蒙特利尔 — 人人都学 DNSSEC：初学者指南
美国东部夏令时间 2019 年 11 月 3 日星期日 — 17:00 至 18:30
ICANN66 | 加拿大蒙特利尔

丹 • 约克 (DAN YORK)： 我要说的是，我们将要提出一些问题并进行回答，如果你想上来发言，请靠近一点，我们今天的会议室非常大，请随时上来发言。我们会提供一个麦克风，我们将四处走动，与你们交谈并请人上台发言。

我是丹 • 约克，来自国际互联网协会，参与一些技术支持工作，我们今天要讨论的是，什么是 DNSSEC，它的目的是什么？我们将通过多种方式来进行。我们将向大家讲述一个小故事，演出一些短剧，讨论一些与此相关的问题，试着在这个周日的夜晚带来一些乐趣。

首先，我有一个问题。在座的有多少人以某种方式部署过 DNSSEC？好的，有一些人。有多少对对 DNSSEC 一无所知？好的，有几个人。我发现这与部署了的人有所重叠，我们开始吧，我们做得很好。我们将带领大家回顾一下，讲述 DNSSEC 在公元前 5,000 年的起源。

在我们的故事中，这是乌格维娜 (Ugwina)。她住在大峡谷一侧的一个山洞中，这是奥格 (Og)，他住在另一侧的一个山洞中。往返他们的住地要走很远的路，所以他们之间不会有太多的交谈或拜访或任何其他类似的事情。在某次见面过程中，他们注意到奥格家的火堆产生了烟雾。因此，他们意识到，他们可以使用烟雾作为信号来聊天；他们可以通过发送烟雾信号相互讲述更多的故事，进行更多的对话。

但是某一天，另一个居住在附近山洞中的人 — 我们叫他卡明斯基 (Kaminski) — 搬到了奥格所在山洞的附近，并开始发送他自己的烟雾信号。突然，在山的另一边的乌格维娜不知道那个信号是正确的，她迷茫了。“我应该与谁…？我在这里看到的哪个才是正确信号？”她试图弄清楚，“我们能做些什么？我们应该怎么做我才知道是谁发送的信号？”

因此，他们请教了村里睿智的长者。穴居人迪菲 (Diffie) 认为他可能有办法。他站起来跑到奥格的山洞里，来到洞穴的最后面，在那里他看到了那堆蓝色的沙子，这种颜色奇怪的沙子只存在于奥格的山洞里。他取了一些沙子跑出来，把沙子扔进了火堆。火焰突然变成了华丽的蓝色，乌格维娜和奥格现在可以聊天了，因为她现在知道哪种火焰信号来自于奥格。其他任何人都无法干扰，因为他们知道蓝色烟雾来自于奥格，而不是来自于其他任何人。

以一种有趣的方式来解释，这就是 DNSSEC 的全部含义。它的目的是确保你获得来自发送人的正确信息。它对信息进行一些特殊的处理，使你能够明白什么是来自发送人的独特信息。我们接下来会进一步讨论，了解与此有关的更多技术信息。

在较高的层面上，这是通常描绘 DNS 的方式。我们最终会到达 DNS 的根区，我们拥有所有这些顶级域，这里的 TLD，所有不同格式类型的 TLD。然后，我们还拥有顶级域下方的二级域。我们实施了所有这些方面。解析器，DNS 解析器知道如何到达根区，知道如何通过各个层级，对其进行计算，在此过程中的各个层级都会告诉解析器，“继续与其他层级交谈。”

DNS 是一个分布式数据库。它指出了你应该如何从每个不同的解析器获取信息，并在此过程中一直进行缓存。但是协议中没有安全措施，就像在我们的小故事中一样，其他人可能出现并恶搞，可以用其他方式提供其他答案。你可以对这些解析器的缓存投毒，因为一旦它们存储了信息，信息就可以保留一段时间。

所以，我们马上就要采取行动了。我们的演出团队准备好了吗？请上台来。我们向大家展示这是如何操作的。你们看到的是，你们将在这里看到我们的演员扮演用户角色，他想搜索信息，想连接到 bigbank.com。我们的演出团队正在做准备。好了。等等。好的。我们开始吧。好的。韦斯 • 哈达克 (Wes Hardaker) 将扮演我们的用户，他将与我们的互联网服务提供商交谈，提供商是解析器，随后解析器将与我们重新排列的 DNS 层级交互。

韦斯 • 哈达克： 测试，测试，测试。

弗雷德 • 贝克 (FRED BAKER)： 第一个问题，我们需要电。

丹 • 约克： 音频师，你能把麦克风拿出来吗？

韦斯 • 哈达克： 开始了，好了。我想买一艘游艇。我一直都想买一艘游艇。它们是超大型的轮船，我喜欢这种大船。我要查看我的银行，登录 www.bigbank.com，我来看看我还有多少钱。你能为我提供 www.bigbank.com 地址吗？这样我就可以与它对话了。

沃伦 • 库马里 (WARREN KUMARI)： 当然，你就是我想保持良好关系的那类客户。我来帮你。你好，根区，我的一个用户想找 www.bigbank.com。你能告诉我它在哪里吗？

弗雷德 • 贝克： 我希望我能，但是我出现了问题。我不知道。我不知道在哪里可以找到 .com，你可以询问 .com。

沃伦 • 库马里： 好的，谢谢，我试试。你好，.com。我的一个用户想找 www.bigbank.com。你能告诉我它在哪里吗？

发言人（姓名不详）： 我不太确定 www.，但是我知道 bigbank.com 在那里。

沃伦 • 库马里： 很好，我来问问他。你好，bigbank。你知道 www.bigbank.com 在哪里吗？

拉斯 • 芒迪
(RUSS MUNDY)： 你好，ISP 先生。我可以告诉你 www.bigbank.com 在哪里，它在 2.2.2.3。

沃伦 • 库马里： 太好了！我终于找到答案了。你好，用户先生 www.bigbank.com 位于 2.2.2.3，改天我能到你的游艇上来吗？

韦斯 • 哈达克： 恐怕我的游艇不允许使用递归解析器，但是没关系。好的，我可以去查看了 — 太好了！我有一轮船的现金。

丹 • 约克： 让我们为他们的精彩表演送上热烈的掌声吧。这就是 DNS 的运作方式。对于所有正在进行的许许多多小型 DNS 查询，这就是一直在发生的情况。但是我们想更多地谈谈这是如何运作的。我们将进行另一场演出。我们会再演一遍，但是这次你们将看到当攻击者介入时会发生什么。

韦斯 • 哈达克： 好的，我们开始吧。今天我要去买轮船，我的超大型游艇。我需要再次前往 bigbank.com 进行转账，我忘记它在哪里了，你能告诉我吗？

沃伦 • 库马里： 很遗憾，我也忘记了。不过，我会为你找到。你好，根区。我的一个用户想找 www.bigbank.com。你能告诉我它在哪里吗？

弗雷德 • 贝克： 如果我知道答案，我就能告诉你。我知道 .com 在哪里。这会有帮助吗？

沃伦 • 库马里： 是的。根区没什么用，我来问问 .com。你好，.com。我的一个用户想找 www.bigbank.com。你能告诉我它在哪里吗？

发言人（姓名不详）： 我不知道 www.，但我知道 bigbank.com 位于 2.2.2.2。

沃伦 • 库马里： 我去那里问问。你好…

安德鲁 • 麦康纳基 (ANDREW MCCONACHIE)： 事实上不是，因为 bigbank.com 位于 6.6.6.6。

沃伦 • 库马里： 好的，的确。没关系。你好，用户先生。

韦斯 • 哈达克： 哦，6.6.6.6，我知道在哪里 — 我可以把我所有的钱都支付到 6.6.6.6，谢谢。我的轮船呢？

安德鲁 • 麦康纳基： 谢谢！哈哈哈！

韦斯 • 哈达克： 我的轮船？

丹 • 约克： 好了。让我们再次为他们送上热烈的掌声！这就是我们所讨论的 DNS 可以如何被投毒。攻击者可以对其投毒。基本上，谁先向解析器返回答案，谁就赢了。在这方面就是以速度定胜负。

在这种情况下，邪恶博士能赶在可怜的拉斯 (Russ) 之前返回答案。现在，部分危险是我们的 ISP 沃伦 (Warren) 要把答案保留一段时间。所以，无论其他任何人询问 www.bigbank.com 在哪里，他们都会得到错误的答案。

安德鲁 • 麦康纳基： 6.6.6.6。

丹 • 约克： 正是这样。他们都会得到错误的答案，直到超时。这就是 DNS 攻击。这就是缓存投毒。这就是与此有关的全部内容。我们现在知道的是，这是 DNS。通过 DNSSEC，我们加入了数字签名的概念，你们可以看到我们的演出团队仍然在这里，因为他们马上将要再次演出。

出现的情况是，你们将密钥和签名存储在 DNS 内，以便你能查看，信息是否真的来自于原始来源？那真的是应该提供 bigbank.com 信息的人吗？解析器让所有这一切运作，解析器知道根区密钥在哪里，或者知道如何获取根区密钥。有多少人听说过去年的根区密钥轮转？是的，好。大家看看那个。

这全是关于确保从 DNS 根区开始建立信任链，直到提供此信息的各个不同的人、各个不同的权威服务器。它们都是彼此衔接的，所以我们可以保护信息的完整性。我们希望使我们的 big bank 域名服务器成为向 ISP 提供信息的服务器，而不是由其他任何服务器提供。下面再次请出我们的演出团队，再演出一次，这次我们要用上 DNSSEC。

韦斯 • 哈达克： 你们将很高兴知道，这是最后一次。

发言人（姓名不详）： 首先我们需要信号。

丹 • 约克： 噢，噢，好的。我们首先必须经历这个过程。请继续。那么，我们在这里做什么？根区正在发出信号。如果事情有这么容易，IANA 就不会不喜欢它，对吗？所以，你们将发现，根区有签名，.com 有签名，big bank 有签名，每个人都有签名。我们很好。现在…

韦斯 • 哈达克： 好的，我们假装这没有发生。我有另一艘值得购买的游艇。这次我真的要买另一艘船。这次你能告诉我 bigbank.com 在哪里吗，你能告诉我正确的答案吗？

沃伦 • 库马里： 好的，我试试。我去问问根区。你好，根区，我的一位用户想找 www.bigbank.com，你能告诉我它在哪里吗？

弗雷德 • 贝克： 不，我不能。但我可以告诉你在哪里可以找到 .com，.com 也许可以告诉你答案。我有签名。

沃伦 • 库马里： 我来快速地检查一下签名。好的，就我看来，签名是有效的。我去问问 .com。你好，.com，我的一位用户还想购买一艘游艇。他想知道 www.bigbank.com 在哪里。你能告诉我吗？

发言人（姓名不详）： 我也不知道 www. 在哪里，但是我可以告诉你 bigbank.com 在 2.2.2.2，并且我可以对这个响应签名。

沃伦 • 库马里： 我来检查一下签名。看起来是没问题的，我继续去了解一下。你好，www.bigbank.com。

安德鲁 • 麦康纳基： 你好。

沃伦 • 库马里： 嘿，你好吗？

安德鲁 • 麦康纳基： 6.6.6.6。

沃伦 • 库马里： 你的签名在哪里？我没有看见[串音] Bigbank.com 的签名，你能告诉我 www.bigbank.com 在哪里吗？

拉斯 • 芒迪： 我当然能。www.bigbank.com 在 2.2.2.3，它有签名。

沃伦 • 库马里： 我来检查一下，我会仔细地检查。是的，看起来没问题。给你，用户，www.bigbank.com 2.2.2.3，我验证过了，你可以信任它。

韦斯 • 哈达克： 谢谢。银行先生，你能将我所有的钱汇给丹 • 约克吗？我要从他手里购买一艘二手轮船。

丹 • 约克： 为什么，谢谢你，韦斯 (Wes)。请大家为他们送上热烈的掌声。这就是我们的做法，这就是 DNSSEC 的运作方式，它们拥有的这些签名可以确保其他任何人都无法进入流程。

这就是它的作用。这就是它的全部，很重要的一个部分。它可以确保信息的完整性，输入 DNS 的信息就是用户获取的信息。它与保密性无关，它的作用不是保护信息的安全，只是验证信息就是用户输入的信息。现在，我们来进一步谈谈，举一个例子，我们将请出拉斯 • 芒迪，他将来到这里，我要把钱退还给韦斯。

拉斯 • 芒迪： 谢谢你，丹 (Dan)。感谢今天下午和我们一道参加会议的每一个人。这些灯光很明亮。因此，我想谈谈，一些… 哦，遥控器，很好。我要举例说明人们在部署 DNSSEC 的过程中需要考虑的事情。“为什么要这样做？”的一部分是“我们为什么担心开始实施 DNSSEC？”我们已经从 DNS 的角度来讨论了这个问题，还姚伦了如何获取 DNS 信息，特别是如果你没有使用 DNSSEC 你就可能受到干扰。

但是人们为什么要追逐 DNS 呢？DNS 本身并不是那么有趣。几乎在所有情况下，人们对 DNS 进行处理后，便可以对实际进行 DNS 查询的应用程序进行处理。如你们之前所见，在那种情况下，当韦斯想要转账时，实际是在偷钱。这对于使用 DNS 的应用程序执行其操作确实很重要。那么，如果它没有达到正确的地方，谁知道会发生什么。

在现实世界中我们有很多这样的例子，具有这样的性质，一些事情得到了确定，它是当今互联网上运行的任何应用程序。它极有可能使用其下方的 DNS，大多数时间应用程序的用户都不知道也不在意 DNS 的存在，但是 DNS 对于他们应用程序的适当运行非常关键。

几年前我发现了一件事，我返回并再次查看，遗憾的是，我没有保留所发现的具体细节。但是我发现在一堂程序课上，一名大学教授要求学生编写一个 DNS 劫持程序。

我查看了整个课程要求和布局，发现没有任何谈论道德或者为什么你不应该这么做的信息。只是说，“同学们，你们要编写一个 DNS 劫持程序。”这真的有点令人毛骨悚然，因为有人长期以来一直在努力防止劫持事件发生。

遗憾的是，在过去的五年中，我一直找不到它，所以也许它已经消失了。如丹所说，重要的是能够到达正确的地方，当你到达了正确的地方，你就能验证获得信息是否是正确的。

为使 DNSSEC 运作而嵌入的公共密钥加密是作为其基础的技术机制。现在，我们在进行先前的工作时，我们在 ICANN 会议上的确进行了真正的劫持。这里是一系列幻灯片，它们以图片的形式向你提供与你看到的舞台表演相同的信息。

我们真正停止进行此操作的原因之一是，在一次会议中，我们不采取只是劫持特定房间内的 DNS 的做法，网络的配置与预期不太相符，而是劫持整个 ICANN 会议的 DNS。当这结束时，它成为了一个笑话，但是在进行中的时候没人觉得这是笑话。所以现在，我们只是展示幻灯片，你们可以看到用户乔 (Joe) 位于左下角，他想前往位于上方的网络服务器。

从这张图片你们可以看到，他发出了一项查询。查询被发送到了他的递归服务器。递归服务器收到并保存了查询，然后将其发送到与网络相关的权威域名服务器。他想访问的网络服务器向递归服务器返回了答案。随后，递归服务器将答案返回至用户。这就是你们看到的，我们在舞台上来来回回跑来跑去所表演的内容。

之后，他就可以进行交易了。当我们放入实际的网站时，这是网站的特殊配置，以便网站上的可视图像显示出你是否在下面进行 DNSSEC。

没有显示存在 DNSSEC 的标准图像，但是将其设置在网站上以便你能看见，事情就会简单得多。当你访问同一个网站时，如果你没有使用 DNSSEC 验证机制，你就会得到另一个不同的符号。所以，你们可以看到上面的是勾号，下面的是三角形警示，这是在告诉你，“你的 DNSSEC 处于关闭状态。”

当我们在做同一类事情的时候，我们在舞台上表演了，用户乔发送了查询，但是这次邪恶博士出现在网络上。所以查询在不断徘徊，在现实世界中会发生的是，邪恶博士看到查询并提供回答，即使查询继续在网络中徘徊，但是用户乔会被引导至模仿网站。

你们可以看到其他查询通过网络后返回，提供一个回答，但是用户乔没有得到那个回答，因为他使用的解析器采用了第一个回答并前往错误的网站，所以除非他使用 DNSSEC，否则他无法到达正确的网站。当他使用 DNSSEC 时，DNSSEC 防止错误答案达到他的解析器，因此，在他得到正确答案之后，他返回到正确的网站并办理相应的业务。

我们采用网站来展示你们可以做什么，特别是，网站的构建使得我们在网站的一个版块中展示这就是可能发生劫持的地方。我们针对没有启用 DNSSEC 的网络浏览器进行的实际劫持，我们真的插入了信息，并且这个信息是一个虚假的故事，说的是，“史蒂夫 • 克罗克 (Steve Crocker) 承认 DNSSEC 无法解决全世界的饥饿问题。”

相当明显，这完全是幽默式的说明，但是你可以看到最前方的“DNSSEC 关闭”图像，在下方你可以看到 .org 向 ISP 分享了 Comcast DNSSEC 建议，以及页面上方的头条故事。从本质上讲，我们通过劫持在页面上插入了部分信息，所以即使它位于浏览器的相同页面上，它也是不同的信息，当然，我们插入的是虚假信息。

在单一的网站页面上，你们知道有多少信息是来自没有缓存信息的空域名服务器吗？这是大约六七年前的 CNN.com，这里一个页面上就有大约 75 至 100 条查询和回复。任何一条查询和回复或者他们中的大部分都有可能被劫持。

现在，情况有所好转吗？没有，在某些方面有，但在某些方面没有。与过去相比，一个商业网站页面上的查询比以前更多。但是这项特别的方式显示，现在，某些查询采用了 DNSSEC 签名，在未来四到五年内，网站的查询数量可能会翻倍。所以当你谈到 DNSSEC 时，人们通常担忧和思考的基本问题是，“哦，我的上帝，这些是加密密钥。我们该做什么？保管好加密密钥非常重要。”

这是真的，但是最重要的是你的 DNS 区数据。你对你的 DNS 区数据的准确性和正确性的关注至少应达到对任何加密密钥的关注，因为设置与任何区相关的 DNSSEC 的目的是让获得信息的用户知道 DNS 信息是正确的。如果你对加密密钥的关注超过区域数据，某人想攻击你的区域，他们将攻击系统中将信息输入系统的那个部分。

如果对此信息进行签名，接收人会说，“哦，那这一定没问题，这有签名。”但是如果某人成功攻击你的 DNS 部分（通常称为对你的信息投毒）并以某些方式在此处获取不正确的信息，那么与不使用 DNSSEC 时相比，你的情况会更糟，这是因为你作为操作者通过加密验证信息是正确的，如果信息不正确，则是你没有正确和适当地处理你的信息。

这里有一个不使用 DNSSEC 进行 DNS 操作的例子。区，对区数据而言，你在此将信息输入你的权威域名服务器。信息进入权威域名服务器，权威域名服务器在互联网上运行并包含该信息，它从递归域名服务器接收请求，递归域名服务器也从客户端接收了请求，并回答了该请求。

所以，如果你将 DNS 纳入你的系统操作，而不是将其外包或让注册管理机构为你提供，如果 DNS 对你的操作功能非常重要，且你在有机组织内部进行所有操作，你可能会拥有精通 DNS 的员工。你可能想进行 DNSSEC 活动，将其作为你正在进行的活动的扩展，以此来运行 DNS。

因此，在他们自己的 DNS 中运行的大型活动可能想进行自己的 DNSSEC 实施和操作，特别是在 DNS 非常关键的情况下。你在注册大型 TLD 运营或者你是大型企业，在此方面 hp.com 始终是一个很好的例子；verisign.com 的业务与 DNS 有关，从 DNS 角度来看他们都是重要组织，因此，他们可能会自行实施。

如果你的 DNS 区对于互联网或组织的经济可行性可能并不那么重要。如果你是这种情况，net-snmp.org 就是一个例子，这是我认为我负责的域名。这个域名不会产生任何作用。哦，现在是你在负责？哦，好的。我把它移交给韦斯。好的。

但是事实是，这实际上不是关键的 DNS 操作 — 正确是一件好事，但对于互联网和你的业务功能而言并不重要。我们在座的所有人都使用 DNS，我们需要在可能的情况下使用 DNSSEC。再次说明，重要的事情是保护 DNS 区数据。现在，我们看到了先前的例子，即加载权威区域并请求信息和答案。

这是需要再执行一些步骤的地方的简单示例。在真正加载进区域的权威服务器之前，你就要先为区域的数据进行签名。我们希望在某个时刻使用递归服务器或者最终应用程序，但是递归服务器本身需要具有根密钥并进行验证，以便在发出请求和返回答案时，你可以进行验证。对于大多数验证域名服务器（当然是开源产品），只需

简单地以适当的方式设置一个配置开关即可打开它，只需这样做就可以。

现在，总而言之，对于运行自己的 DNS 的活动的一般概念，DNS 对他们来说非常重要。他们想要采用自己的 DNSSEC 方式，进行自己的 DNSSEC 活动，以确保其运行与 DNS 一样准确。如果活动外包了他们的 DNS 运营，他们可能还想外包 DNSSEC 活动。在某些情况下，这会变得更加容易。

过去，许多 DNS 外部服务提供商都会提供 DNSSEC。所以，我敦促活动，如果他们找到了自己的服务提供商，如果你进行外包，则不要实施 DNSSEC，让他们来实施。如果他们不，我 — 没有多少人会这样做，但是我们中的一些人会，包括我自己，如果他们没有找到服务器来提供 DNS 服务并更改你要向其提供资金的人，那么他们将会实施 DNSSEC。

这里是我们的总结幻灯片。这些是本次活动、今天下午的聚会的主办组织，上来吧，丹。剩余的时间我们进行讨论和问答。各位，上来吧，我希望我们将会收到一些问题。

丹 • 约克： 是的。如果大家想上来对着麦克风发言，我们应该准备好这些 — 好的，这些应该 — 上来吧。谁要提问？你们已经看完了全部的内容。有人吗？来吧，肯定有人要上来。

凯茜 (Kathy) 在这里了，哦，安德鲁要四处走动一下，邪恶博士。某人肯定有问题要问邪恶博士。好的，在那边，很好，有人要发言了。我担心我不得不开始讲笑话了，这会很痛苦。看看那边的沃伦。好的，请讲。

罗西奥 • 德拉弗恩特 (ROCIO DE LA FUENTE)：好的，非常感谢你的陈述和介绍。我是罗西奥 • 德拉弗恩特，是 ICANN66 英才计划的学员，我想阐明一点，如果我没理解错的话，签名遵循 DNS 的密钥，如果 TLD 没有签名，我注册的域名没有签名，那么是否有任何方式让 DNSSEC 正确运行？

丹 • 约克：好的。你们中是否有人…？好的，答案是，我的意思是，你可以对你的域名签名，你可以做这些事情，但是它不会出现在信任链中，不会出现在 TLD 中，所以要验证它的人可能无法一路确认到根区。所以是的，一般而言，要让 DNSSEC 运作，你需要让你的 TLD 获得签名。

韦斯 • 哈达克：你是否真的需要让所有一切都有签名？只要有签名，DNSSEC 就会为你提供直至根区的保护。如今大多数 TLD 都有签名，我认为 DNSSEC 工作坊中会有图片展示这个方面。

这里有超过 1000 万签名域名，诸如 bigbank.com 等最终域名可能真实存在且没有签名。但是你必须能够验证整个树形结构。话虽如此，对于 big bank 来说，如果下方没有链接，即使你无法验证，即使验证到 .com，也比什么都不做的好。

丹 • 约克： 但就韦斯在周三提出的观点而言，如果你参加 DNSSEC 工作坊，你就会看到，我们有几张图表展示一些不同的区域，并且我们会绘制一些地图，包括许多部分，但是我不知道究竟是哪些部分。你来自哪个国家/地区？阿根廷？好的。不是 .ar 吗？好的，他在检查。继续，回到那里。

亚兹德 • 阿卡胡 (YAZID AKANHO)： 你好，我是亚兹德 • 阿卡胡，来自贝宁，是 ICANN66 英才计划的学员。感谢你的介绍，我要说的是舞台剧帮助我们真正地理解了内容。事实上，我有两个问题。第一个是，为什么部署 DNSSEC 是 — 我不知道用哪个词适当，但是部署非常慢。为什么呢？是因为技术原因吗？政治原因？我只想知道，为什么？

第二个问题，我被告知了 DNSSEC 路演计划，这项计划是取消了还是…？DNSSEC 路演计划的下一步是什么？

我的最后一个问题是，希望进一步解释生成 DNSSEC 密钥的基础设施。我还被告知，有一个单独的基础设施，这个基础设施需要保密。你能进行一些解释吗？谢谢！

丹 • 约克： 明白。部署挑战，DNSSEC 路演，有关如何签名的信息，等等，我理解正确了吗？好的。有人想要回答吗？回答其中一个？

沃伦 • 库马里： 我来回答其中的一些。我快速地检查一下，.ar 有签名，所以阿根廷… 好的，不错。对于部署问题，是的，DNSSEC 的部署速度没有达到预期的速度。这里有一些有趣的统计数据，我们目前在加拿大，13.3% 的请求在加拿大验证，25% 的请求在美国验证，19% 的请求在格陵兰验证，14% 的请求在俄罗斯验证。

所以，部署范围并不广泛，并不是普遍部署，但是部署实际上正在加快，并且大多数（不是绝大多数），但是目前大量请求正在验证，并且绝大多数 TLD 都有签名。在这一点上，部分新 gTLD 合同要求新 gTLD 全部要有签名，并且绝大多数 ccTLD 也要有签名。

丹 • 约克： 拉斯，请讲。

韦斯 • 哈达克： 如果你想要每天跟踪，我的同事 — 维克多 (Victor)，谢谢，我一下记不起他的名字了，他和我拥有一个网站，我们每天都会更新，这个网站名为 stats.dnssec-tools.org。如果你看看图片，你就会发现这个网站自 2011 年以来就一直在上升。有时候出现了大幅度的增长。

这里有一个，就在前几天有一个，因为作为提供商的 one.com 突然对 .dk 域名下的很多东西进行了签名。这里就是这些大幅度的增长，为了进行部署，我们需要更多这些东西，在默认情况下我们需要巨头公司进行部署，因为世界上使用的大多数域名都不是由各位个人运营的，而是由从事 DNS 托管的这些公司运营。

历来都有大幅增长，瑞典是最明显的国家之一，捷克共和国也是，这里有巨大的激励因素推动人们签名。事实上，经济激励让注册更便宜，这大大推动了特定国家/地区代码内的签名。例如，上升。

丹 • 约克： 拉斯，你要不要发表一下看法？

拉斯 • 芒迪： 是的，我想对韦斯刚刚说的进行一点补充。各个组织使用许多不同的激励措施来鼓励人们实施 DNSSEC。带来大量帮助的其中一个方面是，你们看到的大多数大型公共 DNS 解析器（带有四个相同的数字），都是非常常见的事物。这些解析器中的大多数现在都在实施 DNSSEC 验证。

我们中的一些人已经在这一领域做了很长一段时间的一件事是，我们希望看到验证最终被推行到最终应用程序中。这份简报中提供的一个例子是，在我们实施劫持的地方，当史蒂夫 • 克罗克说“DNSSEC 无法解决全世界的饥饿问题”的时候，浏览器中已经进行了验证。

在你与人们进行互动和讨论的时候，应记住，对最终用户的 DNS 信息验证越完善，你就越能确保系统的安全性。所以，应该鼓励人们思考得更远，即使是大型缓存公共解析器，并考虑在应用程序中实施。现在，还有一个问题。是的。

丹 • 约克：

我要对一个特定的问题说几句，部署挑战的一部分是，如图片所显示，这里事实上有两个部分，对吗？每个签名的人以及拥有域名的人都需要对其进行签名。这是一个部分。这是签名方面。现在，如拉斯刚刚提到的，某些可以自动进行，我们有许多可用的工具。如果你与任何 DNS 托管提供商交谈，某些提供商可以使它变得超级简单。

有些人拥有复选框，你们知道，现在你的域名已经签名了。某些很简单，但是另一部分，你必须进行检查，必须进行验证。如拉斯提到的，有时候只是取消选中或删除配置文件中的注释行，现在，突然间，你可以开始验证。

但是，很长一段时间以来发生的部分事情是，我们遇到了这种先有鸡还是先有蛋的问题，在美国，某些网络运营商，ISP，就像沃伦扮演的那样，他们运行 DNSSEC 验证，并说，“我们不会开启验证，因为没有足够的已签名域名。”

运营商说的是，“我们不会这样做，因为没有足够的已签名域名。”一些大型托管提供商说，“我们不会签名我们的域名，因为进行验证的人不够多。”有少数人暂停并且这样说。

现在，许多这种问题都得到了克服，因为如韦斯所说，这里有真正的部署，有大量的人在实施递归解析。如果你们看看某些大型公共 DNS 服务器，例如 Google Public DNS、Cloudflare、Quad Nine，它们都在实施 DNSSEC 验证。

所以，大型解析器在实施，大型 ISP 在实施，位于北美的 Comcast 拥有 2000 万客户，它通过 DNSSEC 验证完成所有操作。所以，那种言论在一段时间内减缓了部署，不过现在已被克服，但是仍然继续存在。我知道你还有另外两个部分，弗雷德 (Fred)，你想要…？是的，开始了。

弗雷德 • 贝克： 我要问拉斯一个问题。你是否知道支持 DNSSEC 验证的具体浏览器？哪些浏览器 — 我的电脑上只有四种浏览器。我应该如何使用？

拉斯 • 芒迪： 很遗憾，没有哪种浏览器置入了 DNSSEC 验证。沃伦，你知道吗？我们过去曾经有一种浏览器支持验证，但是现在已经不再支持了。

沃伦 • 库马里： 稍等一下。我认为你们谈论的是进行 DANE 验证。

丹 • 约克： 不。

沃伦 • 库马里： 我的意思是，所有浏览器都依赖于系统解析器。如果你的电脑在进行 DNSSEC 验证。浏览器中的解析器在很大程度上仅依赖于系统解析器的功能。所以，如果你在计算机指向的任何解析器上启用了 DNSSEC 验证，则可以部分免费地进行 DNSSEC 验证。我认为韦斯现在正在尝试并向我喊叫。

韦斯 • 哈达克： 完全不是。我绝不会对你喊叫。

弗雷德 • 贝克： 好的。你刚刚告诉我，作为用户，我需要在我的 Mac 上，在你的 Windows 设备上，在你的 Linux 设备上，我需要进行一些操作。

韦斯 • 哈达克： 我们将会陷入困境，因为它是技术性很强或更难以描述的问题，但是有一些可以实施验证的要素。如今，包含网络浏览器和电子邮件阅读器以及访问网络的任何其他工具的应用程序通常不会自行进行验证。就像之前演出的短剧一样，我，用户乔，没有自行检查这些证书，我相信我的 ISP 为我进行了这些检查。事实上…

弗雷德 • 贝克： 用户乔，你是一个可怕的人。

韦斯 • 哈达克： 我是一个可怕的人。所以，我会把我的验证代码放进… 实际上，拉斯之前讨论过的 net-snmp 软件包，我们实际上在该开源软件包中设置了验证代码，可以在应用程序中进行检查。实际上很少有应用程序这样做。如果你们前往我之前提到的统计页面，就会发现有一个，最大的之一。

目前人们进行签名和部署的最大动机之一是，这是唯一的方法之一 — 实际上，这是在服务器之间确保电子邮件安全的最佳方法。因此，实际上，它正在非常迅速地增加。不是所有的 DNSSEC，但是如果你看看 DANE 的增加情况，DANE 是对服务器之间的电子邮件对话进行签名的技术，它实际上也增长地很快，并且即使没有在应用程序中完成，至少也在应用程序附近完成了。

丹 • 约克： 好的，沃伦。你有一个…

沃伦 • 库马里： 弗雷德，你说的是，作为用户，你听到自己必须要做一些事情。作为用户，你应该确保你的 ISP 的解析器进行验证，你可以要求他们进行验证。或者，如果他们不进行验证，你可以选择一个大型公共解析器，111199998888，其中之一，因为所有这些解析器都会进行验证。

所以，如果你想获取 DNSSEC 保护，如果你的 ISP 要进行验证，则使用 ISP，如果他们不进行验证，则使用其他方式。这里有一个网站 internet.nl，如果你们浏览到该网站，它就会检查你正在使用的循环解析器是否进行验证。这样，你就可以知道你的 ISP 是否会进行验证。

丹 • 约克： 我想回到亚兹德 (Yazid) 的问题上来，但是我也要说，弗雷德，在网络浏览器方面，另一件事是，我们是否会面临进一步陷入困境的风险，我先把这个问题留到周三讨论。但是正如浏览器所着眼和进行的那些事一样，许多端点都开始实施基于 HTTPS 的 DNS，DOH 服务器也在进行 DNSSEC 验证。如果你的浏览器开始沿该路径运行，你的浏览器实际上可能正在执行此操作，但是我们现在先不要讨论 DOH。

让我们回到亚兹德的问题上来，因为他一致非常耐心地站在那里，如果我把你的名字读错了，我对你表示抱歉。

亚兹德 • 阿卡胡： 我的名字是叫亚兹德。好的，谢谢。感谢你阐明了解析器的验证和区签名，据我所知，这是两个独立的问题。两年前，在我的国家贝宁，当我们发现解析器验证了 80% 的 DNSSEC 请求时，我们感到很惊讶。为什么呢？因为一些 ISP 使用的是公共解析器。

丹 • 约克： 是的。

亚兹德 • 阿卡胡： 这与域签名完全不同，这就是我提问的原因。DNSSEC 路演计划在哪里？

丹 • 约克： 是的。你显然是对的，就某些统计数据而言，韦斯，我不知道你的统计数据，但是我知道杰夫 • 休斯顿 (Jeff Houston) 的 APNIC 统计数据将显示，某些国家/地区的 DNSSEC 验证水平非常高。在探索这个问题的时候，因为他们国家的一些 ISP 已经离开，并且他们只使用公共 DNS 服务器。他们并不运行自己的解析器，他们使用 8.8.8、1.1、9.9，其中一个不同的公共解析器。

对于 ICANN 路演的情况，我不太清楚。我们回头再告诉你相关情况吧，因为我们没有参与那个直接计划。所以，我们需要回头再告诉你相关情况。亚兹德，请向我们中的任何一个人提供你的名字，我们就可以回头再告诉你有关路演计划的信息。

对于与那个问题有关的文件记录问题，你能告诉我你的编号吗？国际互联网协会在我们网站的 Deploy 360 部分发布了一些信息，ICANN 发布了一些信息，其中有一些不同的资源在讨论细节。许多权威服务器公司，例如 ISC、nlnet labs，还有一些其他公司，他们已经获得通过并创建了有关如何开展这项工作的文档。这里有一些很好的链接。还有其他问题吗？好的，那边那位男士。

发言人（姓名不详）： 谢谢！我可能会有点偏离主题，我想知道在响应中 DNSSEC 与 sig 零伪部分之间的关系。

韦斯 • 哈达克： 事实上，一点关系也没有。它们并不相同。DNSSEC 旨在保护一组数据并使其可验证，以便无论数据以何种方式传输至你，你都能理解它。Sig 零和 TSIG 是 DNS 中用于保护事物的另一种技术，但无论采用什么路径，它们都只能保护连接而不是数据本身。它们是不同的技术。

丹 • 约克： 是的，请讲。

沃伦 • 库马里： 我接着这个话题说几句，韦斯说，DNSSEC 允许你验证信息，无论数据以何种方式传输至你。由此带来的好处之一是，实际上很多人现在只是将整个根区下载到其解析器中，因为它们都已签名。

因此，你只需在解析器中对其进行验证，而无需将查询发送到根区。具有签名区的好处之一是，在某些情况下，你可以不处理查询回复，你可以获取整个根区文件或让其他人来做。

发言人（姓名不详）： 这是通过传输请求来进行，还是你会获取整个根区文件？

沃伦 • 库马里： 许多根服务器字母，包括 B 和 F，其他我不记得了，只让你进行传输查询，AXFR。如果你对此感兴趣，可以称之为本地根，它是 RFC 7706，上面有信息，很快就会有新版本。但是，本地根，或者超本地根 —

丹 • 约克： 是的，超本地根。

沃伦 • 库马里： 有一个项目允许你通过网页来进行。

韦斯 • 哈达克： 没错。我的是本地根，localroot.isi.edu，它为你提供了将解析器实际转换为根缓存解析器所需的配置，因此所有内容均已预先缓存。如果你是一位知识渊博的管理员，则上面有很多信息，可以使你轻松进行操作；但可能不适合最终用户。

发言人（姓名不详）： 我能再问一个问题吗，关于 DNSSEC 的问题？如果你看看 .com 之类的域，你就会发现它们可能有十几个域名服务器。每个单独的实例都有一个唯一的 DNSSEC 密钥，还是一个密钥用于整个 TLD？

沃伦 • 库马里： 你签名了一个区，一旦这个区有了签名，它就可以放在任何域名服务器上。如果你运营自己的域名服务器，然后又有其他组织运营从属服务器或辅助服务器，那么这就特别好。你签名你的区，你为他们提供区，不需要其他密钥。显然，你不需要担心他们变得有恶意或者其他任何东西。

丹 • 约克： 是的，这是其工作方式的好的一面，在这个方面，如沃伦所说，一旦你像那样全部签名，你可以在任何地方停止它们。它是公钥，私钥，密码。还有其他问题吗？它们可以是通用的，也可以是愚蠢的，也可以是 — DNSSEC 为什么只包含 SEC 之类的东西？我不知道。是的，回到那里来，亚兹德。

亚兹德 • 阿卡胡： 另一个问题。我听说在进行一些调查或者一些分析，以变更协议，生成根区的公钥和私钥。这些讨论在哪里进行的，后续步骤是什么？

丹 • 约克： 我认为我的一些在座的同事可以简单地谈谈这个问题。你说得非常对。在这个签名方面，当你签名之后，在签名服务器上，你使用特定的加密算法对其进行签名。无论是 RSA 还是椭圆曲线密码学，许多不同的事物，这些密码算法中的每一个都具有不同的属性，在更安全、或多或少的破解方面 — 有些原始协议自从以不同的方式被破解后人们可以采用这些算法设置密码。

所以，人们升级了密码，变得更加安全。现在，我们以不同的方式考虑 2,048 位 RSA 密钥。我们也在考虑比较小的椭圆曲线。所以，是的，存在不同的算法。就根区的状态而言，沃伦，你是不是想按下你的按钮？不是？好的。

沃伦 • 库马里： 我只发表一点一般性的意见。

丹 • 约克： 你刚才正在按按钮，你的手放在上面的。所以，我想…

沃伦 • 库马里： 我在摆弄按钮。好了。在有关什么是最好的加密协议方面，存在许多信仰，如果你让三位密码学家待在一个房间里，那么只有一位密码学家能够活着走出去，因为对于是 RSA 更好，还是椭圆曲线更好，或者 ED 25519 或各种其他事物更好，他们会展开激烈的争论，会有人刺伤其他人。目前，已经有一些从 RSA 迁移到一些较新的协议，但是有一些人在开始谈论量子安全协议。

一些密码学家担心量子计算机将使现有的密码技术无法使用。还有很多人认为这种担忧被过分夸大了。但是这是人们开始考虑的一些事，是人们可能开始部署量子安全协议的时刻。

丹 • 约克： 我认为答案，在根区方面还没有制定进行协议变更的直接计划。哦，拉斯，你想要变更？

拉斯 • 芒迪： 我们没有打算变更，但我想再次宣传一下我们将在星期三举行的工作坊。议程中的一个事项是由金 • 戴维斯 (Kim Davies) 介绍关于下次根区 KSK 轮转的计划。如果你们有兴趣了解更多详细信息，了解他们是如何采纳各种不同意见的，他们如何从社群获取意见，星期三下午举行的 DNSSEC 工作坊期间将召开一场 20 或 25 分钟的会议，由管理 IANA 的 PTI 总裁金 • 戴维斯为大家介绍他们最近发布的计划草案，我认为该草案是在星期五或星期六发布的。

丹 • 约克： 刚刚发布的。顺便说下，该工作坊的召开时间是下午 1:30，地点就在旁边 517C 会议室，人们会围绕有关 DNSSEC 的各种类型的问题进行几小时的讨论。某些问题是高层级问题，某些问题是细节性问题，某些介于这两者之间，以及所有这些问题。你会看到我们中的许多人会参加那场工作坊。还有其他问题吗？

安德鲁站在那里，将他的手高高举起。有人过去帮助他了。有人吗？有吗？你们可以自由地发表意见或者其他什么，否则我们将再次请沃伦来讲笑话。喔，好。看看那个。好极了。只是一种威胁。

发言人（姓名不详）： 好了，这可能是一个愚蠢的问题，我只是想理清我脑海中的一些事情 — 这实际上是对弗雷德先前提出的问题的跟进。基本而言，如果我没有支持 DNSSEC 的浏览器，比如 Outlook，这是否意味着我的 DNS 解析器和客户端之间的部分在技术上不受保护？

丹 • 约克： 好的。清楚地说，沃伦也说过，你设备上的所有应用程序历来始终将 DNS 解析交托给一小段代码，然后操作系统中的存根解析器就会向 ISP 解析器发起查询，并在执行所有类型的操作。

因此，如果你的操作系统不支持 DNSSEC 验证，检查签名，那么是的，你可能面临一定的风险，邪恶博士可能会乘虚而入，向你提供可能将你重定向至其他网站的虚假信息。历来，它一直以这种方式做一些事情，例如人们将 DNSSEC 验证内置到特定浏览器中，更多的就是出于测试目的。

这正在发生一点改变。互联网工程任务组 (ITF) 内有一个小组正在调查越来越多的应用程序执行 DNSSEC 这一事实。我们听到的关于 DOH 和网络浏览器的一些受到更高关注的问题是其中的一部分，但是其他应用程序也在 DNS 验证和其他方面做得更多，这将以某种方式改变 DNS 运作和互联网运作的基础设施。沃伦正看着我，似乎有话要说。

沃伦 • 库马里： 是的。我认为你或者我们在座的所有人可能有点过分夸大了保护。实际情况是，如果你观看了短剧，就是 ISP 离开并进行所有验证，并且 ISP 最终返回到用户跟前并说，“我验证过这个了。不要担心，这很好。”

DNSSEC 实际的运作方式是，验证解析器、ISP 或公共 DNS 进行验证，然后告知客户端其进行了验证，应该信任它。基本而言，它发送一些信息，指出，“是的，这很好。”大家都很高兴。这就表示，如果数据包在从解析器返回到客户端的途中被破坏了，那么就可能有人在做坏事。

最终，如果你的计算机自行进行了验证，如果它不信任 ISP，如果它仔细检查并执行所有加密工作，那么就很好。你可以让某些操作系统强制执行这种操作。例如 Linux，现在许多 Debian 系统都带有一个东西，你可以旋转旋钮，它会自己进行验证。

某些人提供了软件，你可以将其粘贴在计算机上。有一款名叫 Stubby 的软件，它将在计算机上进行验证。但是一般而言，你会在很大程度上信任你的 ISP 或解析器为你做了正确的事情且不会说谎，并且你的 ISP 不会在返回途中篡改数据。

发言人（姓名不详）： 是的，我想对我的问题进行一点补充。我想的是，你在本地网络上找到了一个人，也许他对整个系统投毒，并且他进行了过滤，他更快速地回答了 DNS 查询。

丹 • 约克： 好的，这正是可能发生的攻击媒介，这也是为什么你看到很多围绕 DNS 隐私、围绕基于 TLS 的 DNS、基于 https 的 DNS (DOH) 等等开展工作的原因，就是要考虑你应该如何加密从你的本地设备到递归解析器的连接，以便建立安全的连接，这样就可以避免有人在你的本地网络中发送数据包。这是这个层级的另一个要素，即深度防御和 DNS 保护层。

沃伦 • 库马里： 是的，我对此进行一点跟进，有两种不同的攻击。有人在你的网络中投毒，为你提供错误的答案，这样他就可以迫使你前往错误的位置。但是同样令人恐惧的是，网络中的某个人正在注视着你的数据包，并且如果你前往 https://alcoholicsanonymous.org 并不会真的带来帮助，虽然这个网站的所有内容都是加密了的。

如果人们可以看到你在 alcoholicsanonymous.org、gayrights.org 或者 Human Rights Watch 查询了产品名称，但是事实是你正在解析某些名称，而其未加密的事实可能造成损害，因为人们能够看到你在查询的内容。

丹 • 约克： 拉斯。

拉斯 • 芒迪： 沃伦刚刚描述的这类事情有时被叫做“咖啡店攻击”，你走进你最喜爱的本地咖啡店，他们的 WiFi 可能加密了，但是 — 它是可以自由访问的，咖啡店中的任何人都可以加入该 WiFi，并且他们可以复制你的 DNS 查询或者为你的查询提供欺骗性答案。

如果你有某种方式可以保护计算机连接到你信任其信息准确性的位置，那么你将不那么容易受到攻击。我知道这是可行的，互联网上可以下载软件来帮助你做到这点。

丹 • 约克： 再次澄清一点，DNSSEC 完全是为了确保你获得正确的答案。这纯粹是与完整性有关。我们在此讨论的是隐私增强的额外层级，我们还将在星期三 1:30 的会议上讨论其中的一些问题。这里有关于其组成部分的一些元素的内容。你们都好吗？还有其他问题吗？

发言人（姓名不详）： 是的，是的，我很好。非常感谢。

丹 • 约克： 好的，谢谢。凯西 (Kathy) 告诉我，远程参与者提出了问题。

凯西 • 什尼特 (KATHY SCHNITT)： 这个问题来自科西 (Cosi)。你能解释一下 Firefox 和 Cloudflare 之间关于 DNSSEC 解析器的交易吗，我在先前的演讲中听说过。

丹 • 约克： 哦，DOH。我不确定 — 我们会在这个问题上讨论到什么程度？

韦斯 • 哈达克： 我可以从中立的角度总结一下。

丹 • 约克： 请继续吧，从中立的角度总结一下。

沃伦 • 库马里： 哦，这就暗示不是我来回答。

韦斯 • 哈达克： 问题是，我在先前的对话中提供了答案，沃伦，如果我说错了，你来纠正我。怎么样？让我回过头来先迅速地回答先前的问题。

有多种方式可以保护你与解析器之间的对话。好的，邪恶博士。有多种方式保护你将信息传达到解析器，全世界仍在努力解决这一问题。然后，互联网工程任务组将在两周之内对此展开更多讨论。你可以在你的客户端实施 DNSSEC，你可以使用诸如 DOH、DOT 之类的措施，我们在尝试通过多种方式弄清如何保护它，它们都在通过不同的方式发挥作用。

对于网络浏览器，网络浏览器之所以做出决定，是因为他们已经非常熟悉 HTTPS，他们了解该协议，他们了解如何使用它，他们拥有知道如何使用它的快速数据库。他们已经决定，想采用基于 HTTPS 的 DNS，他们有这样做的动力。他们以不同的方式进行部署。

我知道的两种情况是 Chrome 和 Firefox，我不知道其他浏览器的计划。我首先来谈谈 Firefox，因为他们首先宣布了计划。Firefox 决定与 Cloudflare 合作，Cloudflare 是一家提供网络代理服务的公司 — 它们具有各种功能，并且也是支持 DNSSEC 全球验证解析器的公司之一。

他们与 Cloudflare 合作，如果你使用 Firefox 并且如果你在美国，他们会将你的所有网络 DNS 请求发送到 Cloudflare。他们未来的部署计划目前尚不确定，但是他们已经让步，本月仅在美国进行测试，目前仅在 Cloudflare 上进行测试，但是他们将设置一个下拉框，你可以从中选择其他提供商。

Google 是我要说的另一个方面，如果我说错了，沃伦将为我纠正。另一方面，Google 将测试你的 ISP，看看你的 ISP 是否为 DNS 提供 HTTP 或 HTTPS 服务。如果他们要提供，并且他们是受信任的提供商，他们将使用 DOH 与你的 ISP 对话。如果这两件事都不成立，它们将退回到常规 DNS。但是，除非最近有所变更，否则他们不会将你的流量发送给其他第三方。

沃伦 • 库马里： 虽然这样说让我很痛苦，但这基本是正确的。我的意思是，我要补充的一点是 Chrome 采用的方法。Google 相信你应该继续，目前你应该继续与你当前的解析器对话，因为它可能为你进行诸如恶意软件保护之类的事情。通过与你当前的解析器对话，他们不会变更你的解析器，这便于你获得所有当前的保护，它允许你潜在地查询内部域名等等。那就是 Google 采用的方法。

丹 • 约克： 我要对提问的那位远程参与者说的是，我认为重要的还有了解有协议，DOH，基于 HTTPS 的 DNS，这是由 ITF 定义的，RFC 8484。这份协议基本是关于如何进行基于 HTTPS 的 DNS 连接。这里有一份名为 DOH 的协议，DOH 客户端，它可能是网络浏览器，这是目前的主要观众，可以与任何 DOH 服务器对话。这是在应用程序和 DNS 解析器之间建立加密、安全、私有连接的一种方式。所以，它会对连接进行加密。DOH 作为协议就是这样。

现在，由于 DOH 最初在这些早期阶段进行部署，因此由于这些不同的机制和人们要求的不同方式，出现了一些争论。我认为，重要的是了解存在一种在隐私层面发挥作用的协议，以确保无关紧要的人无法获取有关你的私密信息的元数据。

这就是 DOH，另一种协议是基于 TLS 的 DNS，也就是 DOT，这两种协议都旨在帮助保护隐私。他们提高了我们的隐私级别。争论的焦点在于，在早期阶段如何以不同的方式实际部署它们。拉斯，你想说什么吗，还是 — 稍等。沃伦？

沃伦 • 库马里： 韦斯指出了一点我刚才忘记说的。全面披露，我在 Google 工作，Chrome 就是由 Google 开发的。我刚才想着要披露这点，但是忘记了。

拉斯 • 芒迪： 对于想要了解更多、听取更多与此主题有关信息的参会者，在 ICANN64 期间曾经召开过一场关于 DOH 的持续一个半或者两小时的高关注度主题会议，会上也提到了一些 DOT，但是这是一场比较长的会议，会议有记录，我很肯定能在 ICANN64 存档文件网站上找到，你们可以查看那些文件，了解 ICANN 进行的相关讨论。

丹 • 约克： 还有其他问题吗？安德鲁。

安德鲁 • 麦康纳基： 我认为应该是 ICANN65。不是上一届吗，召开 DOH 会议的那届？

韦斯 • 哈达克： 是的，在马拉喀什召开的。

安德鲁 • 麦康纳基： 是的。是的。没错。

丹 • 约克： 好的，还有其他问题吗？

韦斯 • 哈达克： 我应该披露一下我的工作单位，我在南加州大学工作。

沃伦 • 库马里： 我认为还可以找到更多的内容，尽管我还没有查看 DNSSEC 工作坊中关于 DOH 和 DOT 以及类似方面的内容。

韦斯 • 哈达克： 是的，我们会在星期三召开一场关于 DOH 的会议。

丹 • 约克： 还有其他问题吗？是的，这里的前面，那位男士，就是那里那位。我看到你了，接下来轮到你。

发言人（姓名不详）： 我叫盖伊 (Guy)，来自美国。是否有某种方式可以进行私密 DNS 查询而不会被无关紧要的人破坏，这种方式不允许窥探，因为 DNS 查询本身就以某种方式进行了加密？

丹 • 约克： 是的。DOH 或 DOT 都有这种作用，这些技术可以实现这种目的，如果你想直接使用这些技术，可以在你的网络浏览器上进行设置和连接。如果你将 Chrome 或 Firefox 设置为使用这些技术，你现在可以将其设置为使用 DOH 并告诉它们要连接到哪个服务器。所以，你现在就可以进行这些操作。

你还可以访问 DNSprivacy.org，对吗？在 DNS-privacy.org 上，你可以找到能安装的一系列其他软件。你可以在本地系统中安装一款名为 Stubby 的软件，它将对你发送至某些 DOT 服务器的所有查询进行加密。所以，你可以进行这些操作。如果你愿意，你还可以运行你自己的 DOH 或 DOT 服务器。你可以自行在自己所在的位置运行，并进行上述设置。可以做到这样。

沃伦 • 库马里： 如果想要立即为所有问题提供快速简便的解决方案，你还可以启用 VPN。

丹 • 约克： 好的。是的，你。还有其他问题吗？是的，回到那里。

罗西奥 • 德拉弗恩特： 我的问题与数字素养有关。我们在谈论教育用户或注册人时，我们是否应该向他们解释在他们注册时 DNSSEC 对于其域名的重要性？因为当我们谈论 ISP 时，注册管理机构，注册服务机构 — 不是注册服务机构，注册，对吗？当我们在谈论这个问题的时候，那对于 DNSSEC 的部署有帮助吗？你们对此有什么看法？

丹 • 约克： 我认为我们四个人以及在座的其他人都会说，“绝对应该。”我们鼓励人们强调这种重要性，只需要说，在你获得域名的时候，以及在你进行部署的时候，应该进行签名。

某些注册服务机构，我不知道阿根廷的情况，但是某些注册服务机构直接说到了点子上，注册服务机构和 DNS 托管提供商直接说到了点子上，他们实施 DNSSEC 就像你们所知道的那样简单，勾选复选框或者切换开关或者进行一些其他操作即可。

在理想情况下，这就是我们在签名方面想要采取的方式，使签名变得非常简单轻松，最终用户甚至不用以某种方式真正参与进来。但是我们鼓励人们参与并进行签名，因为从品牌、从声誉角度来看，这可以确保人们访问的是你放入 DNS 的网站。

沃伦 • 库马里： 我可以对此略微表示反对吗？

丹 • 约克： 当然，沃伦可以反对。

沃伦 • 库马里： 沃伦可以反对任何事情，因为他喜欢争论。我的意思是，这取决于它处于数字素养周期中的哪个点。我想我们所有人都会说 DNSSEC 是个好东西，但是对于互联网新用户而言它是最重要的事物吗？可能不是。当某人在注册域名的时候，它是最重要的事物吗？可能是，但是我的意思是，还有许多其他安全事务也很重要，你也需要将这些事情做好。因此，这在一定范围内具有重要性。

丹 • 约克： 好的，沃伦。这是一个很好的反对意见。请讲。

罗西奥 • 德拉弗恩特： 这就是为什么我也在考虑这一点。因为当你在考虑有关激励措施的问题时，就像对我们来说，我们参与的是 ICANN 和互联网治理。如果你没有技术背景，你就必须花时间和精力来理解为什么 DNSSEC 很重要。所以，注册人或用户，他们考虑的是他的公司或者其他方面。比如，我们应该如何构建叙述，比如，“好的，这很重要。也许你的域名会稍微贵些，但是它具备互联网或者安全性。”对吗？

丹 • 约克： 是的。这是挑战部分，坦率地说，这就是为什么我们在许多地方与 DNS 提供商、DNS 托管提供商或注册服务机构合作的原因，他们可能是相同的机构，我们还会鼓励他们采取这些做法，像某些 DNS 托管提供商一样进行签名，他们在默认情况下是进行签名的。或者，让人们能够轻松理解并实施。理想情况下，可以在不付出成本的基础上实施，但是不同的地方拥有不同的商业模型。

因为就像你说的，沃伦，我同意沃伦的观点，对于在新地点上网的某人的宏伟计划中的事情，这仍然是他们清单上的另一件事。但是根据他们的理解程度和使用它的能力，它可能不会升至最高点。

但是基于这样的原因，理想情况下，这只是基础设施中的事情。你们知道，这是在这些层面上处理的事情。沃伦，你是否还要对我说的表示反对？不是？好的。他要给你们展示。还有其他问题吗？我们的时间还够问一两个问题。没有？哦，莱文 (Levine) 先生。我这样说是因为我与约翰 (John) 熟识。

约翰 • 莱文 (JOHN LEVINE)： 不，我要说的实际上只是商业广告。

丹 • 约克： 商业广告？

约翰 • 莱文： 是的。早些时候，你们中的一些人提到了量子加密术可能会对 DNSSEC 产生什么影响，而巧合的是，有一场关于该主题的演讲，这就是在明天“技术日”举行的最后一场演讲。

丹 • 约克： 好极了。

约翰 • 莱文： 是的。坏消息是，演讲人会把它搞成一场浮夸的吹嘘，但是你们对此却无能为力。

丹 • 约克： 好的，谢谢，约翰。

韦斯 • 哈达克： 我们会假定是你，约翰，你没问题的。

丹 • 约克： 好的好的。约翰将在明天“技术日”结束时发表一场演讲，顺便说下，如果你是新人，我看到很多英才计划学员说自己是新学员，明天是“技术日”，会在这些会议室召开许多不同的会议。

我不确定是哪间会议室，你们可以查看“技术日”的日程安排，其中涉及了许多不同的主题，包括量子加密术、DDoS 攻击以及其他不同类型的事物，或者各种不同的主题。我还没有查看过本周的日程安排，所以我还不知道。但是不管怎样，在此期间会召开许多很棒的会议。

沃伦 • 库马里： 应该是在 516C 会议室。

丹 • 约克： 哦，大家听到没。好极了。我们找到了，开始时间是明天 10:30。还有其他问题吗？好的。如果没有，我就对大家今天的出席表示感谢，如果你想了解更多信息，欢迎与我们中的任何人交流，我们会再等几分钟。

再次说下，星期三 1:30 在隔壁的 517C 会议室，我们将举行 DNSSEC 工作坊，届时将涵盖一系列主题。你们可以访问网站的日程安排版块，查看具体的议程以及所有相关信息。非常感谢各位，祝你们在 ICANN 会议期间度过愉快的一周。

[会议记录结束]