神户 — 人人学 DNSSEC：初学者指南
日本标准时间 2019 年 3 月 10 日星期日 — 15:15 至 16:45
ICANN64 | 神户，日本

韦斯 • 哈达克

(WES HARDAKER)： 我们马上就会弄好。现在，它也会出现在所有这些地方。很好。

好的。今天我们要讨论的内容是，什么是 DNSSEC，它如何在你使用互联网时，在每个人使用互联网时保护大家，以及 ICANN 如何参与其中。我是来自南加州大学信息科学院的韦斯 • 哈达克。我们身后有一群优秀的人，他们稍后也会加入我们，等一下我再向大家介绍。

现在，我想给你们讲一个关于 DNSSEC 的故事，它最初是如何诞生的。可以说，在很久很久以前，早在公元前 5000 年的恐龙时代，它就出现了。这个故事始于乌格维娜 (Ugwina)，她是我们今天的主角。她住在科罗拉多大峡谷边上的一个洞穴里。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。他们相隔很远。大峡谷又深又宽。从一边到另一边的路非常遥远，导致他们不能经常见面说话。

在一次难得的见面中，他们跨越了大峡谷，开始交谈起来，然后他们注意到奥格的火堆产生的烟雾，他们觉得这是一个好办法。我们可以用烟雾信号来交流。很快，他们的聊天就变得非常频繁，他们使用烟雾来回交流意见，一切都很顺利。直到有

一天，喜欢捣蛋的穴居人卡明斯基 (Kaminsky) 搬到了隔壁，开始同时发出烟雾信号。

现在，乌格维娜就感觉很困扰了。大峡谷对面有两组烟雾信号，她不知道哪个是哪个。于是乌格维娜沿着大峡谷出发，想要把问题搞清楚。乌格维娜和奥格请教了村里睿智的长者。穴居人迪菲 (Diffie) — 很显然，现在一些人已经知道迪菲是谁了。迪菲是一位著名的密码学家，曾帮助开发了 DNSSEC 背后的技术，稍后我们会深入探讨。他跑进奥格住的洞穴，在那里，他发现了一些神奇的蓝色粉末。粉末的颜色很奇怪，然后，他跑出洞穴，来到火堆旁边，将粉末扔到火堆上，神奇的蓝色火焰开始冒出蓝色烟雾，现在，乌格维娜和奥格又可以愉快地聊天了，她只需要相信蓝色的烟雾，因为只有奥格的洞穴里有蓝色的粉末。

故事圆满结束，没错。我们讲完了。以上就是关于 DNSSEC 的介绍，相信大家都已经充分理解了。稍后我们会作一个更加详细的介绍，但它背后的概念，这种把一个东西变成另一个你肯定它来自正确地方的东西的神奇技术背后的概念，就是 DNSSEC。

下面，我们回到 DNS，首先看一下这张 DNS 概念概括图。如果你们之前了解过 DNS，或者有去参加今天早些时候和昨天早些时候的“人人学 DNS”会议，他们可能给你们看过这样的图。在这张图中，DNS 从最顶端开始，从根区开始，这一部分是

ICANN 大量讨论的内容，然后在它下面是所有 TLD，包括国际和地区代码，以及 com 等等，然后再下来是二级域名，比如 co.uk、bigbank.com 和 nic.ma。今天，我们将重点看看 bigbank.com。

大家需要知道，你们的 ISP 有解析器，解析器知道根区在哪里，只要知道根区在哪里，它就可以沿着这条链一直往下追溯，找到其他所有东西的位置。但首先，它必须从根区开始，然后才能往下，找到 com 的位置，然后以此类推，稍后我们会通过一个例子来详细说明，但基本上，它的工作原理就是，每一级都将解析器指向下一级。所以，在一开始，解析器唯一需要知道的就是根区在哪里。最终，在问题得到回答后，解析器实际上会将信息缓存一段时间，以备将来使用。

问题就在这里。DNS 中并没有安全机制。最初它被发明出来的时候，我不知道是哪一年，反正很久以前了 — 84 年吧，人们没有为它部署任何安全机制。那个时候，每个人都很善良，没有邪恶思想，但在后来，人们发现域名很容易被模仿，他们可以用自己的方式绕过系统，给出一个错误的答案，从而导致缓存很容易中毒，也就是说，解析器不仅会长期记住正确的答案，还会长期记住错误的答案。

为了进一步说明这个概念，我想请出这些穿白衬衫的人们，他们会通过一个例子让大家明白，解析器和 ISP 究竟是做什么的，我们从左边的用户乔 (Joe User) 开始吧。他今天要在

bigbank.com 网站上办一些银行业务，他会开始办一些银行业务，然后我们会看到 DNS 是如何一步步引导他得到答案的，希望是正确答案。

男性发言人（姓名不详）：他们想让我出镜。

拉斯 • 芒迪 (RUSS MUNDY)：你好，ISP。

韦斯 • 哈达克：是。

拉斯 • 芒迪：我要和 bigbank.com 对话。这是他的名字。

韦斯 • 哈达克：我不知道 bigbank.com 在哪里。我去帮你找找看，马上回来。

你好，根区，我想找 www.bigbank.com。你能告诉我他在哪里吗？

男性发言人
（姓名不详）： 你好，我是根区服务器，我知道顶级域在哪里，你是在找 .com 吗？你可以去 1.1.1 找到 .com 服务器。

韦斯 • 哈达克： 好，我现在就去。你好，.com。我在找 www.bigbank.com。你能告诉在哪里可以找到吗？

男性发言人
（姓名不详）： 我不知道 www 在哪里，但我可以告诉你 bigbank.com 在哪里。他在 2.2.2.2。

韦斯 • 哈达克： 你好，我想找 www.bigbank.com。你能告诉我在哪里可以找到吗？

拉斯 • 芒迪： 可以啊，我是 bigbank.com，我知道 www.bigbank.com 在哪里。它在 2.2.2.3。

韦斯 • 哈达克： 太棒了。我现在就去告诉我的用户。

拉斯 • 芒迪： 另外，他可能想要一些钱。

韦斯 • 哈达克： 你好，很显然你可以连接到 2.2.2.3。www.bigbank.com 就在这里。

男性发言人（姓名不详）： 谢谢 bigbank.com。

韦斯 • 哈达克： 好的。好吧。谢谢你们，DNSSEC 教程的扮演玩家们。我们很感激。等一下我们还会需要你们。请大家给他们掌声。不过待会儿会更好的。好的，请翻到下一页。

刚才那段滑稽短剧与乌格维娜和奥格聊天的方式非常类似，即，通过解析器获得信号，不过这是在邪恶出现之前的情况。现在的问题是，在邪恶卡明斯基来到这里并且弄出另一种烟雾信号后，情况会怎么样？这对 DNS 有什么影响？DNS 会如何遭到欺骗？问题是如何产生的？

接下来，我们会再次上演完全一样的滑稽短剧，真的完全一样，我保证。

拉斯 • 芒迪： 你好，ISP。

韦斯 • 哈达克： 你好。

拉斯 • 芒迪： 我需要找 bigbank.com 办理存款业务。你能帮我找到他吗？

韦斯 • 哈达克： 当然，不用担心。www.bigbank.com，我去问问根区。

你好，根区，我的一个用户想找 www.bigbank.com。你能告诉我他在哪里吗？

男性发言人（姓名不详）： 我告诉你，你可以去 1.1.1.1 问 .com 服务器。

韦斯 • 哈达克： 很好，我会去问他的。你好，.com 服务器。我的一个用户想找 www.bigbank.com。请问他在哪里？

男性发言人（姓名不详）： 我没法告诉你 www 在哪里，但我可以告诉你，bigbank.com 在 2.2.2.2。

韦斯 • 哈达克： 很好。我去那里问问。你好，我的一个用户想找 www.bigbank.com。你能告诉我他在哪里吗？

男性发言人（姓名不详）： 当然。没问题。

韦斯 • 哈达克： 很好。

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

韦斯 • 哈达克： 好的，谢谢。你好，用户，你应该去 6.6.6.6。www.bigbank.com 就在这里。

拉斯 • 芒迪： 听起来很不错。管它呢。现在我要 —

男性发言人（姓名不详）： 把存款给我吧，先生。非常感谢。

韦斯 • 哈达克：

好了。现在你们能看到问题在哪里了，对吧？可怜的用户乔，他真的不知道该相信哪个答案。他选择了相信他获得的第一个答案。这就是烟雾信号的问题，就像之前一样，实际上有两个信号，用户只需要相信其中一个，他们不得不随机选择，在这种情况下，乌格维娜真的不知道应该相信哪组烟雾信号。

现在，我们回到 DNS 概念概括图。刚才我们讲过顶部的根区，它下面的 .com，以及再下面的 bigbank.com，如果 ISP 的解析器查询到错误的系统，它可能得到正确的答案，也就是蓝色的那个，也可能得到错误的答案，也就是红色的那个。

DNSSEC 能够解决这个问题，这就是你们今天在这里的原因。通过使用数字签名，DNSSEC 向之前不存在安全机制的 DNS 添加了安全机制。它做了两件重要的事情。一是证明信息在传输过程中的任何阶段都没有被篡改过，二是证明信息来自正确的地方。你可以确保信息来自正确的原始位置，即使它被存储在鞋底或类似的东西上。它已经得到签名，并且签名永远有效。签名的密钥存储在 DNS 系统本身，这一点很好，因为如果要弄清楚信息是否安全，你实际上可以使用 DNS 自己来执行查询操作，找出你需要哪些密钥，稍后我们会用一个例子来说明。

解析器只需要…就像之前的解析器只需要知道根服务器在哪里，然后就可以开始沿着链条一路向下查询，DNSSEC 也是一样。解析器必须知道根服务器在哪里，它们必须知道根区密钥，然后才能在此基础上建立信任链，每一级都对下一级密钥

进行签名，直至信任链完成。所以，只要你沿着加密密钥一直往下，你就能保证自己获得的是正确的答案。

现在的优势是，回到之前我们的那张图，用户乔不知道该相信哪个。他不知道该相信蓝色还是红色。而现在，我们实际上可以进行验证，证明红色是不对的，它没法让你实现自己的目的。

下面，我们通过短剧来看看这个问题是如何得到解决的 — 你们能不能多做点好事，少做点坏事？

男性发言人（姓名不详）：　太棒了。

拉斯 • 芒迪：　你好，ISP，我要和 bigbank.com 对话，并且我需要知道你给我的答案是有效的。

韦斯 • 哈达克：　好的，很好。我来帮你。你好，根区，我的一个用户想和 www.bigbank.com 对话。你能告诉我他在哪里吗？

男性发言人
（姓名不详）： 我可以告诉你 .com 在哪里，它在 1.1.1.1，这是证明信息正确无误的凭证。

韦斯 • 哈达克： 好的，很好，我相信你。让我去问问 .com 服务器。

你好，你猜怎么着？我的一个用户想和 www.bigbank.com 对话。你能告诉我他在哪里吗？并且，我需要检查你的签名。

男性发言人
（姓名不详）： 没问题，感觉你的要求真多。我没法告诉你 www.bigbank.com 在哪里，但我可以告诉你 bigbank 在哪里，它在 2.2.2.2，这是签名。

韦斯 • 哈达克： 很好。我去问问。你好，我想要知道 www.bigbank.com 的地址。你能告诉我吗？

男性发言人
（姓名不详）： Bigbank.com 在 6.6.6.6。

韦斯 • 哈达克： 好的，等一下。你的签名在哪里？

男性发言人（姓名不详）： 我没有签名。噢，不！

韦斯 • 哈达克： 我再去问问其他人，我不相信你，臭小子。

你好，你能告诉我 www.bigbank.com 在哪里吗？

拉斯 • 芒迪： 这个嘛，我确实知道 www.bigbank.com 在哪里，它在 2.2.3，这是签名。

韦斯 • 哈达克： 看起来很合理。你好，用户先生，bigbank.com 在 2.2.2.3，我已经检查了签名，你可以放心。

拉斯 • 芒迪： 我看到这里的签名了，谢谢你。谢谢你，Big Bank。开始存款。

韦斯 • 哈达克： 好的，非常感谢。请问我们的表演者鼓掌好吗？他们做得很好。如果大家以后还来参加 ICANN 会议，你会发现，我们每次都会这么做。有人之前看过这个短剧吗？几个人，好的。

男性发言人（姓名不详）： [听不清]

韦斯 • 哈达克： 这就相当于蓝色烟雾。没错。现在，乌格维娜终于能看到蓝色烟雾了，因为它经过签名验证，在短剧中，我们使用了大家脖子上挂的小奖章，来表示用于在 DNS 树的每一级进行签名的密钥。

接下来，我会把时间交给我在这场 [听不清] 犯罪中的搭档拉斯 • 芒迪，他会通过一些例子向大家说明为什么你们需要 DNSSEC，以及实际部署时的一些简单指南。

拉斯 • 芒迪： 谢谢韦斯。我是来自 Parsons 的拉斯 • 芒迪，我在这里的目的是帮助大家更好地理解应该如何部署 DNSSEC，以及你们在这个过程中需要检查和思考的一些东西。

关于 DNS，很多时候人们会忽略一个非常重要的方面，那就是，如今，互联网中几乎每一个应用程序都会使用 DNS，所

以，如果不能确保 DNS 的安全，让它们遭到篡改或者因为某个原因出现问题，出现漏洞或类似问题，那么最终受到伤害的是应用程序，最终出现问题的是应用程序。你无法获得连接。在我们的短剧中，用户乔无法和他的银行对话。所以，了解 DNS 是什么以及 DNS 做什么，这是最基本和广泛的问题。

那么，既然我们必须确保所有应用程序都正常运行，为什么人们要攻击 DNS 呢？我已经关注 DNS 和 DNS 安全活动很久了，久到我都不想去数有多少时间，坦白说，我从未见过或听说过人们攻击 DNS 仅仅是为了篡改 DNS，然后就此打住，什么都不做。这不是他们的目的。

他们的目的是，他们想要获取在 DNS 查询发生后运行的一些应用程序中的信息。比如说，他们也许想要复制来自某个特定地方的所有电子邮件，这样他们就可以 — 对于该邮件服务器发送邮件的所有目的地，他们就可以坐在那里，将邮件地址提供给中间邮件服务器的伪造人，后者便可以收到来自正常邮件服务器的所有电子邮件，然后经过篡改再发送给用户，最终收到邮件的用户永远不会知道这其中的区别。这就是中间人攻击。

几年前，幸运的是，我之前还回过头去看能不能再次找到那些课程，不过与几年前不过，现在互联网上似乎看不到它们的身影了，那个时候，有一两个课程的老师会在教学大纲中要求学生写一段 DNS 劫持程序。在教学大纲中，我看不出有什么迹象表明这是一件坏事，是错误的。但除此之外，市面上也有一些

软件包可以让你做同样的事情。我们很容易找出世界上已有的帮助工具或软件。那么，DNSSEC 的作用是什么呢？

从短剧中，大家可以看到，用户发起的查询会经历一个过程来验证信息来源的正确性和内容细节的正确性，验证它们没有在查询过程中被篡改。

这是一个说明一些劫持如何工作的例子。很简单的一个例子，不过还是比我们之前的短剧要复杂些，我们继续，请点击…大家可以看到，这是第一条查询，虚线从用户乔出发，一路来到权威服务器，然后带着答案回到递归服务器，最终回到用户，在所有这一切完成之后，查询实际上会发送至 Web 服务器。可以看到，这里面有很多网络流量的传输，但大多数人都不会注意到这一点 — 这就是 Web 服务器流量、电子邮件流量、Facebook 流量或你可能正在做的其他任何事情发生之前的 DNS 流量。

几年前，我们曾建立了一个定制网站，它会验证所有进来的查询，对他们进行 DNSSEC 验证，执行 DNSSEC 验证检查，对于经过验证的查询，我们会提供一个小的 X 符号，一个小的打勾标志，不过这只是针对这个特定网站所做的，如果你发起了同样的查询，但是没有执行 DNSSEC 验证，你可以在网页内容上看到，这些内容事实上没有经过 DNSSEC 验证。

之后，我们实施了一次 DNS 劫持，它会向大家展示会发生什么情况。继续，先点击第一个，然后再点。邪恶博士，我们的帮

手戴着黑色大斗篷从侧面趁虚而入，给出一个答案，这个答案将用户乔带到了经过重定向的网站，虽然合法的查询和答案继续传输到了系统，但用户乔和他的机器永远不会收到了，因为第一个答案，来自邪恶攻击者的答案已经到达他的机器，并且他的机器说：“好，得到答案了，这下我不用再担心别的了。”

有了 DNSSEC 之后，你得到的数据包流与在这里看到的并无二致，不同之处在于，有了验证检查之后，来自邪恶攻击者的数据包和 DNS 答案将不会再被用户乔的机器所接受。我猜还有更多的 [错误]，但无论如何，是的，这些数据包只是不断地流入流出。

现在，我们的定制网页会是什么样子？这个定制网页就跟我之前给你们看的那个一样，现在来看下一个。在我们实施了劫持之后，网页上显示的内容实际上是史蒂夫 • 克罗克 (Steve Crocker) — 他是 ICANN 董事会的主席，参与 DNSSEC 事务已经很长时间了 — 我们在另一个位置放了一个幽默的链接，如果用户在未执行 DNSSEC 验证的情况下访问该网站的话，他们就会在屏幕上看到这个内容。所以在这个例子中，我们实际上是劫持了我们自己的信息，只是为了向大家演示如果这样的网页遭到攻击会怎么样。

这个是在大约 10 年前，你从一个空的解析器和空的浏览器开始访问 cnn.com 时，DNS 系统会执行的解析操作。有这么多。

而今天，它变得更多了。看起来就像这样。这只是为了显示一个网页的内容而已。下一张。

我们做的所有这一切只是为了确保 DNS 区域数据，确保区域内容内容正确无误，并且在流经互联网的过程中始终保持正确，这就是部署 DNSSEC 的原因。

另一张非常简单的图，只是一个没有经过签名的区域，发起查询，给出答案…它的步骤非常少，在后台运行得也非常快。然后当你放入 DNSSEC，无论你是在运营解析器还是提供验证服务，如果是 ISP 或本地企业的话，也无论你是运营大型域名服务器，比如说你可能运营着一家注册服务机构并提供大量的域名服务器。如果你已经能够运营自己的 DNS 系统，那么在这些系统中集成 DNSSEC 应该相对比较简单。你面临的最大挑战将是支持软件集成 DNSSEC 功能，这在过去几年里已经得到了很大的改进，所以大多数时候你都能够实现 DNSSEC 验证。如果你运营的是自己的域名服务器，那么只需安装正确的软件就可以了。

如果你的运营规模非常大，比如你是 TLD 运营商或非常大型的企业，你可能会想要自己来做这件事，而不是把它外包出去。再说一次，这是对你组织已经拥有的职能的一种扩展。

现在我们来看看，如果你是一名最终用户，就像在座的各位一样，那么你可以要求你的服务提供商，无论他们是企业还是 ISP，你都可以要求他们提供 DNSSEC 验证。在这种情况下，你

可能不会运营自己的域名服务器 — 虽然还是有少数人会自己运营 — 但大多数时候是别人来运营，这个时候你就需要要求这些运营商执行 DNSSEC 验证，以防止邪恶博士进来窃取你的 DNS 信息。

就像我之前所说，DNSSEC 最为关注的是确保各个实体，无论是 bigbank 还是 com，亦或是其他企业，确保他们在一开始放进来的区域数据始终存储在系统中，确保这些数据在由 DNS 系统传输给最终用户的途中不会遭到篡改。

所以，区域内容才是最重要的，才是你们真正需要关注的东西，你们要确保区域内容到达正确的位置，这就和其他任何事情一样重要。曾经，大家一度关注很多东西 — 噢，DNSSEC 使用加密，那可是加密啊，那真的是很特别的东西，所以我们需要做一些特别的事情。你需要确保自己的密码得到妥善管理，自己的密钥得到妥善管理，但大多数现代软件都能够做到这一点。你们需要记住，你们还需要妥善管理自己的内容，确保在把它放进域名服务器的途中不会遭到篡改，然后一旦它位于域名服务器中，使用 DNSSEC 对它进行验证直至最后。

从前面的图来看，这和上一张框图没有太大的区别。大家可以看到，它只是从概念上增加了一些额外的记录类型，DNS 系统中所谓的记录类型，包括生成权威域名服务器中包含的区域，然后随着 ISP 往下查询，从根区到 com 再到 bigbank，验证递归服务器一一验证该信息，也就是检查小奖章。

总的来说，对于部署 DNSSEC，最重要的是看你的组织或你的特定实体在运营你当前所使用 DNS 系统方面的参与度如何。如果你在所有域名服务器中都运营当前使用的 DNS 并且自己运营它们，那么你可能需要执行那些额外的功能，以便在适当位置提供 DNSSEC 签名和验证。如果你不是自己运营，例如，许多大型企业会将 DNS 职能外包给其他企业，比如 parsons.com，使用这样的外部服务提供商。他们选择使用外部服务提供商的主要原因之一就是，外部服务提供商会替他们完成 DNSSEC 部署。

所以，如果你使用外部服务提供商，你可能会要求他们来替你部署 DNSSEC，如果第一家提供商或你当前使用的提供商说：“抱歉，我不知道你想要部署 DNSSEC，我做不到。”不要害怕把他们给换掉。找一家能够部署 DNSSEC 的服务提供商。外面这样的服务提供商有很多。

本次活动由 ICANN 和安全与稳定咨询委员会共同主办。今天现场也来了一些根服务器系统咨询委员会的成员，来为大家提供帮助，这很好，还有国际互联网协会的 Deploy360 Programme 计划，他们长期为这些活动提供支持，我想，这应该是我们本次演示的最后一张幻灯片。下面是提问时间。

韦斯 • 哈达克： 好的，非常感谢拉斯 (Russ)。我们会请邪恶博士在下面为大家递麦克风，如果有人对 DNSSEC 的工作原理有任何问题，或者不明白前面讲到的任何信息，或者有其他问题，请举手，安德鲁 (Andrew) — 抱歉，邪恶博士会过来给你麦克风。

安吉拉 (ANGELA)： 你好，我叫安吉拉。我来自通信监管机构。如果公钥被攻击者劫持了，是否有任何机制能够，好吧，我是说，万一密钥被劫持了，我还能通过什么方式验证这是不是正确的响应呢？

韦斯 • 哈达克： 这个问题非常好，让我有点不太习惯。谢谢你。这是个很好的问题。如果密钥泄露了会怎么样？

我说几点吧，实际上现场还有很多其他专家。如果你们想要回答，请直接举手。

实际上这里面有两种密钥，我们简化了很多，但它实际上有一个公钥和一个私钥。你提到了公钥。你可以把公钥给任何人。这是安全的，公钥的目的就是这个，你可以把它广泛分发给其他人。你需要保护的是私钥。如果私钥泄露，有人侵入你的系统，窃取了你的私钥，那么，你必须马上告诉你的父级。举个例子，如果你是 bigbank.com，你必须告诉父级，说：“我需要一个新的密钥，请更改密钥链。”

大家还记得奖章接受检查的方式吧？基本上，你需要换掉其中一个奖章，比如换掉挂在 .com 脖子上的奖章，说：“我有一个新的奖章要给你，我要使用新的密钥。我的私钥现在不一样了。”实际上，这个操作很快就可以完成。虽然这里面涉及到很多复杂的东西，比如说存活时间价值、缓存以及其他各种有用的东西，但从根本上说，你需要做的只有这个，你只需要告诉你的父级：“我有一个新的密钥。我需要马上把它换了。”整个过程相当快，然后你就会变得安全多了。

还有其他问题吗？很好的问题，谢谢。

萨维奥 • 维尼修斯 • 德 • 莫莱斯 (SAVYO VINICIUS DE MORAIS)： 你好，我叫萨维奥 (Savyo)，来自巴西，是新生代计划的成员。我想问的是，你们在让互联网上更多人使用 DNSSEC 方面面临的最大挑战是什么？

韦斯 • 哈达克： 你是问普及 DNSSEC 面临的最大挑战是什么吗？有人想要回答吗？我可以尝试回答一下，不过，拉斯，还是你来吧？

拉斯 • 芒迪： 一直以来，无论在宣传教育还是激励鼓励方面，我们都做了很多努力，通过类似这样的论坛，而且，许多实体也做了大量的工作来鼓励软件提供商确保他们的软件具备所有适当的

结构和功能，同时与应用程序提供商合作，鼓励他们也支持这一技术。

在我看来，要让更多用户使用它，我们面临的最大挑战之一就是来自用户，无论他们是个人用户还是作为企业一部分的用户，最困难的是让他们自愿说出：“我想要使用 DNSSEC 验证。”一些公司的注册服务机构职能就是不愿意使用 DNSSEC，这样的话，如果你正在使用这家公司，你就会很难获得 DNSSEC 验证。现在，几乎所有注册管理运行机构都在使用它，但就最终用户来说，其实最终用户也可以要求他们使用的软件提供商提供 DNSSEC 验证，并不断加大要求的力度，或许这是现阶段这些提供商需要听到的最大动力，因为随着时间的推移，各种程序直接接触到这些实体，大多数时候我们客户获得的答案都不是他们想要的答案，这也是我们举行这些会议的原因之一，即，帮助大家不仅理解它是什么，而且还要理解大家作为最终用户所拥有的权利，那就是要求提供商提供 DNSSEC 验证。

男性发言人（姓名不详）：

我想对拉斯的发言做点补充。在前面的幻灯片中，有一种图提到了验证解析器。我们在衡量 DNSSEC 是否取得成功时，其中一个衡量标准就是，有多少区域使用签名，但在此之外，与之同样重要的是，谁在验证？即便全世界所有域名都使用签名，

但如果应用程序不使用签名，如果递归解析器不对它们收到的信息进行验证，那一切都是白搭。我还想讲一些东西来着，但一时想不起来了，所以，我还是把麦克风关掉吧。

韦斯 • 哈达克： 没关系。很好的问题，其实我们一直在努力收集统计数据和追踪使用情况，以了解 DNSSEC 是否仍在增长，如果大家看看一直以来它的部署量就会发现，DNSSEC 本身仍在增长。虽然增长的速度没有达到我们的期望，因为它从来没有达到过。如果达到我们期望的速度，那今天所有问题都应该解决了。

这是我整理的一个页面。它叫做 stats.dnssec-tools.org。上面的数据来自维克多 • 杜楚尼 (Victor Duchovny)，他是在邮件服务器中部署 DNSSEC 的专家。如大家所见，在最近一段时间里，实际上很近，就在过去几个月里，这张图有一些比较大的增长，它追踪的是邮件服务器是否真的使用经 DNSSEC 签名的邮件记录。其中一些大幅增长实际上源自于，最近一些公司开始启用了所有东西，他们的所有邮件服务器。他们运营着不止一个邮件服务器域名，同时把它们全部打开，这就是为什么会出现这些大幅增长。

好消息是，我们获得了越来越多的使用量，但还有很多宣传工作，很多像这样的活动以及像 ISOC 为推广它所开展的活动。尽管现在已经有大概 1000 万个域名开始使用签名，但我们仍

有很多工作要做。事实上，.com 的数量远比这多得多，所以我们一直在努力提高它的使用量。还有其他问题吗？

[科菲 (COFY)] 我叫 [科菲]，来自加纳域名注册管理机构，我有两个小问题。第一个问题是，我们需要定期更改私钥吗，还是等到它泄露了之后再更改，哪一种做法是良好的标准实践？第二个是，DNSSEC 是注册服务机构和类似机构获得任何形式 ICANN 认证的强制要求吗？

韦斯 • 哈达克： 问得好。关于你的第一个问题，目前有两种不同的观点。有些人认为在密钥泄露之前，你不需要更改它。虽然有时候你能够设置强度非常高的密钥，但有时候你也可能会设置非常弱的密钥，如果改后的密钥没有那么强的话，你真的没必要频繁地去改。其实告诉大家，我就没有经常改密钥。

一般的说法是，如果你不去改，你就不会知道具体应该如何操作。所以，从操作上来讲，如果你经常改密钥，你完全可以确保在需要迅速更改密码加以应对时，你具备所需的技能，所以很多人会定期更改他们的密钥，比如一年一次诸如此类，就是为了这个目的。

关于第二个问题，ICANN 对与他们签订协议的某些实体确实有强制要求。例如，所有新 gTLD 都必须支持 DNSSEC。但我不知

道对注册服务机构是不是也是这样。新注册服务机构 [听不清] 必须支持 DNSSEC 吗？

拉斯 • 芒迪： 不太确定，但我觉得，这对注册服务机构应该不是强制要求。

韦斯 • 哈达克： 很好的问题。谢谢。还有其他问题吗？这里有一个，安德鲁，完了后面还有两个。

[科里 (CORY)]： 我叫 [科里]，来自美国。我有一个特别相关的问题 — 据我所知，DNSSEC 已经存在很多年了，但最近有一些关于 DNS over HTTPS 或 TLS 的讨论，它们与 DNSSEC 有什么关系呢？它们是相互互补或相互竞争的关系吗，它们彼此之间是如何联系的？

韦斯 • 哈达克： 很好的问题。你们都知道的很多。这让我印象非常深刻。总的来说，它们并不是相互竞争的关系。它们在很多方面是互补的。DNSSEC 负责对数据进行签名，但不涉及数据的传输方式或存储位置，它只是一个符号，让你明白这条记录没有被篡改过。最近出现了一种规范叫 DNSSEC over TLS，用于加密和验证两台设备之间的流量传输。DNS over HTTPS 的作用也是如

此，只不过是通过 HTTPS 传输数据，它的主要优势是可以穿过仅允许正常 Web 流量通过的防火墙。

对于每一种技术，人们选择它们所出于的原因各种各样，但 DNSSEC 与其他两种技术之间最重要的区别是，DNSSEC 会对数据进行签名，这样无论你从哪里获得它，你都知道它是真实的。你知道它的完整性得到了保护。如果使用 DNSSEC over TLS 或 DNSSEC over HTTPS，虽然你确定这个事务是真实的，但你不知道它们是如何获得该数据的。

所以，DNS 往往会使用大量附加技术，很多情况下 — 例如，如果你使用 DNS over HTTPS 去跟提供商对话，你就不会知道，在幕后，他们实际上去获取然后检查了数据。目前权威服务器还没有开始使用 DNS over TLS 或 HTTPS。

拉斯 • 芒迪： 快速插一句，是关于周三工作坊的。本周三，我们会举行一场 DNSSEC 工作坊，届时会有关于这个特定主题的报告。

韦斯 • 哈达克： 周三是个好日子。如果你想要了解更多有关 DNSSEC 的信息，周三去参加就对了。

拉斯 • 芒迪： 我快速总结一下你说的，DNSSEC 的目的是保护数据。而基于加密协议的 DNS 是为了保护查询的隐私，这是两码事。

韦斯 • 哈达克： 是。在你后面，安德鲁。后面那位，好的。

[巴尔吉什纳 (BALGISHNER)]： 你好，我是来自尼泊尔的 [巴尔吉什纳]。DNSSEC 的目的是保护最终用户，对吗？那么，将 DNSSEC 变成一项强制性规定有没有什么困难？或者说，或许你们可以规定一个截止日期，在这一天之前所有人都必须转移到 DNSSEC，这有什么困难吗？

韦斯 • 哈达克： 很难，因为我们所处的是一个自由的世界，人们可以选择使用，也可以选择不使用。人们经常说的一句话是：互联网世界里没有警察。在互联网世界，没有任何人能强制实施善与恶，你必须选择适合自己的技术，确保你的网站能够正常运行，诸如此类，所以很遗憾，我们没有办法强制每个人都使用它。如果有这样的办法的话，事情就变得容易得多，不是吗？但现实是没有。

拉斯 • 芒迪： 我们听说，有些组织已经选择开始实施规定使用某些安全技术的安全政策。所以，某些组织已经选择这样做，但在这一点上，没有放诸四海而皆准的答案。

韦斯 • 哈达克： 说得非常好，目前确实有一些政府规定其所有政府基础设施都必须使用 DNSSEC，以树立良好榜样。谢谢，说的很好。

男性发言人（姓名不详）： 你好，我是来自斯里兰卡的 [听不清]。我有一个小问题。不可否认，DNSSEC 中断了正常的 DNS 流程。那么，当这种情况发生时，互联网的速度是否会有所降低，如果是的话，会有怎样的降低？

韦斯 • 哈达克： 好的，如果我没理解错的话，你担心的是，DNSSEC 验证会导致网络变慢。非常好的问题。我说几点。首先，使用 DNSSEC 确实会慢一些，因为它实际上要多几个步骤，相关方面有很多研究。你可以去找一下这些研究，人们实际上已经衡量过了。

最重要的一点是，DNS 数据会缓存，在幻灯片中我曾提到过一次，但当时我们没有讲太多。与它一样，安全密钥也会缓存，所以一旦你完成 bigbank.com 查询，所有这些记录都会存储在缓存里，缓存时间取决于你自己的设定。它们并不会每次都重

新验证。一旦完成验证，它们便会把它放在缓存中，把它标记为安全，然后，已经缓存的数据可以使用很长一段时间。这是 DNS 很棒的一点，即，虽然第一个人在查询时，服务器的响应速度可能会稍微慢一点，但这种速度降低几乎难以衡量，然后，之后所有人在查询时都会收到缓存的数据，响应速度会非常快。很好的问题。

[克莉丝蒂安 (CHRISTIANNE)]： 你好，我叫 [克莉丝蒂安]，来自象牙海岸。我想知道的是 — 我不是太专业，所以我的问题听起来可能有点愚蠢。

韦斯 • 哈达克： 不，没关系，请讲。

[克莉丝蒂安]： 我想知道的是，在 DNS 已经被劫持的情况下，DNSSEC 有没有什么程序可以解决这个问题，有没有什么实例，比如说你可能不得不违反这些实例，直接采取行动？

韦斯 • 哈达克： 我认为，你提出的这个问题，在很多协议甚至很多物理系统的安全机制中，都是一个非常难的问题。人们都是这样，在为时已晚的时候才会想起保护自己的系统。

所以从本质上讲，你问的是，如果有人已经闯入你的房子，偷走了你的钱，你能对这个既定的事实做点什么？你不能。你只能在事情发生之前给自己的系统上更好的锁来保护它。所以，对于已经遭到 DNS 劫持的情况，DNSSEC 不具有任何修复功能。好消息是，希望缓存最终能以同样的方式过期，这样那些不良信息也会消失，然后，希望你的用户能开始获得良好的信息，但现实是，如果你想要自己的 DNS 数据从今天开始受到保护，你就必须在遇到这些问题之前部署好 DNSSEC。明白了吗？谢谢。

亚伯拉罕 (ABRAHAM)： 我叫亚伯拉罕，来自尼日利亚。我的问题是，在部署 DNSSEC 时，我们需要升级系统硬件吗，还是说就用我们在部署前使用的那些硬件就可以了？谢谢。

韦斯 • 哈达克： 好的，我想如果我没有听错的话 — 因为我挨着显示器的，有很多回声。你想知道的是，部署 DNSSEC 是否需要升级硬件。是这样吗？比如说加 CPU 或内存，这种？好的，很好。

拉斯 • 芒迪： 关于这个问题，已经有人做过一些不同的分析，大多数是由关注 TLD 或根级别的人所做的，简单来说，他们的结论是，我们目前的正常增长和硬件更换周期就已经足够了。

但是，具体数字是多少呢？根据我的记忆，硬件对签名的影响可能是 3% 到 8%，但这不是实时的时间。它不是…签名发生在加载区域之前。对于验证，影响大约在相同的水平，可能高达 10%，虽然这不是什么显著的影响，但在你分析自己 DNS 基础设施当前的硬件升级计划时，有必要考虑到这一点。

韦斯 • 哈达克： 谢谢。另一件值得注意的事情是，验证确实会带来内存需求的增加，因为会有更多的记录，诸如此类。你需要更大一点的内存。举个例子，我想我服务于区域可能有 20 年左右了，在我做的所有事情中，我从来没有为部署 DNSSEC 购买过新硬件。如果你是一家有大量记录条目的大型 TLD 运营商，那么你可能需要考虑，但大多数人都不需要考虑，就用你们现有的硬件就可以毫无问题地使用它。

[保罗 (PAUL)]： 你好，我是来自英国的 [保罗]。政策有没有规定任何机制来追踪和监控对 TLD 或寄存器的 DNS 入侵？

韦斯 • 哈达克： 监控什么？我们今天讨论的是 DNSSEC。你的意思是，监控它们的安全性能还是它们 [传输] 的数据？

[保罗]： 建立一个入侵数据库以便清除坏人？

韦斯 • 哈达克： 要监控资源是否遭到滥用，这真的很难，因为现实情况是，最终你不得不监控整个世界。我可以在 TLD 旁边监控，我可以验证，比如验证他们每次都传输的是正确的信息，但通常攻击并不是发生在这里。攻击往往发生在 [你的最终用户那里]，诸如此类，所以最终你将不得不监控世界上的每一个 ISP。这是一个非常复杂的问题。如果你想要更深入地讨论，稍后尽管来找我，因为这个问题很难，如果我们有答案的话，现在我们应该已经抓到所有坏人了。

男性发言人（姓名不详）： 谢谢。针对前面对 DNSSEC 硬件需求的回答，我想简单补充一点，目前，捷克网络信息中心 nic.cz 正在发布关于 DNS 和 DNSSEC 服务器的常规基准。你们可以之后来找我。我会告诉你们链接，总的来说，它对硬件的影响微乎其微，只有一点点，除非你一台设备每秒钟要处理大约一百万次查询，否则你根本不会注意到有任何影响。

韦斯 • 哈达克： 好的，非常感谢。安德鲁，这里。

[布朗温 (BRONWYN)]： 你好，我是来自澳大利亚的 [布朗温]。我想问的是，在你们刚才的短剧中，是解析器去对每一级域名的证书执行验证，所以我想问，为了支持这些额外的验证，是否需要对解析器层级进行任何更新或软件更改？因为在我看来，解析器需要同时对使用 DNSSEC 和未使用 DNSSEC 的域名进行验证。

韦斯 • 哈达克： 非常好的问题。好消息是，如今大多数解析器软件实际上都支持 DNSSEC，比如 BIND 和 unbound，这可能是最大的两个了。我不记得 unbound 的版本了，但至少在过去的 5 年或 10 年里，它们都支持所有比较重要的 DNSSEC 功能。所以，如果你是最近开始使用，或者甚至向操作系统那样使用任何 ISP 服务器平台分发内容，我几乎可以向你保证，Windows 解析器目前也能做到，所以如果你是最近部署了什么，这真的不是问题。它已经存在很久了。

[克里扬 (CREJAN)]： 你好，谢谢你。我叫 [克里扬]，来自瑙鲁。我猜这是为傻瓜们准备的 DNSSEC 课程，所以我要问一个傻瓜问题。从 ISP 的角度来看，是否有任何能告诉他们必须部署 DNSSEC 的指示物或危险信号？

韦斯 • 哈达克： 这是一个很好的问题。ISP 是需要部署验证工具的人，是需要部署 — 在短剧中，你们可以看到，我的朋友沃伦 (Warren) 从一个人走到另一个人。他们需要完成大部分的工作。他们需要与根区对话，需要与 TLD 对话，需要与服务器对话等等，而且他们还需要确保自己的软件能够同时处理安全和不安全的查询，因为现实情况是，除非整个世界都安全，否则你不能强制别人部署 DNSSEC。

值得注意的是，虽然我们并没有在幻灯片和短剧中提到，但 DNSSEC 本身暗含这样一个答案“我是安全的。你询问的另一台服务器不安全，我可以为你验证它不安全，但最终你需要自己判断。”所以，实际上它有一些内置技术来实现部分保护功能，这样你就可以知道，你到底是安全的还是不安全。

毫无疑问，ISP 应该做的当然是监控他们的日志，确保 — 尤其是在他们开始发现验证失败时，可能有地方遭到攻击了，或者可能互联网上出现了问题。事实上，无论你要不要部署安全技术，监控日志都是一件非常重要的事情。

[阿尔菲法 (ALFIFA)]： 你好，我是来自孟加拉国的 [阿尔菲法]。我不确定你适不适合来回答这个问题。

韦斯 • 哈达克： 如果我不适合，还有他。

[阿尔菲法]： 我的问题是，你们在实施 KSK 轮转后有没有遇到过重大事件，你们又是如何处理的？

韦斯 • 哈达克： 很好的问题。你来吧，因为要我回答的话，我会说去参加 DNSSEC 工作坊吧，问题是，实施 KSK 轮转后有没有什么问题，你们是如何处理的？

拉斯 • 芒迪： 谢谢。抱歉，我听的不是很清楚。这里的音响效果有点具有挑战性。言归正传，之前很多人预测，KSK 轮转会是一件虚张之事，事实上，在旧的密钥被撤销后，流量方面出现了一些显著的不同，但我们随后就此举行了一场工作坊会议，后面会有一些相关的信息出来，事实是，从运营的角度来看，这对 KSK 没有任何明显的影响。可以说，无论从哪个方面来看，这都是一次成功的行动。结果非常成功。

韦斯 • 哈达克： 之前的 DNSSEC 研讨会有很多关于 KSK 轮转为何推迟一年，具体发现了什么的演示报告，大家可以去看一看。我本人就做过很多次报告，很多其他人也是如此。周三还会有关于这个主题的报告，这大概是最后一组报告了，因为旧密钥的撤销工作已经在 1 月 11 日执行，这是密钥轮转的最后一个步骤，然后会有一些有趣的数据出来，值得大家去看一看。如果你想要网址

列表，可以稍后来找我。如果你真的很无聊，我还可以把视频发给你，内容挺好的。还有其他问题吗？我们还有一点时间。

好的。没有人举手，那么，感谢大家提出这么有见地的问题。我想，你们真的是我遇到过的最有见识的观众之一了。你们提出的所有问题都有很强的技术性，看来你们都提前做了功课。这里没有愚蠢的问题。如果有人还有问题的话，稍后可以尽管来找我。所有这些技术都需要很长的时间来学习，我们已经做这行 10 年，20 年了，所以，这里没有什么愚蠢的问题。这里只有一些你刚刚学过的，以及你还有很多要学的问题。

稍后我们很多人都会继续留在这里。欢迎大家来交流。与此同时，祝大家在 ICANN 会议剩下的时间里玩得开心，可以的话，请一定来参加周三的 DNSSEC 工作坊，因为那是另一个学习东西的好地方，还有通常在周一举行的技术日也是如此。非常感谢。

[会议记录结束]