务器的密钥。只要了解了这些起始信息，解析器就能验证树的其他部分。

它通过构建信任链实现这一点。每个层级都会签署下一层级以及当前层级中的数据，直至在链路中找到你所需的答案。

通过这种方式，ISP 处的解析器最终可以确定这最下面的两条 bigbank 记录中的哪一条是正确的，蓝色这条记录是正确的，X 表示恶意记录。

现在让我们通过表演来看看 DNSSEC 发挥的作用。我们今天将做几件事。你现在可以看到这些小徽章。这些表示数字签名。这三个 DNS 服务器都有这些徽章，ISP 拥有对应的徽章，以便他能够验证自己是在与正确的人对话。交给你了。

帝姆： 哇哦！我现在又有一笔钱要存起来。我要去 www.bigbank.com 存这笔钱。

男性发言人（姓名不详）： 好的。我来帮你查一下。

你好，根。你知道 www.bigbank.com 在哪里吗？

弗雷德 • 贝克： 好的。我是根，我可以证明我的话的真实性。但我不知道 bigbank 在哪里。你可以去问问 .com。他在 1.1.1.1。

帝姆： 谢谢。你好，.com。你知道 www.bigbank.com 在哪里吗？

男性发言人（姓名不详）： 你好，ISP。我是 .com。核实我就是 .com。没错！我就是！很好。我可以告诉你 bigbank 在哪里。Bigbank 在 2.2.2。

男性发言人（姓名不详）： .2。

男性发言人（姓名不详）： .2。

男性发言人（姓名不详）： 你好，bigbank。你知道 www.bigbank.com 在哪里吗？

男性发言人（姓名不详）： 当然。不过我没有签名，你不应该相信我。

男性发言人（姓名不详）： 噢，不会吧！再见。你好，bigbank。你知道 www.bigbank.com 在哪里吗？

拉斯 • 芒迪： 事实上，www.bigbank.com 在 2.2.2.3。

帝姆： 谢谢。我可以验证一下你的签名吗？

男性发言人（姓名不详）： 叮！

男性发言人（姓名不详）： www.bigbank.com 在 2.2.2.3，它有签名。

帝姆： 非常好。我现在可以去那边安全地存我的钱了。

男性发言人（姓名不详）： 钱钱！

韦斯 • 哈达克： 好的。这是这个三幕剧的最后一幕，掌声送给他们。说明一下，我们以后需要这一声“叮”来核实各种信息。那简直太好了。

好的。虽然很幼稚，但 DNS 系统和 DNSSEC 的运行原理确实就是这样。当然，实际情况会更复杂一点。但是解析器确实会从根开始一路向下查询。他们接下来要遍历 TLD，然后是各个层级，才能找到最终答案。

但是有的时候，这些层级可能非常深，然而只要有 DNSSEC 在全程保护这个链路，你最后就能获得正确答案，就像蓝色烟雾可以帮助解析器验证就是奥格在发信号一样。

接下来，我要把主持的工作交给拉斯 • 芒迪。我应该先做自我介绍的。我是来自南加州大学信息科学院的韦斯 • 哈达克。拉斯 • 芒迪来自 Parsons，他将向我们详细介绍我们为什么需要 DNSSEC。

拉斯 • 芒迪： 谢谢，韦斯。也感谢所有其他参加演出的人。通过一群新的人员来表演这出戏挺好玩的，因为你们是全新的表演团队。感谢大家参加表演。再次表示感谢。

“人人都学 DNSSEC”会议的这个环节的目的在于帮助大家思考一个问题：在邪恶先生可能随时跳进来搞事情的情况下，为什么任何人都需要进行 DNSSEC 验证，无论是最终用户、ISP 还是权威服务器运营商。因为这就是 DNSSEC 的设计用途。

从 DNS 角度思考问题，我们会发现 DNS 并不负责在用户和银行之间转账。这项活动将通过其他应用来完成。

当有人攻击 DNS 并替换其中的信息时，基本上在所有案例中，他们都会那样做，因为其他应用和功能都是通过互联网发挥作用的。

所以，当 DNS 出问题时，网络浏览器、电子邮件服务器或者其他聊天引擎都将无法正常工作。你无法转到你想要前去或者预期要去的位置。

这便是我们要确保 DNS 正确的根本原因：它必须保持正确，从而使用它的其他应用才能正常运行。

我们这出戏中演的劫持，实际上就是将应用软件引导至用户预期目的地之外的位置。

长久以来，遭受从 DNS 开始的攻击的应用数量已经数不胜数。事实上，某些从 DNS 开始的攻击最终会利用两到四种其他协议。但是它们都是从 DNS 开始，作案者会将 DNS 信息替换为他们希望用户前去的位置，从而他们可以在那里对用户为所欲为。

曾经有一门大学课程会要求 CS 学员实际动手编写一个 DNS 攻击工具。这个课程在互联网上应该已经找不到了，我在过去几年中都没有找到它。我记得是有两家大学开设了两门这样的课程。这个例子可以说明这件事情是如何简单。互联网上提供的 DNS 攻击软件非常多。

但是，这些大学课程的问题在于没有考虑道德问题，至少他们的在线信息中没有提到这方面的说明，他们没有向学员说明即便教授给大家布置了这么一个作业，但大家在实际生活中不应该干这种事情。

所以我们不清楚世界上有多少个劫持软件，但肯定有很多，对于有兴趣编写软件的人来说，这些软件都很容易获得或编写很简单。

就像韦斯在前面提到的，并且刚才的表演中也演了，当用户使用 DNSSEC 时，其理念就是在常规的 DNS 结构中添加加密信息，因为 DNSSEC 是 DNS 的一部分。它完全整合在标准 DNS 中。

当答案的接收者收到一个带有 DNSSEC 签名的答案时，无论是通过本地验证解析器还在应用本身中进行验证，其基本理念都是发出信息查询请求的用户能够得到加密保证，确定信息是来自预期位置，并且没有在传递过程中被篡改。

这让你能够确信自己获得的信息就是应该使用的信息，无论你是在进行网络查询，还是邮件服务器之间的通信，又或者在进行闲聊、Twitter 会话或其他上网活动。

作为 DNS 交换活动的简化示例，这显示了用户乔发出了查询请求。我没有将这些数字更改为我们 T 恤衫上的数字。很抱歉。不管怎样，用户乔向他的 ISP 递归域名服务器发出了一个查询请求。然后这个递归域名服务器向权威域名服务器发出查询，以便弄清楚用户乔想要前往的位置。权威域名服务器将答案传回递归域名服务器，然后他将这个答案传递给用户乔。这便是第一幕剧所演的情形。

接下来，一 哦，抱歉。收到传回的答案后，数据实际是在应用之间传递。所以，用户乔随后与网络服务器对话并在这里完成他的活动。

现在，如果在戏中加入一组带 DNSSEC 签名的区域和验证解析器，你就可以对网站进行定制，指出当前交换的信息事实上就是正确信息。目前，大多数已部署 DNSSEC 的网站都没有这样的指示器，但几年前我们就是这样做的，从而人们可以直接在信息传递过程中看到这条 DNSSEC 链。如果信息传递的底层没有 DNSSEC 链，那就要在传回信息时提供其他指示。

所以网站定制中应该插入攻击指示器。这些攻击就像是邪恶先生，他会观察用户在什么时候发出了查询。递归服务器向权威服务器发

出查询，在权威服务器收到查询之前，邪恶先生便会将答案传递给用户乔。这样，用户乔就会前去错误的位置。他转到了邪恶先生的网站。

与此同时，标准 DNS 查询还在网络上进行，但用户乔的机器已经获得了答案，所以它就会忽略正确答案，并将应用连接至邪恶先生的网站。

在 DNSSEC 加入之前，他将永远得不到正确信息。DNSSEC 加入剧中后，用户乔拒绝了那个错误答案，然后来到了正确位置。

在这里。

那么在这个例子中，这个设计好的网站拥有正确的信息，尽管我们在网站上提供了这种信息，但我们的设计让人们感到像是进入了另一个网站。

这便是验证解析器将得到的信息，也就是大家看到的带有绿色对勾的信息。第一项是，“.org 向 ISP 分享 Comcast DNSSEC 建议。”但非验证解析器会在第一条中看到史蒂夫 • 克罗克会说，“DNSSEC 并未解决全球饥饿问题。”大家看这一页下面的下一项，“.org 向 ISP 分享 Comcast DNSSEC 建议。”

基本上，这些信息是以非常隐蔽地方式插入网页中的，如果不是看到了顶部这个三角形，用户根本不会意识到他们的网站受到了 DNS 劫持攻击，遭遇了内容替换攻击。

你可能会说，“这中间的 DNS 解析量应该不太大吧？”你们看，这是十年前我们通过 CNN 衡量到的数据。这是五年前的数据。只是一

页 CNN.com 内容就会产生如此之多的 DNS 查询。所以查询量是很大的。

DNS 和 DNSSEC 的关键点在于，区域数据本身非常重要。

这个图表显示了这个流程的工作原理，以及需要发生变更的位置。大家可以看到，在最左边，权威服务器中嵌入了区域信息。然后这些信息会出现在 DNS 上。在响应从客户端收到的查询时，中间的递归服务器将与权威服务器通信。

客户端，就是 .1，这第一个箭头，1。2，递归服务器查询权威服务器。3，权威服务器响应递归服务器。然后递归服务器响应客户端。

在实施 DNSSEC 时，你将在某些步骤中添加客户数据和功能。在实施这个机制时，不论您是否负责运营还是负责管理这部分 DNS，实施工作都取决于您在 DNS 整体架构中的位置，以及您需要做些什么。那些需要涉及 DNS 更深更广的活动的机构则可能希望自行完成所有任务，因为它们拥有可以胜任 DNS 业务的员工。

如果您负责的工作的规模和复杂程度与 DNS 拥有紧密联系 – 您在这里可以看到一些例子，比如[大型]注册管理机构、大型企业、非关键 DNS 根区（这些部分运营简单、规模较小、处理容易） – 这些机构类型可能希望自行完成大部分工作。再次强调，请谨记保护 DNS 根区数据是关键因素。

在最后一张图片中，这里显示了我们需要在哪里添加区域信息，以便实施这个 DNSSEC 签署和验证功能。我们可以看到，权威服务器所有者负责将签名信息添加到系统中。然后这些信息才会纳入查询

响应中。然后，底部这个验证递归服务器将实际执行验证，然后指示说，“对的，它是正确的，它经过了加密。”

如果你目前与之打交道的组织需要实施大量 DNS 活动和功能，需要高度关注 DNS，那么你们就需要自己在内部实施 DNSSEC。

如果组织的活动基本不涉及 DNS 的核心功能，你们可能拥有 IT 部门，或者将 IT 外包给其他组织，那么你应该咨询各个提供商，了解应该由你们的 IT 部门还是外包供应商来实施 DNSSEC。如果他们没有说，“你需要学着自己实施，否则我就不和你做生意了”，因为现在的 DNSSEC 业务领域有许多专业人士，你可以选择通过外部供应商来实施 DNSSEC。

主要演示就是这些。我们准备进入开放问答环节。我们将 — 是的，我现在将麦克风切换给韦斯，由他继续主持会议，在座的既有许多 DNSSEC 从业人员，也有许多对 DNSSEC 拥有深刻了解的人士。

如果大家有任何问题，请直接发问。我们很乐意回答大家的任何问题。

韦斯 • 哈达克： 好的。DNSSEC 还没有 — 这个怎么样？没有。是的。我得重新把麦克风打开。

测试、测试、测试、测试。测试，噢，好了。好的。好的。这个怎么样？好的。我们有两个麦克风。随便用哪个都可以。

DNSSEC 并不简单，实际上很复杂。我相信大家肯定会提出很多问题。我们专门为这个环节安排了足够的时间来回答问题。许多曾协

助创建 DNSSEC 的专家都来到了现场，如果大家有什么问题，我们应该能回答。

现在有谁要提问？请举手示意，我会将麦克风传给你。

阮清 (THANH NGUYEN)： 大家好。我是来自越南的阮清。感谢你的演讲。非常有帮助，有非常多的信息[听不清]DNS。

我看到有很多的[听不清]DNSSEC，在部署[听不清]以确保国家和地区顶级域以及通用顶级域的安全，但我认为，在 DNSSEC 中实施时，需要考虑[听不清][一些挑战]。似乎你需要有[听不清]DNSSEC、DNS 签名、域签名，还有一些步骤，我记不太清了。

但是基于这一步，我认为黑客或[听不清]可以通过 DDoS 发动攻击，利用 DNSSEC 的弱点，比如 DNSSEC 的时间同步问题，因为它需要时间 — 首先，你会抛出 DNS 系统的一些额外点，但需要时间等待响应。所以黑客可以基于这个弱点，攻击 DNSSEC 系统的间隙。

对于这个问题，你们有解决方案吗？

韦斯 • 哈达克： 我觉得你问了好几件事。首先，你问的是，用户在请求数据时会不会有更长的延迟，对吗？由于你请求更多的数据，因此 DNS 查询工具被拖慢了一点。确实，只是一点点…最关注这方面的用户是那些使用即时应用程序的人，他们需要执行大量的 DNS 查询，他们需要查看所有的响应，以及速度如何。所以通常，那是网页浏览及类似的东西。

要记得，由于缓存的存在，那只会拖慢一次查询，而之后的所有剩余查询，包括安全记录，都会被缓存。

所以初始查询可能会有毫秒级的迟缓，但它随后就会被缓存。所以通常如果能看到延迟，只会是 ISP 的一个用户在前往某个网站时看到一次。

我觉得你问的另一件事是说，有些 DNSSEC 记录非常大，它们可能会让放大攻击有机可乘。

所以，如果你向 DNS 服务器发出请求，而它返回了一个比较大的响应，如果在发出的位置作假，那么响应就可以发给错误的人。

对于这个问题，通常的解决方案时是响应率限制，如今的大部分 DNS 服务器都不会允许你一次查询过多记录。也就是说，如果你尝试在一秒钟内查询 100 个记录，那么你的行为就是有问题的，我将停止响应你。

这就是目前普遍采用的解决方案。我实际上负责其中一个根服务器的运营。在我们启动服务器的瞬间，我们一下子收到的请求并不多。那是多年以前的事情了。现在已经是不存在的问题了。

安德鲁 (Andrew)，我想 —

安德鲁 • 弗雷泽 (ANDREW FRASER)： 是的。沃伦 (Warren) 要补充吗？

沃伦 • 库马里
(WARREN KUMARI)： 没有。

安德鲁 • 弗雷泽
(ANDREW FRASER)： 没有？好的。

韦斯 • 哈达克： 好的。

沃伦 • 库马里： [听不清]攻击者发出响应[听不清]。

韦斯 • 哈达克： 你想要坐上来吗？欢迎这个房间里的专家来坐到桌子前 … 继续。

埃伯哈德 • 布劳赫
(EBERHARD BLOCHER)： 大家好。我是来自德国的埃伯哈德 • 布劳赫。我不是专家。我是完全的门外汉。

韦斯 • 哈达克： 没关系。

埃伯哈德 • 布劳赫： [听不清]。我有个关于历史的问题。我知道 DNSSEC 已经存在很久了，我想应该十年前就有了。有人跟我说是史蒂夫 • 克罗克创建或者参与创建了它。

现在我了解到，经过这么久的时间，我们现在正面临新的情况。今年，我域名业务的所有最终客户都在要求 SSL 加密。现在我们开始免费提供加密服务。所以基本上，这是另一种保护网站的方式。

我理解 SSL 证书只能链接到一个域名，那么问题来了，我们仍然还需要 DNSSEC 吗？或者 DNSSEC 加密和 SSL 加密的网站之间有什么区别？

如果我使用了 SSL 证书加密网站，为什么还需要 DNSSEC？

第二个问题是，我已经看过了统计数据，我知道许多注册管理机构都提供有多少域名采用 DNSSEC 加密的数据。而有些注册管理机构的渗透率则非常低。为什么会这样？另外，还是同样的问题：我们还需要 DNSSEC 吗？

韦斯 • 哈达克： 非常好的问题。在互联网安全性方面，最难的事情之一就是你不能孤立地解决一个问题，因为你会发现所有事情都是息息相关的。

比如说，如果你执行 DNS 查询，假设你前往的是 SSL 加密网站。你知道，只要能访问到，你就会抵达正确的网站。但事实上 DNS 在那之前就介入了，它将把你重新引导至一个完全错误的位置。

那就会产生很多问题。第一，你会被引导至错误的位置，而且也将永远无法抵达正确的网站。路由也有同样的问题。所以，如果不对路由层和路由基础设施加以保护 — 事实上互联网就是建立在一个堆栈上。堆栈中的每一层都需要被保护，从而为最终用户提供完全保护。

是的，我们仍然需要 DNSSEC。

你想要谈谈 DNSSEC 的历史和创建过程，或许还有 DNSSEC 的部署和史蒂夫 • 克罗克吗？有许多人都对 DNSSEC 贡献良多。史蒂夫确实提供了帮助，不过…

拉斯 • 芒迪： 是的。DNSSEC 的设计、实施和部署是一段很长的历史。正如韦斯所说，它的目标是确保 DNS 发挥作用，为用户带来正确的答案。

现在，使用它的应用程序会相对[独立]。实际上主要的工作发生在 1993 年，DNSSEC 开始被开发、设计和布局。当时有很多电话往来。在这些电话往来中，史蒂夫 • 克罗克就是其中一位涉及其中的人员。我也其中一位。

不过那之后还进行了多次重新设计，因为这是史上第一次真正地将运行中的安全能力插入一个运行中的协议。前两次的设计存在一些严重问题。第三次才大功告成。

2010 年，根区被签署。在那之前，有多个顶级域被签署。

所以，有很多人都做出了很多贡献。也有许多组织为此付出了巨大的努力。不过为了避免这张幻灯片上的事情发生，不管是否使用 SSL 证书，在认证机构方面都有足够多的挑战，还有错误证书或坏证书的问题，事实上这确实会导致一些后果，并且让网站接触存在问题的认证机构，而用户仍然会去到 SSL 签名的网站。

韦斯 • 哈达克： 另一件要注意的事，在域名查询方面，网页并不是唯一需要保护的机制。电子邮件就是很好的例子，传统的证书系统并不能解决问题。

在周三举行的 DNSSEC 工作坊中，所有相关内容都会被讨论到，我们可以在那时再做讨论，欢迎大家前来参加。那是全天的活动，不仅仅只涉及 DNSSEC。

我将会谈到 DNSSEC 是真正能够保护网络服务器免遭中间人攻击以及保护电子邮件不被窃取和误发到错误位置的唯一可行解决方案。常规的 TLS 证书在这方面无法提供帮助，至于原因我会在那天解释给大家听。相当复杂。

安德鲁？

艾哈迈德 • 阿尔萨德 (AHMAD ALSADEH)： 我是艾哈迈德 • 阿尔萨德。我是英才计划学员。我想问的是，为什么它不像 DNS 一样被广泛部署。为什么有人不部署 DNSSEC？这是第一个问题。

另一个问题是，你们认为像区块链这样的新技术能够成为保护 DNS 的解决方案吗？谢谢。

韦斯 • 哈达克： 分开两部分回答。第一，有其他人问过为什么有些注册管理结构部署的更广泛，以及类似这样的问题。是个很好的问题。似乎世界上每个地区的部署程度都不一样。

有些 TLD 会提供财政激励，促使你签署区域，尤其是瑞典、捷克还有其他一些国家。所以他们的接受程度较高。

但越来越来的技术涌现，都有激励吗？当地有真正推动公司使用这项技术吗？所以，采用率已经普遍放缓。

重申一下，如果你周三来参加，我会提供一些数据统计，不过现在很难这样做。目前已经签署的区域数以百万计。所以即使由于域的数量众多而显得百分比例较低，但实际上我们已经部署了数百万例。比如，85% 的 TLD 已经签署。不过，要让全世界都切换过来，还需要很长的一个过程。

拉斯 • 芒迪： 我来补充一下，其中一项原因并不仅仅在于 TLD 和二级域。最终用户、企业对 DNSSEC 的需求也不算热切，因为大部分时间他们并不会意识到 DNSSEC 对他们的实用性有多高。

不够在过去的五年间，美国政府和其他一些国家政府已经站在了相似的立场，就像以前他们在制定要求签署所有 .gov 域时所做的那样。不过美国是我最熟悉的。

他们现在还要求所有的域必须经过验证。所以一些组织正在推给最终企业。比如说，我工作的公司 Parsons，parsons.com 就是一个签署的域并以那样的方式运营。

所以要继续普及知识，鼓励更多的人发出请求。因此你会看到有很多地方说：“请让你的 ISP 或提供商，或者任何为你提供 DNS 服务的供应商为你提供 DNSSEC 能力。”

韦斯 • 哈达克： 而且，很多现代注册服务机构和注册管理机构只需要按下按钮即可。如果你要让他们托管你的 DNS，只需要点击按钮，然后你就会获得一个签名的根区。这非常简单。

不过，对于许多自己运营内部 DNS 的人来说，部署任何安全性机制都需要付出一定的成本。无论是 TLS 证书或是 DNSSEC 或其他什么。你必须学习。你必须着手去做。现在有很多工具可以让这部分工作变得更容易，但十年前并非如此。那时这样的工作还是非常技术型的。

还有其他问题吗？能听到吗？

男性发言人（姓名不详）： 早上好。我的问题是，你们对上周的密钥轮转有怎样的评论。

我的另一个问题是，是否有计划为浏览器添加一个到 DNSSEC，到域的签名？

韦斯 • 哈达克： 密钥轮转在上周执行，这是史上第一次。进展非常顺利，结果也非常好。

约翰 (John)，你想就此发表意见吗？

约翰 • 莱文 (JOHN LEVINE)： 我来回答下一个问题。

韦斯 • 哈达克： 好的。你来回答下一个问题。密钥轮转进行的非常顺利。有一小部分受影响的 ISP 实际上并没有更改他们的密钥，但通常，网页浏览器并不需要那个密钥。ISP 才需要，就像那天你看到的那样。作为网页浏览器的用户 Joe User，实际上并不需要做什么。他甚至不需要知道 DNSSEC 是什么。

不过，还有一个另外的问题，如果你在咖啡店使用无线网络，而你的 ISP 使用 DNSSEC，那么那里会被保护吗？那完全是另一回事。

但通常，只有 ISP 才需要知道新的密钥。

就 ICANN 的未来流程而言，密钥会被再次轮转吗？是在什么时候？这些问题将会在本周稍后时间进行讨论。我们将会得出一个决议，确定密钥轮转的频率如何？还是说以相同的方式来轮转？轮转密钥的机制是怎样的？

所以在吸取了这次的经验之后，还会有很多事情需要确定，毕竟只过了一个星期或一个半星期。

拉斯 • 芒迪： 韦斯，我还想补充一句。在决定下次密钥轮转的相关事项时，一定会征询社群的意见。ICANN 中的组织 — 英联邦电信组织 (CTO) — 非常渴望得到来自社群的意见。所以如果你们有任何内容贡献提案、创意或想法，他们一定会愿意听。我们将会设立多项机制来征询社群的意见，请大家都积极思考，贡献想法。

韦斯 • 哈达克： 重申一次，在周三的 DNSSEC 工作坊，将会有关于密钥轮转的演示。

约翰 • 莱文： 你好，韦斯。我是约翰 • 莱文。我要提一个我一直在问的同样问题，我为大约 300个根区托管 DNS[听不清]。其中有一半左右，由我担当注册服务机构分销商。所以我实际上可以直接接触注册服务机构。这些注册服务机构都在使用 DNSSEC 签名。

对于另一半根区，我是第三方 DNS 提供商。有了全球最优秀的[听不清]，目前对于所有其他用户而言，唯一能够开展 DNSSEC 工作的只有注册人，或者具有注册人凭证的人。所以，要么我得让我们用户们完成安装 DS 记录的过程，这对你我而言相对容易，但对所有人来说并不必要；要么我得为他们的注册服务机构帐户获取凭证，但我并不愿意这么做。

我知道这个问题可以在注册服务机构层面解决，通过添加一些 DNS 更新服务联系人，或者也可以在 IETF 中解决，通过设置一些自动化程序。

然而这两种方式都未见进展。我意识到可能是因为这不是最常见的问题，但是我觉得第三方 DNS 提供商并不算少，我们需要解决这个问题。

韦斯 • 哈达克： 是的。你说的没错，我们需要在这方面有所作为，尤其是为了这么一群运营大量根区的人。我自己也运营有根据，这些问题我都亲手解决了。已经有人在处理。情况会越来越好。

我可以透露的是，在过去的几年已经有一些工作在进行了。有些提供商创建了一个按钮，如果你要发布 DS 记录，只需要点击密钥并说“这是正确的那个吗”，不再需要粘贴进去了。然后它就会为你找到。

你可以跟两个人聊聊：你应该抽空跟沃伦 • 库马里聊聊，或者是[奥利佛]，他创建了 CDS 记录，这是一种自动更新密钥并在 DNS 中子区和注册服务机构之间传达。

不过，我知道 —

约翰 • 莱文： 是的，但它不会安装。只会更新。[听不清]

韦斯 • 哈达克： 我们有一个关于完成“初始信念的飞跃”或类似事情的讨论。其实上个月讨论过很多：人们开始 — 你为什么不上来，沃伦？我应该让沃伦来谈谈。不过，人们现在更多是在谈论推动技术产出。所以最终我开始看到有人说，让我们实施这个。谁实施了它？实际上，这是最近才刚刚出现的情况。

你想要发言吗？

男性发言人（姓名不详）： 是的。

韦斯 • 哈达克： 让沃伦先发言吧。

沃伦 • 库马里： 不，你先发言。

男性发言人（姓名不详）： 是的。我想说的是，这些天至少有两到三个国家现在已经（推进 CDS 记录）：捷克共和国、瑞士和列支敦士登。所以在那些国家，如果你有一个域并且在你的根区显示了一个 CDS，那么它就会被注册管理机构采用，然后[整个]链条就准备完毕了。

所以至少现在已经开始有些尝试了，当然这也证明了它将成为被 .com 所支持的全球性倡议。不过，那可能只是开始，我们可以从中学到很多。在本周的 DNSSEC 工作坊中将会有一场相关演示。邀请大家参加。[听不清]。

韦斯 • 哈达克： 所以还有些工作要做，不过好消息是，我们目前有了向前冲的动力。是的，正如他所说，周三有一个专家组参与。

鲁道夫 • 丹尼尔 (RUDOLPH DANIEL)： 嗨！大家好。我是鲁道夫 • 丹尼尔。现在是 ICANN 英才计划的学员。

韦斯 • 哈达克： 欢迎。

鲁道夫 • 丹尼尔： 我不知道我的问题是否合适，不过刚刚提到了密钥签名密钥轮转。我想知道，目前一切顺利，但那些旧的密钥已经被抹掉了吗，还是仍在运行中？

韦斯 • 哈达克： 问得好。我要讲两点。目前来看一切顺利。缓存中的数据可存活时间 (TTL) 只有两天。现在已经过去十天了？具体时间我忘了。嗯 — 是。我会做算术。十天。21 减 11。现在已经过去十天了，也就意味着应该没有 DNS 解析器再保留了。他们必须更新信息，他们应该能注意到失败的情况，除非他们运行的内容非常破碎。

我们已经有所进步，现在任何人都应该能注意到失败的情况。

至于移除旧密钥，涉及两个方面。一，根区仍然有旧密钥，但并未使用。它只是安静地待在那里，并未被使用。

在 1 月 11号，它将被标记出来。旧密钥上的标签将会更改，表示“现在已不再信任该密钥。”这就是所谓的撤销比特。换句话说，你撤销了对它的信任。这将在另外三个月后发布出来，也就是 4 月 11日，旧密钥将从根区完全移除。

所以密钥轮转流程还未完全完成。目前来看，我们将不会再切换回使用旧密钥，因为密钥轮转似乎一切顺利。

好的。问得好。谢谢。

男性发言人（姓名不详）： 早上好。如果我们[听不清]使用 DNSSEC 的站点的话，是否有计划在浏览器中集成给用户关于证书的通知？

另一个问题。我会提议我的客户使用 .com 而不是通用顶级域，因为它们在通用顶级域中是未签名的。这可能其他域名业务的市场推广更加相关，需要加速实施 DNSSEC 的速度。

我的问题是，我们是否有计划向用户显示他们所访问的是正确的站点？

韦斯 • 哈达克： 抱歉，最后的问题是什么？计划显示什么？

男性发言人（姓名不详）： 在浏览器中。[听不清]，我们可以看到[听不清]签名 … 我在幻灯片中看到一则浏览器中的通知，我看到了一幅浏览器的图片。也许它是在浏览器扩展或其他类似程序中集成的？

韦斯 • 哈达克： 你是在说那个吗？没有？好的。你们确实可以安装一个浏览器扩展，叫做 DNSSEC … 名字记不太清了。如果你搜索适用于 Chrome 和 Firefox 的浏览器扩展，就会找到可以在浏览器中安装 ICANN 的扩展。

浏览器供应商对于直接在他们的浏览器中执行 DNSSEC 的兴趣不大。这个就说来话长了。你们可以联系他们投诉一下。

哦，DNSSEC Validator，谢谢你，蒂姆。那个扩展的名字是 DNSSEC Validator。找到之后，就可以安装了。拉斯和我在很多年前曾经为某个浏览器做过将 DNSSEC 植入浏览器基础程序库的工作。那款浏

览器叫做 Bloodhound。顺便说一下，它并未被更新，所以并没有新密钥。当时它是应用在 [Twitter] 上。

拉斯 • 芒迪： 是的。我们需要研究这件事。

韦斯 • 哈达克： 是的。那实际上会特别修改 Firefox，使其直接在浏览器底层 DNSSEC。在电子邮件和其他事情上还有很多应用。我会在周三详细谈谈，到时候你们可以看到很多关于电子邮件的趋势图表，对[听不清]的使用已经越来越多。

巴里 • 雷巴 (BARRY LEIBA)： 在告诉用户这一点方面，长久以来有很多证据表明，用户并不知道他们已经被告知了，并且对于并不知道 DNSSEC 是什么的用户而言，尝试告诉用户他们这件事并不必要。这样做并没有什么意义。

韦斯 • 哈达克： 是的。换句话说，现在的普遍做法是：你只需要给出一条错误消息，也不必给给他们继续或停止的选择。只要阻止他们前往即可。有很多证据表明，通常最终用户并没有足够的知识来做出良好的安全性决策，所以不要让他们来做安全性决策。直接拒绝即可。

在你后面，安德鲁。

男性发言人（姓名不详）： 是的，不过我只是想说，这并不意味着我们不需要告诉最终用户并向他们解释出现这条消息的原因。它不应该是一个横幅或被阻止的内容。它应该是一条稍微带点解释性的消息，因为，如果是第一次出现，那么，可能还比较新奇。你不知道它是什么。但如果消息是带有解释性的，在某种意义上，它可能是个很好的方式，在下次出现时，就会有所帮助，或者…

韦斯 • 哈达克： 是的。这一点长久以来都是一项安全性争论中，关于在多大程度上让用户自主操作。我个人作为一个技术极客，当然希望他们永远都会给我一个尽可能显示最多信息的选项。但是我有很多不懂技术的亲戚朋友，他们只能求助于我。所以这个是需要全面考虑的。

其他人还要提问吗？

男性发言人（姓名不详）： 我想提个问。我们有很多问题。我们可以在本地主机中存储，也可以托管[听不清]。如果我们可以在浏览器中看到通知…我不知道是否[听不清]代理，我们可以让任何其他问题拥有获得签名优势的先机。所以这对寻找用户，以及让互联网的许多问题[听不清]很重要。

韦斯 • 哈达克： 是的。所以今天我们才讨论域名。如果代理也使用 ISP 的解析器并且经过验证，则它也将被保护。你是对的，在 HTTP 类型的机制或在邮件和所有其他东西中，存在着多个层和多个缓存。所有这些

DSN 查询都需要经过验证，以便获得完整的安全性链条。你说的没错。

在你后面，安德鲁。总是在你后面。你提示过吗？

何塞 • 阿尔韦托 (JOSE ALBERTO): 大家好。我是何塞 • 阿尔韦托。是 ICANN 英才机会的学员。

我的问题与 Tor. 有关。[我们时候使用 Tor，DNS 安全性也适用于 Tor 吗？]它适用于 … 我不知道。这可能吗？还是说他们在 DNS 中采用另一种安全性？

韦斯 • 哈达克： 这是个很好的问题，也提醒了我好像跳过了前面的区块链问题。在互联网中，还有另外的命名系统正在使用。相对没那么普及。Tor 是其中一种。实际上还有一种 Namecoin，这是基于区块链的命名系统。它们域 DNS 不兼容。所以，DNSSEC 只保护 DNS — 常见的命名解决方案。并不能阻止其他机制被使用。它不能阻止他们拥有自己的安全性系统。

我不认为 DNSSEC 适用于 Tor。在理论上它是可以的，因为 Tor 的运作方式与 DNS 类似。很遗憾，我不是 Tor 专家。还有其他补充吗？

我没有足够的信息来回答。好的。

我猜可能没有，可能现在没法帮忙回答。你最好去问问更熟悉 Tor 的人。很遗憾，这里目前没有 Tor 专家。

帮不上忙。好的。我们有了确切的答案。帮不上忙。

林方杰 (FAN-CHIEH LIN)： 大家好。我来自台湾中华电信的林方杰。也可以叫我 Jason。又是我。在我的理解中，DNSSEC 专门用于保护 DNS 事务。我读到一篇文章声称 DNS cookie 被 [RFCs、MTAs、MT3] 和引入。是否存在更轻量级的方法？能否请你们分享下关于这种言论的看法？

谢谢。希望我没有跑题太远。

韦斯 • 哈达克： 没有，很好。DNS cookie 解析是一个完全不同的问题。我想纠正一下你最开始说的那句话。稍微有一点错误。不是完全错误，不过你说它保护事务。DNSSEC 并不保护事务。它保护数据。

让我来举个例子。如果我传递给拉斯某些 DNS 信息并且说：“在 DNS 之外，我准备告诉它我的主机名是 1.1.1.1，这是我的签名。”则他可以将此信息给到整个房间，并且它可以验证所有返回的途径。实际上它自己就锁定了数据。

我并不关心它是如何传输的。可以是通过 DNS。也可以通过信鸽。都没关系。DNSSEC 保护的并不是连接。而是数据本身。

这很重要，因为 DNS 中的缓存，有时可以有多重跳跃。如果你使用 Google 的 8.8.8.8 解析器，他们有多个主机来组成系统，并共享一个缓存。

跟谁来询问谁来回复没有关系。只有最终可以验证数据，得到的方式并不重要。

Cookie 机制专用于保护单项事务，通常这样的事务非常大，能让您从服务器获得更大的回复，避免拒绝服务之类的事情。服务器可能会要求您返回 TCP 或其他不可能被仿冒的内容。

这是 Cookie 所能处理的另外一件事。它并不保护 DNS 事务中的数据。

男性发言人（姓名不详）： 大家好。据我了解，为了保护 DNS 数据，我们有两种机制。第一种是 DNSSEC，而第二种是通过 TLS [听不清]的 DNS。

通常我们看到 DNSSEC 非常普遍，比 TLS 上的 DNS 更加普遍。能否比较一下这两种机制？DNSSEC 相比另一种，最有利的特征是什么？谢谢。

韦斯 • 哈达克： 它们两者的目标也不同。DNSSEC 是为了保护数据。所以它并不关注数据是否通过 TLS 传输。你怎么得到数据并不重要。

TLS 上的 DNS 设计用于保护某人提出请求以及从哪儿获得回复这两者之间的事务。

如果你的网页浏览器请求你的 ISP，就可以通过 TLS 连接，从而确保其他无关的人不会看到你的请求。但是你并不知道 ISP 的解析器是否能够通过 TLS 向根区和 bigbank.com 发出请求。

DNSSEC 保护完整性，你是否得到了正确的回复。TLS 上的 DNS 设计用于保护隐私，确保没人可以看到你的请求和你获得的回复。

也许有一天，TLS 将被普遍采用，但由于多重跳跃的存在，你仍然不知道你从 A 到 B 到 C 到 D 获得是数据是否被保护。DNSSEC 则提供这样的安全性，无论有多少重跳跃，你都知道数据是正确的。

肯 • 赫尔曼 (KEN HERMAN)： 嗨！大家下午好。我是肯 • 赫尔曼，一名独立顾问。好吧，现在我被 DNSSEC 的价值说服了。

韦斯 • 哈达克： 哈哈！

肯 • 赫尔曼： 你能谈谈渗透率水平吗？有多少人在用它？组织甚至个人如何能知道 DNSSEC 已经建立了这样的信任链？

第三，请你谈谈组织实施成本？对于依赖 ISP 的小型商业用户来说，可能成本不宜过高，对于大型组织而言，也许可以高一点。谢谢。

韦斯 • 哈达克： 所以请来参加 DNSSEC 工作坊。这次的 DNSSEC 工作坊将在周三举行，相比以前的惯例要晚一些，通常在每次工作坊的第一场演示中，会有大量的地图和数据，展示全球哪个地区使用率最高，还有类似的内容，包括：我会发表关于域[听不清]数量以及 DANE 部署情况的演示。还有很多技术信息。我就不再重复了。[听不清][电池]。所以请前来参加。

至于 … 问题的第二部分是什么来着？

肯 • 赫尔曼： 成本。

韦斯 • 哈达克： 哦，成本。过去更难实施。如果你要求 ISP 转向 DNSSEC 验证，他们可能不会听，除非有人这么要求。当有很多人都这么要求时，他们才会这么做。而现在，对他们来说几乎不需要进行配置就能启动 DNSSEC，所以他们没有太多借口，除了说他们需要知道在中断时如何调试。他们需要知道密钥轮转时发生了什么。

现在大部分工作都应该可以自动完成了。以前可不是这样。你得了解更多知识。现在就很明了了。

在刚开始能够对根区签名的时候，如果你要自己做，你得要托管自己的 DNS，得要自己前面，这些需要一系列操作，大概 12 个命令。我们在早期的配置指南中有存档。过程非常冗长乏味。拉丝和我曾经共同工作。我们跟同事们一起开发出一个工具。只要运行 [zone-signer-space-file name] 就能搞定，然后你就可以发布结果了。

工具让很多事情变简单了，成本也就更低了。但是，并没有零成本的安全。在某种程度上安全性总是有的。

关于 DNSSEC 还需要知道的是，如果你要自行配置，以前使用的 DNS 是一种发布并忘记方式。你不再必须修改根区。只需要一次性发布它。你可以放任三年不管，数据仍然完好。

而 DNSSEC，由于它是有时间限制的，你必须每个月或在你选定的时间周期内重新签名。通常是一个月。我自己的根区每两周重新签名一次，即使安全链接足以应对一个月。

男性发言人（姓名不详）： 我想谈谈对你刚刚说的，例如 Knot 解析器对你的根区做了最终签名 … 如果有系统发布 CDS 记录，过去就是这样的。只要发布一次，所有的自动化机制就会搞定安全性。所以，成本就真的非常低。

韦斯 • 哈达克： 是的。你说的非常好。只需要告诉你的解释器 — 我认为大部分授权解析器现在都已经在自动签名 — 它就会一直为你签名。要让全部工作自动化，涉及一大串东西。

我是偏执狂。我在我自己的笔记本电脑上完成了这些工作，那是因为我开了头就不想停下来了，现在不会了。

还有其他问题吗？你们的问题都非常棒。非常感谢。

阮清： 我还有一个问题。不是个技术问题。对于一个特定国家，比如我的祖国越南，举个例子，在我们政府自己的 DNS 系统中，[听不清]。我们想要将所有的 DNS 系统更改为 DNSSEC。从 DNS 转到 DNSSEC 需要多少费用，多长时间？你能估算一下时间和成本吗？

韦斯 • 哈达克： 很难估算，我不太确定…

拉斯 • 芒迪： 让我来说两句。我没法给出一个精准的回答，但可以给你一个思路。

当人们开始实施 DNSSEC 以及进行设置和投入运行时，常常会发现一件事，他们会发现他们的 DNS 软件未正确更新。

所以，事实上他们可能在权威域名服务器，或者如果也运营 ISP 和递归域名服务器的话，他们可能已经落后三年、五年甚至十年了。所以大部分情况下，第一步就是检查你们的 DNS 基础设施。

如果基础设施良好并且时新，而且软件也不落伍，那么实施 DNSSEC 的挑战就很简单了，只需要在给权威服务器进行实际分配的隐藏主服务器的配置文件中更改一到两个选项设置即可。

如果你想要设置单独的离线加密机制，则会相对更复杂一些。

但不管怎样，首要也最重要的是查看你的 DNS 基础设施。从这一步开始。线上有大量信息可用。这么久以来，DNSSEC 社群已经做出了非常不可思议的分享工作，线上已经有海量信息，关于在国家范围内如何开展实施工作。

韦斯 • 哈达克： ISOC 已经接管了你们之前看到的网站，那个网站已经部署了 DNSSEC，就是张贴了史蒂夫 • 克罗克照片的网站。那是关于 DNSSEC 资源的门户网站，可以帮助你走好接下来的路。所以，那是个信息丰富的好网站。

我的那个 DNSSEC-Tools 就稍微有点极客。不过也可以告诉你们的注册服务机构。很多注册服务机构都有工具，如果你让他们托管数据，而他们也运行 DNS 服务器，那么可能简单到只需要勾选复选框。

所以成本多少取决于你要做什么。你必须得先做拉斯刚刚提到的评估。开始先弄清楚要做什么，然后再算出需要多少成本。

鲁道夫 • 丹尼尔： 嗨！又是我，鲁道夫，ICANN 英才计划学员。我刚刚想起来，我看到过一个名为 EDNSSEC 的东西。有这种东西吗？

韦斯 • 哈达克： 我认为你可能搞混了。EDNS，没有 SEC，是 DNS 机制中的一个扩展，用于在你请求信息时增加额外信息。

实际上就是在那里，你说：“我想要执行 DNSSEC。请给我所有的签名和各种东西。”所以，那是 DNSSEC 所需的 DNS 内部扩展机制。

鲁道夫 • 丹尼尔： 哦，好的。谢谢。

韦斯 • 哈达克： 最后问一下，还有人有问题吗？巴里 (Barry)？

巴里 • 雷巴：

如果还有一点时间的话，我想重复一下之前关于 DNSSEC 和 HTTPS 的问题。

最开始，你并不常常访问 HTTPS 网站。你会去到 HTTP 网站，然后被重定向。而攻击者可以避免你被重定向，并骗你进入不使用 HTTPS 的网站。所以你仍然需要验证。

然后我们弄出了所谓的“强制安全传输”(Strict Transport Security)，这样当你前往网站时，它会接收指令“使用 HTTPS，总是使用 HTTPS，不要接受没有 HTTPS 的连接。”那使用了一个称为“首次使用信任”(trust-on-first-use) 的技术，假设攻击者不会拦截第一次请求。

为了避开那样的攻击，现在的浏览器中置入了一份强制安全传输列表，所以你甚至不需要首次使用信任。你永远不会尝试访问那个网站。

但是你还会遇到无赖的 Ca，正如拉斯提到的那样，如果查看浏览器，看看浏览器信任了多少根区认证机构，就会发现成百上千，从 Verisign 到一些你根本没听说过的台湾公司。

如果它们中的任意一家被攻陷，并且发出一张针对 bigbank.com 的证书，那么你也会被攻陷。

为了避免那样的事情，我们现在有了 DANE，在那里银行在其 DNS 中发布其自己的记录，并且指示：“这些是我想要你使用的证书。”那就避免了那样的问题，但你猜 DANE 需要什么？DNSSEC，因为你正获得 DNS 以外的证书。

所以这是一个循环，而且如韦斯所说，所有事情都被分层了。你需要保护这一路上的每一个环节。

韦斯 • 哈达克： 现实是，如果用户在任何应用程序、网页或其他地方的字段中输入的第一个内容是一个域名，则该域名就会被查询。所以，那是第一个漏洞。所以虽然有其他方式可以避免所有那些类型的问题，但它们也都有问题。不过，如果你对 DNS 提供保护，那么实际上所有的问题就都不复存在了。

那并不意味着你不应该使用 HTTPS。它解决的是不同的问题。

还有其他问题吗？

艾哈迈德 • 阿尔萨德： 我是艾哈迈德 • 阿尔萨德，ICANN 英才计划学员。我看到了草图，链中的每个人都必须有证书或是验证签名。如果其中一个未部署，DNSSEC 就会失败。对吗？我理解的对吗？

韦斯 • 哈达克： 很接近。并不是说失败，而是你会知道你现在正前往一个未经 DNSSEC 签名的地方，所以你不得不提高警惕，不能完全信任。

DNS 树的某些部分也没有签名，但你的浏览器也能与它们协作无间，因为 DNSSEC 已经给了你答案。它说“好吧。你需要前往 bigbank.com。顺便说一下，它们没有部署 DNSSEC。你别无选择。你只能以常规 DNS 继续访问。”

所以有了这样的机制，当解析器沿着链下行并最终达到一个点：“我无法再保证超过这里的安全性，但你可能还是需要一个答案。”

那就是我们今天的情况，有很多东西已经被签署，也有很多没被签署。除了消息之外，我们并没有为大量用户提供这方面的信息。

艾哈迈德 • 阿尔萨德： 好的。谢谢。

韦斯 • 哈达克： 好的。我们可能只有一个问题的时间了，有没有人想要提最后一个问题。

这边这位。

男性发言人（姓名不详）： [听不清]。那种情况下会收到错误消息吗？

韦斯 • 哈达克： 问得好。在那种情况下会收到错误消息吗？是的，当你进入不安全的部分但却没有收到错误消息时，是因为你的解析器还在继续为你找答案。你的解析器将会告诉你的应用程序，它得到的答案是否安全。

目前，浏览器或其他应用程序并没有真正查看该信息，因为如何向用户呈现该信息以及向用户呈现是否明智，它对最终用户是否有帮助，仍然是个悬而未决问题。

你会看到的是，如果 DNSSEC 在某个环节失败，如果半路杀出个程咬金，那么不完整的网页消息就会显示：“未找到该域名。”因为解析器已经尽力了。它已经尝试查询域名，如果因为一直得到错误答案而没有找到合适的答案，没有收到已签名的答案，那么你将会看到跟你前往残缺域名一样的残缺网页。它会表示：“我找不到改域名。”

你不会知道，那是因为 DNSSEC 在保护你。你只是知道它在为你查询域名时失败了。

好的。关于那方面，我想我们会总结一下。关于周三的工作坊，你们有什么想要增加的内容吗？

拉斯 • 芒迪： 我们已经有了不少关于周三的广告了，虽然不是刻意的，但确实很好。我们将邀请很多嘉宾出席。其中有人对 DANE 非常熟悉。我们会在介绍部分谈谈目前的版图，并按照全球各地的地理位置展现 DNSSEC 部署的类型和数量情况。

我们诚挚邀请所有人周三前来参加。工作坊 9 点开始，下午 2 点半结束？凯西，对吗？

凯西 • 什尼特 (KATHY SCHNITT)： 3 点。

拉斯 • 芒迪： 3 点。好的。请考虑一下。感谢大家的到来。希望你们的疑问都得到了解答。如果你想跟我们中的任何人，或者今天出席的人员谈谈 DNSSEC 的问题，我们都很乐意在大厅跟大家一对一倾谈，给大家做更多解答。

谢谢各位。

韦斯 • 哈达克： 是的。谢谢。最后一点。在明天的技术日，通常也会有非常多跟 DNSSEC 相关的理念和讨论。几乎一直都是这样我不太记得具体的日程了。但通常会有很多关于 TLD 部署 DNSSEC 等类似事情的演示。

拉斯 • 芒迪： 对。开幕式结束后就会开始，10 点半。

韦斯 • 哈达克： 开幕式结束后。好的。感谢大家的到来。希望大家都有所收获。

[会议记录结束]